



## **Exhibit 2.3.1**

### **Solution**

### **Modification 23**

VA-180112-ATOS

**COMMONWEALTH OF VIRGINIA  
VIRGINIA IT AGENCY (VITA)  
SUPPLIER STRATEGY AND PERFORMANCE DIVISION**

7325 Beaufont Springs Drive  
Richmond, VA 23225

## Table of Contents

1.0	Introduction .....	5
2.0	Information Security Program Requirements .....	5
2.1	Information Security Program .....	5
2.2	Information Security Practices and Processes.....	6
2.2.1	Security Awareness and Training .....	7
2.2.2	Governance, Risk and Compliance Tracking.....	7
2.3	Service Integration .....	8
2.3.1	Systems and Tools .....	9
2.3.2	Supplier Security Tools .....	10
2.3.3	Patch Management .....	11
2.3.4	Reporting .....	12
2.3.5	Security Dashboard.....	12
3.0	Security Requirements .....	13
3.1	Threat Management.....	13
3.1.1	Digital Forensics Investigation .....	13
3.1.2	Managed Detection and Response (MDR) .....	15
3.1.3	Security Incident Response .....	18
3.1.4	Rapid Malware Response .....	19
3.1.5	Major Security Incident Response.....	20
3.1.6	Threat Analysis and Intelligence.....	21
3.1.7	Security Operations Center .....	22
3.2	Perimeter Network Security .....	26
3.2.1	Managed IDS/IPS .....	26
3.2.2	Web Content Filtering .....	28
3.2.3	Malware Protection.....	31
3.2.4	Network Forensics/Full Packet Capture .....	32
3.2.5	Data Loss Prevention (DLP) .....	33
3.2.6	Compliance Management .....	35
3.2.7	Vulnerability Management.....	35
3.2.8	Penetration Testing .....	35
3.2.9	Managed Firewall .....	36
3.3	Internal Network Controls.....	39



---

3.3.1	Managed IDS/IPS .....	39
3.3.2	Web Content Filtering .....	40
3.3.3	Malware Protection .....	43
3.3.4	Full Packet Capture .....	44
3.3.5	Data Loss Prevention .....	45
3.3.6	Compliance Management .....	46
3.3.7	Vulnerability Management .....	46
3.3.8	Penetration Testing .....	47
3.3.9	Managed Firewall .....	47
3.4	End Point Security .....	53
3.4.1	Malware Protection .....	53
3.4.2	Managed Host Intrusion Prevention .....	55
3.4.3	Managed Firewall .....	56
3.4.4	Data Loss Prevention .....	58
3.4.5	Network Access Control (NAC) .....	59
3.4.6	Endpoint Application/Process Whitelisting .....	61
3.4.7	Endpoint File Integrity Check .....	62
3.4.8	Compliance Management .....	63
3.4.9	Vulnerability Management .....	63
3.4.10	Penetration Testing .....	63
3.4.11	Full Disk Encryption (Attached Device) .....	63
3.5	Application Security .....	65
3.5.1	Source Code Scanning .....	65
3.5.2	Vulnerability Scanning (Application Scanning suspended on MOD 23 Effective Date) .....	65
3.5.3	Web Application Firewall .....	68
3.5.4	Compliance Management .....	70
3.5.5	Vulnerability Management .....	70
3.5.6	Penetration Testing .....	70
3.5.7	Access Management .....	70
3.6	Data Security .....	71
3.6.1	Managed Encryption (Managed Encryption Platform suspended on April 1, 2022) .....	71
3.6.2	eDiscovery/Preservation .....	73
3.6.3	Certificate/Key Management .....	74

---

---

3.6.4	Reserved .....	75
3.6.5	Data Loss Prevention .....	75
3.6.6	Data removal / device disposal .....	78
3.6.7	Enterprise Remote Access .....	78

## 1.0 Introduction

The solution that Atos proposes to the Virginia Information Technologies Agency (VITA) is designed to add additional dimensions of strength and agility to the Agency, whose current security posture is already very strong. Our solution differentiates itself through our:

- ▶ foundational adaptive platform (vs. a series of disparate point solutions), a highly integrated and open architecture providing maximum security protection near real time, and elasticity to change as VITA's needs dictate,
- ▶ our evolutionary approach – minimizing risk in transition for VITA by modernizing and replacing the pre-existing tooling currently deployed at VITA, and Atos' approach to re-shaping the role of the Atos security staff to that of managed detection and response (MDR) proactive security hunters leveraging the foundational tools embedded; and
- ▶ our proven public sector experience with the Multisourcing Service Integrator (MSI) model

To accomplish this objective, Atos is migrating premise-based services, wherever possible, to cloud-based solutions. This strategy reduces complexity, enhances integration, and provides high-availability due to the resilience of cloud fabrics. Services we are migrating from premise-based include the SIEM, network intrusion prevention, and endpoint security services.

The Virginia Information Technologies Agency (VITA's) participating Agencies (VITA customers) remain committed to the immediate and long-term goals of maintaining exceptionally high standards of services while leading technology transformation for the various Commonwealth agencies. VITA's Commonwealth Security & Risk Management (CSRM) Directorate is tasked with protecting citizen data and providing a safe, secure technology environment that enables the Commonwealth's agencies to accomplish their respective missions. Atos understands that VITA seeks to continuously improve security, disaster recovery (DR) capabilities, and to provide reliable IT security services across the Commonwealth.

Atos' approach is to continue the progress that is underway at VITA, and to blend VITA's vision of security with Atos capabilities to deliver on it. The Atos team consistently applies rigorous standards of accountability, transparency, and cost-efficiency across our security practice. Additional, Atos bring the following advantages to VITA's security practice:

- ▶ Experienced leadership and continuous availability from senior project management based in Virginia
- ▶ Active engagement with VITA customers through focused service teams and governance participation
- ▶ Experience in supporting large-scale state agency programs and IT projects like Virginia
- ▶ Extensive experience in working in multi-vendor environments in coordination with a Multi-sourcing Service Integrator (MSI)

## 2.0 Information Security Program Requirements

### 2.1 Information Security Program

Atos Cyber Security Services achieve compliance and sustain secure and uninterrupted business operations, with particular emphasis on managing end-to-end protection across the extended enterprise. Atos will maintain an Information Security Program that will provide programmatic oversight for on-going activities that across VITA. Information Security Program activities include, but are not limited to:

- ▶ Developing and maintaining the Information Security Plan (ISP)
- ▶ Maintaining a set of comprehensive security policies and procedures aligned with the Service Management Manual (SMM)
- ▶ Security performance monitoring and periodic security assessments and testing
- ▶ Ensure adherence to the Information Security Plan that will comply with the security requirements of VITA and Customers systems
- ▶ Participating in security meetings with VITA, VITA customers, and the MSI

## 2.2 Information Security Practices and Processes

Atos' information security practices and processes will support Commonwealth business needs, security, technical requirements, and end-user requirements. Security requirements will be communicated in detail to VITA, its agencies, end users (including agency departments and groups), and to other suppliers when appropriate in accordance with the SMM. Atos will also participate in technical and business planning sessions to establish security standards, establish architecture and identify initiatives. Atos will develop and document technical design plans and environment configuration based on VITA and Commonwealth security requirements. Information security practices and processes will comply with VITA and Commonwealth policies, VITA Rules, standards and regulations for information, Systems, personnel, physical and technical security while also adapting to future changes in laws, regulations and policies.

Atos will deploy security processes to enable the effective monitoring and reporting of the services in the Customer Environment through the deployment of the relevant tools and procedures, and where such security processes do not exist, designing processes that are in compliance with security requirements. The solution provides for the timely creation, updating, maintenance and provision of all appropriate project plans, project time and cost estimates, technical specifications, management documentation and management reporting in open industry standard portable format, for all projects and service activities. Service delivery deployments will be coordinated with other Suppliers as well as other support groups with Customers, VITA, and all appropriate third parties. Atos will provide flexibility to the Commonwealth to provide for VITA-identified immediate support services.

The solution will identify security risks and vulnerabilities and recommend improvement opportunities for reducing the impact of such risks and vulnerabilities as they are identified. Atos will also assist in fraud prevention, detection and reporting in accordance with the SMM. Relevant parties will be notified of risks as outlined in the SMM. Atos' security improvement recommendations will be provided in via a monthly report based on identified vulnerabilities and the outcome of risk assessments. Atos continuously monitors security trends through independent research; and will document and report on products and services with potential use for the Commonwealth. Atos will provide infrastructure, security planning and analysis, installation and upgrade recommendations. As part of the normal continuous improvement for all processes, Atos will perform in feasibility studies and evaluations when applicable for the implementation of new security technologies that meet Commonwealth business needs and meet cost, performance and quality objectives. Atos will implement these recommendations after they are approved by the agency or VITA where appropriate.

Atos will also conduct technical reviews and provide recommendations for improvements to the infrastructure that increase efficiency and effectiveness of security and reduce costs in accordance with planning and analysis policies and procedures as required by the SMM. Application security reviews will also be conducted to recommend potential improvements to application security architecture and to infrastructure service architecture in compliance with infrastructure requirements in accordance with the SMM.



New and upgraded service components and services will be evaluated for compliance with VITA and Commonwealth security policies, regulations and procedures. Security testing for Networks, Software and Services including unit, System, vulnerability, integration, as well as regression testing will be completed on all new, changed, and/or upgraded equipment. Any recommended changes to VITA's security requirements will be done to incorporate industry best practices, infrastructure roadmap changes, and the documented the evolution of such changes and practices will be provided in a quarterly report.

### **2.2.1 Security Awareness and Training**

Atos will work with VITA and VITA agencies to develop an enterprise security awareness training program for VITA, VITA Agencies, and Supplier. This program will promote security awareness through a role-based training program that includes creation and delivery, measure and report on such program's effectiveness. This campaign will include Customer privacy and security topics and standards as well as a simulated social engineering attack. The Atos Security SDM will engage in an Agency-outreach effort that involves Agency Information Security Officers (ISO) participation - Security Awareness Training for VITA included as part of that outreach effort. In accordance with the SMM the ISSO and Agency ISO's will implement and maintain processes and procedures, and provide communications, that are intended to increase security and privacy awareness, including:

- ▶ Urgent communications on high-risk threats
- ▶ Communications regarding changes to security requirements
- ▶ Routine communications on general awareness topics

In addition to this outreach, Atos will obtain and review industry-recognized information sources regarding security, provide this information to the Customer, and, on a quarterly basis, recommend security risk reduction actions and opportunities based on review of such information in the form of a report. Atos is an active participant in industry standard security forums and End-User groups to remain up to date with current security trends, threats, common exploits and security policies and procedures. Security awareness will be a continuous process updated regularly in accordance with the SMM.

### **2.2.2 Governance, Risk and Compliance Tracking**

Atos will be responsible for conducting internal operational security reviews, to assess operational processes and performance to determine compliance with Customer security requirements on an annual basis. The annual reviews also ensure customer and VITA security requirements are met along with continuous efforts for process and control improvement is enabled. The annual security reviews will also provide a mechanism to present recommendations for improving security requirements and processes with the goal of improving operational efficiencies, deliver annual customer reporting for security review and gain VITA approval for corrective action plans within 5 days following VITA receipt of a security review report. The standard approach is for Atos to remediate any process that is not in compliance within 30 days or less following approval.

The Atos Governance, Risk, and Compliance (GRC) process provides a framework for the leadership, organization, and operation of VITA's IT and security areas to ensure that those areas support and enable VITA's strategic objectives. The integration with the source data will also allow tracking and reporting on the status of all systems with exceptions requested, needed, or identified as specified in the SMM. This tool provides the capability that accepts data imports and management of a central repository for security policy, governance processes, management reporting and task management. Atos will collect, analyze, rate and report on the security compliance status of VITA services and applications. Atos will also develop a repository of projects and other initiatives and their associated security risks and compliance issues and gather requirements and document the use cases for all new functions. Policy exceptions will be managed based on the policy requirements and exception information from the governance risk and compliance tool(s).



The GRC Tool will use the security impact level, operational criticality, assessment data and vulnerabilities in a risk management framework to track all controls, policy exceptions, risks identified, exception expirations, and all remediation activities for regular reporting, alerting and dashboard presentation. The initial assessment information will be provided to the Customer for the determination of the data risk rating for the vendor supplied service being assessed. The GRC tool will enable data exports in appropriate formats to users with approved security access and data feeds to approved tools. Atos will educate and train Supplier Personnel on the proper use of the governance, risk and compliance tool(s). Atos will adhere to VITA’s process and procedures including configuration and role-based requirements. The governance, risk and compliance tool(s) will provide support the integration process (which is led by the MSI) with the asset compliance data repository or application (i.e., MSI provided asset management system). This will enable a two-way data exchange that is required with the asset compliance system. Atos will create data exports of security compliance information as required to feed data to other security Applications. Atos will also develop an automated and secure file transport process for the data extracted from the governance, risk and compliance Tool.

New GRC use cases, reporting, alerting and dashboards can also be added as needed based on the emerging needs that are identified in the future. Atos will assist with design, development and implementation of the use case in the governance, risk and compliance Tool(s) including the integration with other source systems as needed to automate the use case. Atos will also assist with the implementation of the required workflow, notifications, dashboards and reporting as defined by the use case specification.

2.3 Service Integration

To meet VITA’s requirements for service management, Atos will integrate our global ITIL-based governance and delivery framework, commonly referred to as the Atos Service Management Methodology (ASMM). Atos’s ASMM methodology aligns with Commonwealth’s vision of separation of duties, meaning that Atos will seamlessly integrate into the MSI’s IT Service Management (ITSM) systems, processes, and tooling. (e.g. Password Vaults, Multi-Factor Authentication (MFA) systems, Identity and Access Management (IAM), etc.).

All service management activities performed across VITA will be:

- ▶ Documented and communicated in accordance with the SMM
- ▶ Flexible in their approach which will allow the ability to evolve with VITA & Agencies
- ▶ Executed utilizing best practices leveraged in accordance with the SMM

The Information Systems Security Officer (ISSO) and Customer Relationship Manager (CRM) work directly as Governance Body Representatives with the VITA, Agencies, the MSI, and third-party vendors to define, document, and maintain the process flows, integration points, and procedures in the SMM. The ISSO and CRM will work with the appropriate stakeholders to ensure that VITA’s IT Governance Risk and Compliance (IT GRC) tool is up to date, providing an Agency-level view of key metrics and reports that create a culture of “Risk-Informed” Agency with “Risk-Informed” employees. Table 1 provides sample of ITIL-centric processes that will be included in the SMM.

Table 1 – Governance Leadership Body Roles

Processes	Governance Leadership Body - Representative Team
Incident Management	Responsible for managing lifecycle of all incidents. The Governance Leadership Body team will work with the MSI, VITA & Agencies, third-party vendors, and is focused on driving value to Agency business needs. The Governance Leadership Team (GLT) will interact with Cross-Functional (CF) teams to Agencies are delivered security

	services that are delivered efficiently, effectively, focusing on Continual Service Improvement (CSI) initiative to identify trends, adjust processes, and fine tune technologies to continuously identify and improve security services.
<b>Major Incident Management</b>	Work with the MSI and STS to manage Major Incidents effectively and efficiently, ensuring appropriate communication and swift resolution.
<b>Change Management</b>	<p>Manage IT changes and deliverables while managing risk. The Governance Team will integrate into VITA's Change Advisory Board (CAB), including working with the MSI to accomplish the following:</p> <ul style="list-style-type: none"> <li>▶ Provide objective, risk-based recommendations to the CAB on changes</li> <li>▶ Participate in Independent Verification &amp; Validation (IV&amp;V) activities across the Change Management lifecycle. (e.g. post-change scanning)</li> <li>▶ Review the implementation</li> <li>▶ Participate in the CAB meetings</li> </ul>
<b>Problem Management</b>	Responsible for managing the lifecycle of all problems. The entire operations team will identify needed corrective actions; create and manage action plans to resolve known errors; update the knowledge database; provide quality assurance (root cause analysis, actions identified and closed); and provide proactive problem analysis to identify trends

### 2.3.1 Systems and Tools

The following security tools are included in the Atos solution.

**Table 2: Systems and Tools**

Manufacturer	Product	Description
		Managed Firewall Services
		Server Managed Host Intrusion Prevention Active Response, File Integrity Management, Management of Native Firewall, Management of Host-Based Anti-Malware (legacy Unix servers)
		Managed Detection and Response, Security Monitoring, Log Management, & Analysis (i.e., Security Information and Event Management - SIEM) and dashboarding
		Anti-malware for legacy Unix servers
		Next Generation AV, Endpoint Detection and Response, Integrated Threat Intelligence, File, Application and Device Integrity
		USB Device Control
		Host Firewall Management (for Windows, Linux and MacOS endpoints)
		Threat Intelligence Feeds
		Compliance Testing, Network Access Control (NAC)



Manufacturer	Product	Description
		Digital Forensic Investigation
		Managed Firewall Services
		Centralized security management platform for Windows Native Encryption and legacy components such as Trellix Web Gateway.
		Application Process Whitelisting
		Data Loss Prevention
		File Level Encryption
		Management of Native Encryption
		Proxy and Web Content Monitoring
		Cloud Access Security Broker (CASB)
		Native MS encryption
		Management of Native Encryption
		Managed Network Intrusion Protection
		Managed Firewall Services,
		Basic Proxy
		Secure Remote Access (user and network)
		Full packet capture
		Vulnerability Scanning
		Certificate/Key Management
		Web Application Firewall
		Certificate/Key Management
		Source Code Scanning & Analysis

Access to security tools will be granted based on the principle of least privilege, enabling the appropriate access to the system. Atos will provide for granting additional access in support of other designated Third Parties (e.g. auditing organizations) upon request in compliance with the SMM. Solution will provide access to security tools to Customers, business units of Customers, and authorized Third Party Vendors, and any other parties identified in the SMM. This access will include all appropriate and required licenses and interfaces.

Solution will present in the program-wide dashboard, monthly reports on the status of and maintenance activities for the security tools. Atos will educate and train Supplier and designated personnel in current information security trends and the use of security tools used in the environment or anticipated to be used in the environment. Atos will support activities to verify security tool contents and correctness of the information contained therein by VITA, Customers, and other designated Third Parties (e.g. auditing organizations) in compliance with the SMM. Atos will recommend new security Tools to be included as part of the Services (including any Equipment, Software products, and infrastructure services) as appropriate.

### 2.3.2 Supplier Security Tools

Atos will primarily be using a variety of security tools. Specific tools are listed above in Table 2 – Systems and Tools. Atos will maintain the technical and functional specifications and requirements for the Supplier-provided security Tools and any related interfaces. Atos will ensure security tools and any related data have clear separation from all other customers of Supplier and the customers of Supplier's subcontractors or other vendors. Customer information will be partitioned in management and reporting, such that Customers cannot inappropriately access

the information of another Customer. Atos will maintain separation of duties between administrator and security personnel.

Atos will supply monitoring and reporting interfaces for the security tools dedicated to customer and customer-identified entities with respect the applicable SMM processes and procedures. Atos will provide a mechanism for centrally collecting security data that remains independent from Supplier services. All tools will integrate into the existing authentication services.

Atos will deploy, install, implement, configure, maintain and administer VITA/Customer-approved security Tools, including security Tools that support ITIL-based processes, and those tools identified in the SMM and accordance with VITA Rules. Subject to the Customer's prior written approval, leverage new security Tools that would improve Customer's business processes. The data associated with the inherent capabilities of the toolsets will be made available for integration with elements of the MSI ITSM.

### **2.3.3 Patch Management**

The Atos Patch Management solution (for Atos owned and operated devices) administers software updates for desktops, laptops, and servers. Patches for third party and custom applications for Windows and Mac Platforms can be managed and deployed. Using this solution, Network Administrators can see what software is installed on each machine and what security patches need to be installed to maintain the best possible security. Atos will initiate a patch management piloting process and report on the results to the impacted Customers and VITA. Any device under supplier control used to provide services will be maintained at appropriate patch levels. As part of this solution, Wake-on-LAN can be used to wake up sleeping machines and deploy patches at optimum network times. All security updates are automatically updated when updates become available.

The features for this solution include the following:

- ▶ Enterprise Scalability - Delivery of patches to large organizations, also meets requirements of small-to-mid-sized organizations, enterprise-wide monitoring and maintenance of patch compliance
- ▶ Reports on the status of patching every 30 days and upon request.
- ▶ Communication with and/or alert the Customer IT Security team when patches are not installed within the designated timeframe.
- ▶ Agent-based patch management ensures complete security coverage for desktops, also protects remote users on laptops and workstations.
- ▶ Patches to devices will be applied within the timeframe guidelines in accordance with Customer's security policies and the SMM
- ▶ Always applies patches in proper sequential order to specific computers, groups, or entire enterprise
- ▶ Compliant with corporate and government regulations and policies
- ▶ 100 percent accurate helping pass security audits
- ▶ Scans and reports all software applications on Windows and Mac platforms
- ▶ All policy approved software updates automatically when patches become available
- ▶ Ability to schedule patches to individuals, groups, or site machines
- ▶ Weekly analysis of security patches impacting the environment including advisory actions and recommended patch time frames.
- ▶ Allows the administrator to control the scanning and patch distribution schedule to minimize any end-user disruptions
- ▶ Granular reports on what patches are available, current patch status, and what computers have what patches, and which do not
- ▶ Automated for maximum efficiency – saving administration time, effort, and reducing costs



- ▶ Third party and custom patches (Including Adobe) for software applications on Windows and Mac platforms
- ▶ No disruption to the end user – Patching can be scheduled in hours when the users are not on the system
- ▶ If the patch process disrupts Customer operations the Supplier will roll back the changes made.
- ▶ Distributed patch repositories available for local use rather than managing centralized patching over many locations

#### 2.3.4 Reporting

Atos will leverage VITA's GRC (Please reference section 2.2.2 above) to capture key data points from the provisioned Cyber Security tooling and processes for data correlation. Overall, the GRC tool will provide custom use case benefits in many ways such as the ability to schedule tasks, manage interface execution and maintenance tasks and the ability to automate processes and reporting. The GRC tool provides periodic (weekly, monthly, quarterly, and yearly) and on-demand enterprise reporting. Benefits of the GRC include the on-demand and online, drill-down dashboards available based on data in the GRC for each process use case implemented.

The GRC tool scales to enterprise level reporting spanning all of Governance, Risk and Compliance (GRC) systems and processes. Key areas include:

- ▶ Risk Assessments and audits
- ▶ Legal and regulatory compliance tracking
- ▶ Integrated security service (e.g. vulnerability scan results)

The Atos Prescriptive Security offering supports multi-tenancy with delegation of roles to local and/or global users. Data can be provided via the dashboard and access to local logs; in conjunction with analytical tools, a variety of out-of-the-box and customized reports are available. All reporting information will be retained online for 90 days, archived for 1 year, and available as a 3-year trend.

#### 2.3.5 Security Dashboard

Atos Digital Security Services maintain continuous visibility and transparency on their customer implemented IT security measures to manage potential IT risks and to react on identified business threats in a timely fashion. Through the Enterprise Governance, Risk and Compliance tool (GRC), Atos has a continuous view pertinent to:

- ▶ Security Monitors
- ▶ Security Reports
- ▶ Security Information Feeds

Solution will provide monthly, quarterly, and annual reporting in the Security Dashboard on the deployment of Tools and procedures to the Customer Environment. Customers will also have the ability to run and export ad hoc reports.

Security data and alerts will be made available through dashboards and reports in accordance with SMM. Where identified, the solution will integrate with the program dashboard. Security information will include the most recent security advisory list for the software, equipment, systems, and infrastructure in use, the compliance requirements for patching status, security baseline requirements, and any other compliance requirements identified in the SMM. Criteria inherent in the solution toolset will be made available to the MSI ITSM.

Customer user access to all security information, incident information and threat data will be made available either through the MSI ITSM or directly from the solution toolset in accordance with the SMM. Training will be provided for the dashboard to Suppliers, Customers, and designated users.

Information will be maintained online for a period of 90 days online with 1-years' worth available in near time. Three (3) years' worth of trend data for the security dashboard will also be maintained.

## 3.0 Security Requirements

### 3.1 Threat Management

#### 3.1.1 Digital Forensics Investigation

VITA and its customers will have enhanced support for investigating security events through Atos' digital forensics support. When the VITA or one of its customers makes a request, Atos will provide digital forensics based on VITA or customer security policies, applying investigation, examination, reporting, and coordinating services as needed with the VITA or customers'

VITA and its customers will have support based on the following general principles relating to the handling of digital evidence for forensic analysis:

- ▶ Application of the general rules of evidence to all digital evidence, regardless of when or where it is located, including environments for cloud, data center, offices, wearable, or non-network.
- ▶ Upon sequestering digital evidence, actions will not change the evidence and will follow the rules of evidence handling.
- ▶ When an authorized person from Atos, VITA, or its customers' needs to access the original digital evidence, that person will be suitably trained for the purpose, regardless of location of service or tools being used.
- ▶ All activity relating to seizure, access, storage, or transfer of digital evidence will be fully documented, preserved, and available for review.
- ▶ A clear chain of evidence will be documented for all actions taken with respect to digital evidence.

##### 3.1.1.1 Processes & Methodologies

Whether it is evidence on the host computer or on the network, a digital forensics toolkit automates routine tasks and more. Atos uses a combination of COTS and open-source forensics tools to create a holistic forensic investigative toolkit. This toolkit enables the collection and preservation of digital evidence.

In consideration of the VITA and customer security policies, Atos has developed our security processes and methodologies based on the following National Institute of Standards and Technology guidelines and regulatory information:

- ▶ National Institute of Standards and Technology Special Publication 800-86, *Guide to Integrating Forensic Forensics Techniques into Incident Response*
- ▶ National Institute of Standards and Technology Special Publication 800-61, *Computer Security Incident Handling Guide*
- ▶ Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*

Atos will engage subject-matter experts to provide appropriate responses to security incidents such as computer intrusion, service disruption, security compromise, inadvertent data disclosure, or other matters of breach.

Atos will provide the following practices applicable to digital evidence examinations:

- ▶ Preparation of evidence

- ▶ Anti-Contamination Precautions—Minimizes any chance of accidental contamination of items, which may subsequently be required for other laboratory examinations, e.g. fingerprints, DNA.
- ▶ Searching the Scene—Systematic and thorough search for digital evidence and related material, targeting and prioritizing areas, which in the context of what has been alleged are most likely to contain material of evidential significance.
- ▶ Collecting the Evidence—Preserves items for forensic examination securely as soon as possible following appropriate jurisdictional practices.
- ▶ Packaging, Labelling and Documentation—Makes a record at the time of seizure of items from the scene, or from the suspect(s) or victim(s), describing the exact locations from where the items were recovered. Properly packages and seals evidence. Packages are labelled at the time of seizure.
- ▶ Analysis Protocols—Procedures for analysis of digital evidence including:
  - Performing keyword searches, filter and bookmark important evidence discovered.
  - Rebuilding webpages and display webpages in their original format as they were seen by the user.
  - Identifying and report geo-location data indicating physical locations.
- ▶ Salvage Data – As applicable, Atos will attempt to salvage deleted or otherwise unrecoverable data from a variety of media and data types including server and Workstation hard disks, backup media, optical media, email information stores, smartphones, tablet computers, and .pst files.
- ▶ Case Records—the exact requirements for recording casework information will be based on the VITA or VITA customer security policy. Records will be in sufficient detail to allow another examiner to be able to identify what has been done and to assess the findings independently. Case records will include administrative and examination documentation.
- ▶ Presentation of Findings—Report of relevant information in a clear, concise, structured and unambiguous manner.
- ▶ Case File Review— Reviews for technical and administrative accuracy.
- ▶ Technical Review— considers the validity of all the critical examination findings and the raw data used in preparation of the statement/report. It considers whether the conclusions drawn are justified by the work done and the information available.
- ▶ Administrative Review—Ensures the requester’s needs have been properly addressed, editorial correctness, and adherence to policies.
- ▶ Expert Testimony—Computer forensic evidence is just like any other evidence in the sense that it must be authentic, accurate, complete, convincing to juries, and in conformity with common law and legislative rules (admissible).

Atos will work with VITA, VITA customers, and the MSI to provide digital forensics support for the following types of security incidents:

- |                           |  |
|---------------------------|--|
| ▶ Security breaches       | ▶ Privileged account compromise  |
| ▶ Litigation support      | ▶ Unprivileged account compromise  |
| ▶ Acts of terrorism       | ▶ Application compromise   |
| ▶ E-discovery             | ▶ Availability: DoS/DDoS   |
| ▶ Criminal investigations | ▶ Sabotage   |
| ▶ Data spills             | ▶ Information security: Unauthorized access or modification to information |
| ▶ Information gathering   | ▶ Fraud: Unauthorized use of resources                                     |
| ▶ Intrusion attempts      | ▶ Masquerade   |
| ▶ Intrusions              |  |

### 3.1.1.2 eDiscovery



Atos recommends that VITA maintain its EnCase License as part of this eDiscovery solution. Atos has EnCase-certified personnel who can produce forensically sound, court-admissible, incident documentation and reports. EnCase has the capability to provide evidence that meets litigation integrity standards from a wide variety of devices. Atos will work with any other related third parties within the scope of their contracts with VITA, as required by the eDiscovery request.

### 3.1.1.3 Third-Party Providers

When Atos encounters an incident that requires investigation into any technology provided or managed by a third party, Atos will first consult with VITA to establish any contractual obligations or restrictions that may apply. Once there is an understanding, Atos will work with VITA and the third party to determine the best possible course of action for any issue that arises.

### 3.1.2 Managed Detection and Response (MDR)

Today's rapidly evolving threat environment requires the ability to detect complex, targeted, or unknown attacks. In response, we have evolved beyond SIEM, and built a truly comprehensive Managed Detection and Response (MDR) service powered by our next-generation Artificial Intelligence (AI) platform, [REDACTED].

The [REDACTED] platform is a cloud-native solution with hybrid and multi-cloud support. [REDACTED] combines our award-winning artificial intelligence for cybersecurity, proven high-performance computing, and innovations in edge AI. [REDACTED] collects and aggregates data and events from security devices, network infrastructures, systems, and applications, then applies intelligence to that data to provide actionable information. Tools will be customized by leveraging the configuration capabilities to meet VITA's requirements as per the SMM. Services which require monitoring include:

- ▶ Host based intrusion detection/prevention systems
- ▶ Network intrusion detection/prevention systems
- ▶ Firewalls
- ▶ Network access control
- ▶ Workstations (e.g., operating system security logs, firewalls and security agents)
- ▶ Network devices such as routers, managed switches, traffic management switches, application layer switches, and wireless access points
- ▶ Servers (e.g., operating system security logs, firewalls and security agents)
- ▶ Access control, authorization services such as proxies, reverse proxies, TACACS, Microsoft Active Directory, LDAP, multi-factor authentication systems and single-sign-on systems
- ▶ Applications
- ▶ Any other sources or services specified in the SMM

The solution will develop and maintain of an inventory of systems and applications with alerts being collected and analyzed. The inventory includes: Application names, service names, versions, service descriptions, data collection method, and data collection component as well as event description documentation. This inventory information is available electronically to VITA and Customer personnel as identified by the SMM.

[REDACTED] produces the following types of content:

- ▶ Customizable real-time rules based on complex logic.
- ▶ Customizable, scheduled and ad-hoc reporting based on complex queries with complex logic.
- ▶ Customizable page and content layout.

- ▶ Trending data based on source log values. Trending will be used in both reporting and proactive anomaly detection and alerting.
- ▶ Data values that result from custom real-time rules used for future reporting or secondary rules.
- ▶ Filter logic will be applied to existing rules, reports, and event feeds sent to the SIEM for capacity management.

All [REDACTED] components communicate via an AES encrypted channel to protect operationally sensitive data in motion. The Atos MDR solution provides:

- ▶ Atos in conjunction with VITA and participating Executive Branch Agency customers will determine the content and frequency of report generation. These submitted reports will provide the following information:
  - Summarize event counts per month, week, day, or other time period required.
  - Summarize real time rule alerts from past 30 days including the top 10 alerts generated.
  - Provide ad-hoc reporting requested by VITA's customer.
- ▶ Atos will conduct performance assessment and tuning exercises.
- ▶ Atos security teams will provide content development, custom content tuning, real time alarming, escalations to VITA and the customer and proactive content development in response to public and private threats.
- ▶ Atos will have the necessary equipment in place to allow security monitoring (SOC), network monitoring (NOC), and endpoint device and software-as-a-service monitoring.
- ▶ Atos will establish a process to monitor all security tools. System health alarms will enable various teams to respond effectively and timely.
- ▶ Within MDR, Atos will provide mechanisms to customize and trigger alerts as understanding of the threat horizon evolves.
- ▶ Atos will provide VITA and participating Executive Branch Agency customers with access to a central dashboard for the purposes of reporting on requested content.
- ▶ Atos will provide agency ISOs and AITRs with read only access to real time and historical event feeds, rule logic, report components, filters, data lists, variables, queries for validation and investigation.
- ▶ Atos will provide mechanisms so that any real-time alarms, reports and email notifications may be directed at more than one user. Designated recipients may be individual agents or a larger distribution list.
- ▶ Atos will also provide up to five authorized users, per agency, with the ability to develop and apply complex read only query logic to real time and historical data.
- ▶ Atos will provide classroom training to CSRM analysts on how to interact with [REDACTED] once installation is complete and after any upgrades or changes.
- ▶ As required and/or for auditing purposes, Atos will provide authorized personnel with inventory information.
- ▶ In conjunction with VITA and participating Executive Branch Agency customers, Atos will provide necessary resources to participate and support in incident response processes to resolve security incidents.
- ▶ Semi-annually or as specified in the SMM, Atos will perform a capacity analysis for all components that use any infrastructure resources (i.e., WAN bandwidth, storage, process, etc.), for the purpose of business impact mitigation.
- ▶ The ability to detect changes to audit records created by the solution (i.e., data hashing).
- ▶ Classification and prioritization of collected data for the purpose of applying access control and retention policies and the ability to apply retention policies by data type and source.
- ▶ Role-based data access control; restrict data view by role.



- ▶ Mechanisms for filtering rules and report creation including obtaining approvals for all filters implemented and documenting the justification for all filters implemented for rules and reports related to security content.
- ▶ An operational report to summarize and provide data as specified in the SMM or on demand from VITA.
- ▶ In-scope server and infrastructure device logs will be consumed by [REDACTED].
- ▶ Ability to export events into common file formats such as XML, CSV, etc.
- ▶ Maintenance of a repository of collected logs accessible by Customers for consumption or review in line with the SMM.
- ▶ Participation in the Security Incident response processes to provide necessary resources to support resolving Security Incidents.

### 3.1.2.1 Log Event Collector (LEC)

The Log Event Collector (LEC) enables the collection of security events and network flow data from multi-vendor sources including firewalls, virtual private networks (VPNs), routers, IPS/IDS, NetFlow, sFlow, and others. The LEC allows for the collection of this data and normalizes it into a single manageable solution. This provides a single view across devices from multiple vendors and allows event and flow data collection from Network Intrusion Protection System (NIPS) devices and routers that send data feeds to the LEC. This solution provides for aggregation on logs and event collectors for event storage de-duplication. High Availability LECs (LEC-HA) can be used in primary and secondary mode, acting as backups for each other. The secondary LEC (B) monitors the primary LEC (A) continuously and new configuration or policy information is sent to both devices. When LEC B determines that LEC A failed, it disconnects LEC A's data source NIC from the network and takes over as the new primary. It remains as the primary until the administrator intervenes manually to restore LEC A as primary. The LEC is configured to forward a backup of the raw data to a storage device for long-term storage.

A correlation data source analyzes data from a log source, detects suspicious patterns within the data flow, generates correlation alerts that represent these patterns, and inserts these alerts into the LEC's alert database. A suspicious pattern is represented by data interpreted by correlation policy rules, which can be created and modified. These types of rules are separate and distinct from NIPS or firewall rules and have attributes that specify their behavior. Only one correlation data source can be configured on a LEC, in a similar fashion to configuring syslog or OPSEC. After the LEC's correlation data source is configured, the user can roll out the correlation's default policy, edit the base rules in this correlation's default policy, or add custom rules and components and then roll out the policy.

[REDACTED] supports the storing, managing, accessing, and reporting of log data. The data received by [REDACTED] is organized in storage pools. A retention time is associated with each storage pool and the data is retained in the pool for the period specified. Search and integrity-check jobs can be configured. Each of these jobs accesses the stored logs and retrieves or checks the data that is defined in the job. The administrator can then view the results and export the information. Storage is cloud-based, high-availability and resilient.

[REDACTED] checks file integrity to verify if the defined files have been altered since they were originally stored. This will alert the administrator of unauthorized modification of critical system or content files. The results of this check show which files were altered. If none of the files were altered, one will be notified that the check was successful.

[REDACTED] mines collected event data three ways. [REDACTED]

- Hunts for attack campaigns and hidden threats with 100+ machine learning models and 500+ use case scenarios across industries

- Anticipates attacks by correlating over 200+ threat intel sources for impact on Commonwealth assets and proactively raise defenses
- Monitors for known threats with over 1000+ rules and signatures and detect threats in real-time.

### 3.1.3 Security Incident Response

Atos has considered VITA's environment and selected a customized set of processes, tools, and components to meet VITA's security incident response needs. These tools will allow Atos to respond to any event quickly to address the problem, employ the correct solutions, and strengthen the environment against future incidents. Atos will provide a dedicated investigative group, who will serve as a security incident response point of contact. The group will respond to any security incident related requests including a phone 'hotline' and will contribute to the delivery of emergency Incident response services.

Atos will conduct security incident response and investigation activities in coordination with other suppliers in accordance with best practices, VITA rules and the SMM. Each incident will be classified based on established procedure or as classified by VITA. As part of the Atos response there will be a secure collection, capture, and retention of any data or hardware deemed necessary to assist with Security Incident response using forensically appropriate process, including logs, disk drives, files, servers, work stations, and other items which may be of evidentiary value. Atos will not serve any notice or otherwise publicize a Security Incident without the prior written consent of VITA. Atos will provide and execute an enforceable chain of custody process for all Security Incidents, such that evidence integrity is maintained for any items (physical or logical) relating to the incident response investigation. Atos will attempt to identify the initial point of entry into the system, the source of the intrusion, the tools and methods employed by the intruders, and any data compromised, as well as a list of all other systems, Applications, or third-parties potentially compromised.

Atos' response will, in coordination with the other suppliers, MSI, equipment owner as necessary in accordance with SMM collect of any data or hardware deemed necessary by VITA and Customers to assist with the Security Incident response, including logs, disk drives, files, servers, work stations, and other items which may be of evidentiary value. Coordination investigation activities in conjunction with VITA and Customer will be embedded in Atos' processes to maintain the data integrity of any asset which may be needed for evidence. Atos will train and designate the security leads within Supplier and Service Tower Providers that will have ownership and responsibility for handling Security Incidents. Atos will maintain evidence integrity and strict chain of custody procedures for any items (physical or logical) relating to the Security Incident response investigation.

In accordance with SMM processes Atos will:

- ▶ Refer requests for information regarding incidents to VITA/participating Executive Branch Agency customer and do not provide information about the incidents to outside sources.
- ▶ Record timelines, actions, and events in accordance with VITA Rules and the Incident Management System instructions in the event of a Security Incident.
- ▶ Follow the escalation notification processes in accordance with security requirements and VITA Rules when Supplier identifies or is made aware of a security violation, Security Incident, or potential Security Incident.
- ▶ Invoke and execute the IS-IMP, in cooperation with Customers whenever an Incident threatens the security and safety of VITA, Customer's and Supplier's environment, or a significant sector of the Customers.
- ▶ Work with VITA and Customers in the restoration of the Customer environment in accordance with VITA Rules.
- ▶ Document the policies that govern the response to Security Incidents.



- ▶ Document and implement the specific processes and tools for managing and responding to Security Incidents in cooperation with VITA and Customers.
- ▶ Lead in the investigation of Security Incidents and report findings to VITA and VITA identified parties.
- ▶ Lead in the creation of a remediation plan that is acceptable to VITA and Customers.
- ▶ Conduct a forensic investigation to determine what Systems, data and information have been affected by the Security Incident.
- ▶ Facilitate the identification of the initial point of entry into the environment, or other source of the Security Incident; including the tools and methods employed by the intruders, any data compromised, as well as a list of all other systems, Applications, or Third Parties potentially compromised.

Atos will provide reports in the portal dashboard of all Security Incident response details and activities. A summary of all Security Incidents related to the Services and VITA Data to VITA, will be provided upon the request of VITA, for all Security Incidents since Commencement. Records of all Security Incidents related to the Services and VITA Data will be maintained and provided to VITA using a real-time function. As aligned with Exhibit 3.0, Supplier will not close an Incident until VITA/Agency is satisfied with all aspects of the investigation and all required data is provided.

Atos has developed our security processes and methodologies based on the following National Institute of Standards and Technology standards and regulatory information:

- ▶ NIST Special Publication (SP) 800-61, *Computer Security Incident Handling Guide*
- ▶ NIST Special Publication (SP) 800-86, *Guide to Integrating Forensic Techniques*
- ▶ NIST Special Publication (SP) 800-84, *Guide to Test, Training, and Exercise Programs*

Atos's Information Systems Security Officer (ISSO) will engage Agencies to determine:

- ▶ Computer security incident severity levels
- ▶ VITA and participating Executive Branch Agency customers will also receive an approved security response test plan designed to validate the proposed responses of the security response plan.
- ▶ The approved security response test plan will contribute to and be part of the annual security response test plan exercise schedule.
- ▶ The test plan issued to VITA and participating Executive Branch Agency customers will contain the approved test objectives and success criteria designed to verify that the IT organization, security organization, other service providers, and third-party vendors can respond effectively to system security incidents.
- ▶ Coordination with all required IT technical and services operational teams (including computer systems, networks, applications, data repositories, telecommunications, environment, technical support, and service desk) for test execution.
- ▶ Using our standard methods, Atos will facilitate the security response test plan exercise, capture all results, and prepare a written report for the approval of the VITA and its customer.
- ▶ Within 30 days of the exercise, the written test plan report shall contain the following information:
  - The objective of the test
  - The results achieved
  - A comparison of the results to the measures and goals identified in the security response plan
  - A plan and a schedule to remediate any incident response issues identified during testing
  - Continuous tracking and ad hoc reporting

### 3.1.4 Rapid Malware Response

The Rapid Malware Response solution, primarily based on the [REDACTED] provides:

- ▶ [REDACTED] (next generation malware detection
- ▶ [REDACTED] Endpoint detection and response (EDR)
- ▶ [REDACTED] managed endpoint threat intelligence
- ▶ [REDACTED] (USB device control
- ▶ [REDACTED] (host-based firewall

The Atos solution to Rapid Malware Response provides the following:

- ▶ The technical expertise, leadership and oversight to manage and resolve security incidents such as malware outbreaks
- ▶ Identification, cleaning, and prevention malicious binaries from executing within the environment.
- ▶ Identification of malicious and suspicious URLs to designated personnel to categorize URLs as malicious.
- ▶ Containment of malware compromises to prevent further spread.
- ▶ Reaction and rate events related to systems or users with access to sensitive data, based on the sensitivity of the data or device.
- ▶ Continuously scan for malware.
- ▶ The capability to reverse engineer malware to provide a detailed analysis of attack vectors using sandbox technology.

### 3.1.5 Major Security Incident Response

VITA will have high-priority, heightened readiness-level access to Atos' highly skilled Incident Response teams. Atos will provide incident management services based on requirements driven by VITA and VITA's customers. In preparation for major incidents, VITA will have the ability to work with senior level response preparedness experts to design, execute, and test Incident Response (IR) plans. Atos will document protocols for declaring Security Incidents in compliance with VITA Rules, Customer policies and state statutes.

Atos' Incident Management team will handle potential incidents and determine their severity, priority, and then apply the appropriate remediation activities in accordance to customer policies. VITA and participating Executive Branch Agencies will have support based on the following solution features and activities:

- ▶ Incident management support 24 hours per day, 7 days per week, 365 days per year, including a dedicated investigative liaison that will be accessible via hotline through the incident management lifecycle
- ▶ Coordinate an escalation process that notifies designated personnel based on the priority of the incident. This effort includes VIP level notification and law enforcement escalation if required.
- ▶ During the incident response process, coordinate the appropriate response personnel, including all required stakeholders across VITA and the MSI.
- ▶ After the incident has been contained, coordinate the appropriate response including the MSI, the Security Operations Center (SOC) team, and Security and Threat Analysis team.
- ▶ For incidents that meet certain criteria, conduct lessons learned training session with all stakeholders, potentially including other Commonwealth agencies. This effort provides very effective security awareness training.

- ▶ Upon customer request, participate in an annual incident response test plan. In addition to annual testing, also conduct tabletop testing exercises quarterly or on an ad hoc basis.
- ▶ During all phases of the incident management lifecycle, including testing, conduct a root cause analysis, leaving detailed documentation for future use.
- ▶ All Customer notifications to required entities based on the type of Security Incident will be facilitated in accordance with applicable SMM policies and procedures.

The CSIRT team can analyze potential incidents and determine their severity, priority, and what activities to undertake to mitigate the threat.

The Atos CSIRT offering consists of the following comprehensive security services components:

- ▶ Escalated Security Incident Response—Analyzes detected security incidents, initiates mitigation measures, and generates recommendations to remediate the root cause
- ▶ Threat Management—Consolidates and compares data from different data sources, provides information about known threats and vulnerabilities, and prepares lists of recommendations
- ▶ Forensic Analysis—Allows Atos to investigate and analyze suspicious activities on systems (e.g. evidences malicious activities, data loss or data manipulation)

**Third Party Incident Response Retainer** - Atos offers as part of its solution, access to an on-demand Third Party incident response service to immediately begin assessing and responding to an information security incident. If deemed necessary, Atos will provide a Third Party with an Annual Incident Response Retainer, in which customers pay an annual fee and receive service as needed. Unused retainer fees will be creditable towards other services offered by the Supplier. Also, if required, Atos will facilitate a Third Party On-demand Response Retainer, in which customers pay no annual fee and receive and pay for services on an as-needed basis.

**Response Preparedness** - Atos will test all components of the Security Response Plan in cooperation with the Customer, its designees, other Suppliers, and any other Third-Party vendors. Test execution will demonstrate, at a minimum, the validity of the Security Response Plans ability to respond to Security Incidents. All testing activities are conducted in such a manner so that active production, test, and development environments are not impacted. Notification of Customers of any anticipated risks, where a Customer may choose to exclude the impacted services or systems from a portion of the testing. Atos will evaluate the results of the test and identify potential corrective actions. Initial test results will be provided to the Customer and incorporate Customer feedback into the final test results report. Retests will occur within ninety (90) days if any test objectives are not met due to Supplier failure to coordinate and schedule between the Customer, its designees, other Suppliers, or other Third-Party vendors.

### 3.1.6 Threat Analysis and Intelligence

The Atos Threat Analysis and Intelligence solution is based upon a suite of industry leading security products that permit collection, aggregation, analysis, and reporting for systems across the entire enterprise. Tight integration between the components ensures that all warnings, alarms, and alerts are rapidly routed to the right systems for action or reporting as required.

This Threat Analysis and Intelligence solution will provide VITA and participating Executive Branch Agencies the following:

- ▶ In collaboration with the VITA MSI and their customers, identification of the value of customer information assets to attackers



- ▶ A profile of threats in the environment
- ▶ Identification potential resources, tools, and techniques that could be used to exploit the identified threats
- ▶ A catalog subset of credible threats based on potential threats, resources, tools, and techniques
- ▶ A catalog subset of high-priority threats based on credible threats, vulnerabilities, and value
- ▶ Identification of recommended mitigation measures to counter high-priority threats
- ▶ A report of the threat analysis in a format as specified in the SMM

The individual components of the Threat Analysis and Intelligence solution are:

- ▶ Atos Managed Detection and Response featuring [REDACTED] comprising:
  - SIEM: Detect known threats in real-time
  - SOAR: Investigate, contain, and orchestrate threat response
  - CSPM: Detect and remediate misconfigurations on the cloud stack
  - EDR: Uncover and contain threats on endpoint devices
  - UBA: Detect threat originating from malicious insiders
  - NTA: Identify network threats using NetFlow, rules, and threat intelligence
  - Security Analytics: Mine the entire IT and cloud stack for threats.
- ▶ [REDACTED] Enterprise, comprising:
  - [REDACTED] (threat intelligence)
  - [REDACTED] (endpoint detection and response)

### 3.1.7 Security Operations Center

Atos will maintain VITA's Security Operations Center (SOC) out of the Commonwealth of Virginia, ensuring that IT services are stable, secure, and are protected by the people who know the systems and people those systems support. In accordance with the SMM, the VITA SOC will:

- ▶ Be staffed twenty-four hours a day, seven days a week, each day of the year (24x7x365).
- ▶ Operate twenty-four hours a day, seven days a week, each day of the year (24x7x365) to receive incoming security data from multiple sources, correlate the security data, and provide real-time alerting and reporting.
- ▶ Provide emergency notification for identified security alerts, issues, or incidents.
- ▶ Generate real time security alerts, trend analyses, and reports.
- ▶ Gather intelligence by analyzing reports, interviewing Customers, and examining logs to identify Events, risk, exposure, compliance, and suspicious activity throughout the infrastructure network(s)
- ▶ Map attack vectors and sites of alerts in real-time on a topological map of the state's information technology infrastructure.
- ▶ Provide URL content analysis to identify suspicious/malicious destinations and then perform URL re-categorization and/or URL blocking as required in the infrastructure content filtering and web security solution.
- ▶ Support integration capabilities with the MSI, as well as the Service Desk.
- ▶ Provide denial of service mitigation controls and denial of service attack reporting information. This information will include network utilization and attack data.

- ▶ Provide a technical recovery team to assist with response and remediation of Security Incidents and large-scale Security Events.
- ▶ Ensure compliance of systems involved in remediation efforts.
- ▶ Close security events, to include support case closure and, where required, root cause reporting.
- ▶ Own, monitor, track, and communicate security event reports back to Customer (e.g., immediate report, root cause analysis report, monthly summary reports).
- ▶ Receive and respond to escalation calls or contact for any security-related issues.
- ▶ Receive and respond to escalation from any Supplier, Customer or Customer authorized third party help desk or support group for any security-related issues.
- ▶ Keep designated Supplier, Customer and Customer authorized third party contacts informed on status and progress.
- ▶ Act as one of the small cyber-talent incubators for the development for the Commonwealth of Virginia by turning entry level cyber employees into the next generation of cybersecurity specialists for VA.

The Atos SOC has security specific Keystone Edge process flows for incident creation, notification, escalation, and remediation. The [REDACTED] is fully integrated into the VITA Archer instance for the auto-creation of filtered, consolidated, and correlated security incidents that are routed to the appropriate Atos SOC support Tier VITA queues for immediate action by SOC analysts. Based on Customer requirements this system can be calibrated to classify alert and security event severity. The solution documents a time between receipt of verified alerts and the notification of customer personnel based on severity of the alert. Furthermore, the [REDACTED] is fully integrated with the Managed Services Incident, Problem, and Change workflows that will be integrated into the MSI's Keystone Edge solution.

### 3.1.7.1 Atos SOC Analysts

#### Tier 1 Alert Analyst:

- ▶ Continuously monitors the alert queue
- ▶ Triage security alerts
- ▶ Monitors health of security sensors and endpoints
- ▶ Collects data and context necessary to initiate Tier 2 response

#### Tier 2 Incident Responder:

- ▶ Performs deep-dive incident analysis by correlating data from various sources
- ▶ Determines if a critical system or data set has been impacted
- ▶ Advises on remediation strategies
- ▶ Provides support for new analytic methods for detecting threats

#### Tier 3 Subject Matter Expert/Hunter:

- ▶ Possesses in-depth knowledge on network, endpoint, threat intelligence, forensics, malware, and the functioning of specific applications or underlying IT infrastructure
- ▶ Acts as an incident "hunter" not waiting for escalated incidents
- ▶ Closely involved in developing, tuning, and implementing threat detection analytics
- ▶ Direct liaison to pre-sales, consulting, engineering, service lines, and CSIRT

#### Security Architect:

- ▶ Understands overall business strategy and goals



- ▶ Possesses a deep understanding of existing technologies architecture
- ▶ Conducts in-depth review of Agency's infrastructure and develops detailed plans to execute service integrations

Atos' SOC solution delivery processes ensure the confidentiality, availability, and integrity of the Commonwealth's assets, including software, hardware, and data. To resolve security incidents in accordance with incident response requirements, the SOC will work with VITA and Customer employees, contractors, consultants, and other vendors. These activities will be coordinated among experts to resolve a security event and maintain a log of actions. The SOC will coordinate and collect security operation information from Suppliers. Confidentiality of the state's operational security posture, vulnerability status, and attack status will not be compromised. Security Operations Center infrastructure communications will be encrypted between elements and components. Storage, transmission, display, and access of state data will remain, always, within the United States. SOC operations are based on industry best practices. The solution scales to support the Commonwealth environment inputs over secure channels. Secure logon and communications to SOC systems for remote management are provided.

SOC components will be supported by a centralized problem reporting and resolution system staffed twenty-four hours a day, seven days a week. Solution delivery environments will maintain sufficient technical and organizational capacity to support the needs of the state in the event of a catastrophic event that causes simultaneous severe information security incidents for many or all participating Executive Branch Agencies. SOC solution delivery model will scale to accommodate new operational locations, growth in network traffic, and increasing and changing threats.

#### SOC Vulnerability Scanning - Pre-Production (~~Application Scanning suspended on MOD 23 Effective Date~~)

The Atos solution will scan any applicable new Systems, devices, ~~or Application Software~~ (or any Systems ~~or Software~~ to be deployed in a new project). Scans will include an operating system scan, ~~a web vulnerability scanning for Web servers, and any other applicable scan types~~ identified in the SMM. This process will include a rescan of the system(s) and notify the owner of the results. No System ~~or Application~~ will be moved into production until any identified vulnerability is corrected or an exception has been granted. Atos will conduct pre-production consulting with the teams responsible for the assets in question on an ad-hoc basis.

#### 3.1.7.2 Vulnerability Scanning – Production

Atos will perform security vulnerability assessments in accordance with security requirements. Scan results and recommend remediation activities will be documented and communicated to reduce security risks. Scan results will be reviewed to identify the vulnerabilities which require remediation. Atos will coordinate with the MSI and track to completion any remediation tasks related to any vulnerabilities discovered in accordance with the SMM. Scheduled vulnerability scans will be performed as required by policy, statute or federal program guidelines and VITA Rules.

#### 3.1.7.3 Vulnerability Scanning – Application Scanning (~~Application Scanning suspended on MOD 23 Effective Date~~)

Atos will scan Applications as requested by Customer to evaluate, test and recommend security maintenance activities including upgrades, patches, and fixes. These scans will be conducted on a frequency defined by the SMM using approved tools designed for application scanning. In accordance with the SMM and in coordination with the MSI Atos will work with the Application's owner or external vendor to remediate Application scan vulnerability issues.

#### 3.1.7.4 Vulnerability Scanning – Network Scanning

Network devices will be scanned to identify any deviations from specified configurations, misconfigurations, or device vulnerabilities. Detected vulnerabilities and non-compliance issues will be reported as defined in the SMM.

#### 3.1.7.5 Vulnerability Scanning - Reporting

Updated vulnerability scan report will be provided once every calendar month. Reports will be available via a portal that allows filtering on required reporting areas. Vulnerability scan report will at a minimum include the following fields. The report will be able to sort on each field including:

- ▶ The target IP address
- ▶ The vulnerabilities discovered
- ▶ CVSS scores and the CVE and where applicable CWE of the vulnerabilities discovered
- ▶ Severity level of vulnerabilities discovered
- ▶ Description of vulnerability
- ▶ Affected software, firmware, and/or hardware
- ▶ Indication of whether the vulnerability is confirmed by the tool or is a potential vulnerability
- ▶ Vulnerability identifiers
- ▶ List of the target's open ports
- ▶ Host information such as device name, MAC address, NetBIOS name, etc.

Each vulnerability scan report will include corresponding recommendations for remediation. Atos will work with the owner of vulnerable system to advise, complete, and develop remediation plans and take any approved steps necessary to correct the issue.

#### 3.1.7.6 Penetration Testing (Third-Party)

Atos will have an independent Third-Party conducting penetration tests on an annual basis. These tests will provide:

- ▶ At least once annually external penetration testing (from outside of the Customer Environment), using a variety of tools in accordance with industry best practices to attempt to gain access to the environment. The test will attempt to gain as much access as possible (i.e. enterprise level administrator access). Testing will include all Customer and Supplier Environments.
- ▶ At least once annually internal penetration testing (from within the Customer Environment), using a variety of tools in accordance with industry best practices to attempt to gain access to the environment. The test will attempt to gain as much access as possible (i.e. enterprise level administrator access). Testing will include all Customer and Supplier Environments.
- ▶ External and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub- network added to the environment, or a web server added to the environment).
- ▶ The results and any related work product for review within 30 days of test completion.
- ▶ The rules of engagement for the independent third party are subject to approval prior to initiation of the penetration test.

- ▶ Scope of the penetration test will include a material representation of the different configurations throughout the environment and/or as requirements as described in the SMM. The scope will be approved by VITA prior to implementation of the penetration test.
- ▶ Work with the owner of vulnerable system to advise, complete, and develop remediation plans and take any approved steps necessary to correct the issue in accordance with the SMM and Supplier Towers.
- ▶ Examination the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment.
- ▶ Verification that noted exploitable vulnerabilities were corrected and testing repeated.
- ▶ Social Engineering, which includes a testing method used to extract information or gain physical access to a location through the end-user. This may include phones calls or emails to targeted individuals or attempting to bypass physical controls to access sensitive information.
- ▶ Report preparation will start with overall testing procedures, followed by an analysis of vulnerabilities and risks. The high risks and critical vulnerabilities will have priorities and then followed by the lower order. However, while documenting the final report, the following points needs to be considered:
  - Overall summary of penetration testing
  - Details of each step and the information gathered during the pen testing
  - Details of all the vulnerabilities and risks discovered
  - Details of cleaning and fixing the systems
  - Suggestions for future security

### 3.1.7.7 Compliance Management

Atos will provide a solution that will ensure systems and web application infrastructure resources always maintain compliance with security configuration requirements of VITA Rules. This solution will:

- ▶ Produce on demand and scheduled compliance reports.
- ▶ Evaluate all software devices and applications within the VITA, Customer's and Supplier's environment for compliance with configuration settings.
- ▶ Use industry regulations and standards as well as customized rule sets for evaluating whether a configuration complies.
- ▶ Provide a multi-tenant portal that will provide the compliance check results to each agency. The portal will limit the results of the compliance check to the device owning agency and to VITA.
- ▶ Identify unmanaged devices and perform pre-connect compliance check.
- ▶ Utilize [REDACTED] to assess all compliance data based on industry standard controls as mapped to Customer's security policies and external regulations. The controls will be maintained and made current at least annually.

## 3.2 Perimeter Network Security

### 3.2.1 Managed IDS/IPS

Atos will use [REDACTED] which discovers and blocks sophisticated threats in the network. [REDACTED] is firewall-native and provides multiple layers of prevention, confronting threats at each phase of an attack. In addition to traditional IPS capabilities, [REDACTED] has the unique ability to detect and block threats on all ports instead of invoking signatures based on a limited set of predefined ports.



To ensure holistic protection, [REDACTED], brings together multiple defensive mechanisms:

- ▶ Heuristic-based analysis detects anomalous packet and traffic patterns, such as port scans, host sweeps, and denial-of-service (DoS) attacks.
- ▶ Easy-to-configure, custom vulnerability signatures tailor intrusion prevention capabilities to Commonwealth network unique needs.
- ▶ Other attack protection capabilities, such as blocking invalid or malformed packets, IP defragmentation, and TCP reassembly, protect against evasion and obfuscation techniques.

[REDACTED] employs natively integrated defensive technologies to ensure that, when a threat evades one technology, another catches it. The key to effective protection is to use security features that are purpose-built to share information and provide context around both the inspected traffic and the identified threats being blocked. The [REDACTED] represents an industry first by inspecting and classifying traffic as well as detecting and blocking both malware and vulnerability exploits in a single pass. Traditional threat prevention technologies require two or more scanning engines and multiple rule bases that need to be managed separately, adding significant latency and management overhead while dramatically slowing throughput performance. [REDACTED] uses a uniform signature format for all threats to ensure rapid processing by performing all analysis in a single, integrated scan, eliminating redundant processes common to traditional solutions. [REDACTED] combs each packet as it passes through the platform, looking closely at byte sequences within both the packet header and payload. From this analysis, important details about a packet are identified, including the application used, its source and destination, whether the protocol is RFC-compliant, and whether the payload contains an exploit or malicious code. Beyond individual packets, [REDACTED] analyzes the context provided by the arrival order and sequence of multiple packets to catch and prevent evasion techniques. All of this happens within one scan, so Commonwealth network traffic will not be throttled.

Altos' Managed IDS/IPS solution provides the following:

- ▶ Expertise and participate in network design and change discussions
- ▶ Experienced and trained network security analysts to participate with the SOC in review of IDS/IPS alerts in real-time
- ▶ Custom dashboards for focused views of IDS/IPS data for the program, each individual customer and other authorized parties, as requested
- ▶ Evaluation network design, Systems and Applications, and traffic patterns when defining policy and rule settings
- ▶ Customized intrusion prevention System policy and signature settings
- ▶ Detailed listing of all active and inactive IDS/IPS signature and policy components upon request
- ▶ Incorporation of the SMM defined threat matrix scoring system into the alert review and escalation process
- ▶ An alert communication template to be used with notifications and escalations. The template will include:
  - An event summary
  - Summary of the threat matrix rating
  - An analyst brief on the signature fired, the source, target systems, vector and attack type as it relates to Customer exposure
  - An analyst brief of false positive analysis
  - An analyst brief of packet capture analysis
- ▶ Implementation of ad hoc requests to change signature and policy settings in accordance with the SMM



- ▶ Roaming users (those not connected to Customer network) to have a content filtering policy that may be different (e.g., more liberal) than when the same user is connected to the Customer network
- ▶ A mechanism to request URL (re)categorization; mechanism will provide requestor with emailed response explaining action(s) taken on request and implementation timeframe as required in the SMM
- ▶ A multi-tenant solution with the ability to monitor browsing activity and provide reports - activity reports will include an estimated browsing time, the number of requests for a site, the sites a user visited, and an overall dashboard showing summary information about this data for the program and each Customer
- ▶ The capability for customers to manage their own users.

#### **User Authentication**

- ▶ Integrated Active Directory user authentication for a seamless access without requiring users to re-enter credentials
- ▶ Allow for the option to require users to enter credentials to access Internet

#### **Content Filtering Bypass**

- ▶ Ability to temporarily bypass the content filtering solution for an individual user when troubleshooting to confirm whether content filtering solution is the cause of an identified issue such as an Internet performance issue, or issue with an individual web site's functionality

#### **URL Categorization/Content Scanning**

- ▶ Manually override of the following URL categorization:
  - For all users on all content filtering policies
  - For all users on a single content filtering policy
  - For a subset of users within a single content filtering policy
  - There will not be a limit on the number of URLs that can have their default categorization overridden

#### **Centralized Policy Management**

- ▶ Secure web-based portal(s) to manage and examine content filtering policy, run reports, look up URL categorizations, and submit URL re-categorization requests
- ▶ The following access roles in portal(s) providing content filtering policy management and reporting functionality:
  - Read-only access to one or more policies
  - Read-write access to one or more policies
  - Access to management portal audit trail
  - Access to reporting for one or more policies/user group(s)

#### **Logging/Log Retention**

- ▶ An audit trail will be maintained for all logins (both successful and unsuccessful); additions, modifications, and deletions; and reports run in the portal(s) providing content filtering policy management and reporting functionality. For logins, the public IP address from which access was attempted will be logged, in addition to the username. For additions, modifications, and deletions, both the user making the change and the specific changes made will be logged. For reports, the user running the report as well as the report run (including applied filters) will be logged. Audit logs will be maintained for a minimum of 12 months.



- ▶ Solution will provide detailed logging of each user's Internet activity down to the individual object level. Detailed logs will include the following information: timestamp (UTC) – to at least a hundredth of a second, policy, username, machine name, machine LAN IP address, public IP address, category/categories, content type (examples: Application/JavaScript, Application/pdf, image/gif, image/jpeg, image/png, text/CSS, text/html, text/JavaScript, video, etc.), disposition (e.g., allowed, blocked), URI, request size, response size. Detailed logs will be retained for 90 days.
- ▶ Summary level information, which outlines activity at the (sub) domain level (excluding user/machine information), will be provided and retained for one year.

## Reporting

- ▶ All types of report content will have the ability to be saved (with selected report filters).
- ▶ All reports will be run on a scheduled basis and the result emailed to one or more email addresses and delivered as identified in the SMM. Scheduling options will include now (on-demand), one-time at specified date and time in the future or on a recurring basis at specified time interval
- ▶ There will not be a limitation on the number of scheduled reports
- ▶ Reports showing trends and baselines will be available
- ▶ Multi-tenant and program-wide detailed and summary reporting of each user's Internet activity will be available
- ▶ Detailed level reports will include the following information: Timestamp (UTC) – down to a second, Policy, Username, Machine Name, Machine LAN IP Address, Destination IP, Category/Categories, Content Type, Disposition, URI, Request Size, Response Size
- ▶ At a minimum the following summary level reports will be available with the ability to drill down to supporting details:
  - Daily level of internet activity per user and IP.
  - Activity by category.
  - Trend information for all summary level reports.
- ▶ Reporting on Internet activity response time: Timestamp (UTC) – down to second, Policy, Username, Site, Number of Requests, Total Request Size, Total Response Size, User Proxy Round Trip Time (seconds/request), Proxy Internet Origin Round Trip Time (seconds/request), Total Response Time (seconds/request)
- ▶ All reports will support filtering by time period, username, user group(s), policy/policies, site(s), category/categories, disposition, IP address(es)
- ▶ Reporting on scanned and blocked file types
- ▶ Summary and detail level reporting on security threats blocked, by service and threat type
- ▶ Summary and detail level reporting on number of unique users/unique machines with activity
- ▶ Trending as follows: Number of Unique Users/Unique Machines, Usernames/Machine name, Number of Requests, Total Request Size, Total Response Size, IP addresses, On-network or Off-network Location
- ▶ Reports will support filtering by time period, time increment (e.g., x minutes, x hours, x days, x weeks), policy, IP address(es), total request size volume /total response size thresholds

## Test Environment/Phased Feature Deployment

- ▶ Ability to test new code and features prior to production deployment



- ▶ Ability to phase in introduction of new features across user base

### 3.2.3 Malware Protection

The Atos solution for malware Protection will provide VITA the following:

- ▶ Capturing and monitoring of context and system state changes that may be an indicator of attack (IoA), as well as attack components lying dormant, and send intelligence to analytics, operations, and forensic teams
- ▶ Ability to adjust to changes in attack methodologies, automate data collection, alerts and responses to objects of interest, and customize configuration to customer workflows
- ▶ Persistent collectors trigger on detection of attack events, alerting people and systems to attack activity
- ▶ Dedicated malware technology to detect and alert for malware attacks at the network perimeter
- ▶ Verification that all anti-virus components are performing within documented performance characteristics, and assistance in all performance troubleshooting and testing activities
- ▶ Understanding of Customer operating systems and Applications to effectively troubleshoot performance issues related to security product
- ▶ Determination of what if any data was/is compromised due to the security event. Include identified information in the security incident report
- ▶ Submission of malicious URLs to Web security vendor to be classified as malicious
- ▶ Real-time malware and malicious activity monitoring at Internet access points, using Tools to pull binaries from the live Internet stream - Actions performed on binaries include reverse engineering and exploding malware in supported operating systems and/or as defined in the SMM
- ▶ Monitoring of DNS traffic for DNS requests to known malicious Internet addresses, interrogate URL and check for malware, phishing, and any other malicious activity
- ▶ The ability to re-route traffic back to a central location and run the traffic through the real-time malware monitoring Tools
- ▶ Assessment of the scope of damage related to all malware events
- ▶ Arresting of the spread and progressive damage from the malware
- ▶ Eradication of malware through techniques such as reverse engineering, custom scripting in endpoint management system, and working with the anti-virus vendor
- ▶ Documentation of troubleshooting steps that can be used by field associates to respond to malware outbreaks or product issue
- ▶ Proactive alerts for consumption by Users regarding current threats in the Environment or based on industry information
- ▶ Daily, weekly, monthly and quarterly reports in the Security Dashboard on malware infections and remediation
- ▶ Custom interface services using standard APIs including those identified in the SMM, between approved anti-virus products and compliance, reporting and deployment Applications
- ▶ Developed interfaces using standard APIs including those identified in the SMM to provide a standard interface for other Tools to gather malware detection data in an automated fashion

- ▶ Monitored logs from Web filtering, firewall, anti-virus and proactive malware Tools for malware infections and possible zero-day infections
- ▶ Development of standard and custom reports to assist in Incident inquiry, correlation and response activities
- ▶ Correlation activities to identify ongoing threats based on data and reports from VITA, Customer, Supplier, authorized third parties and industry sources
- ▶ Installation instructions for the anti-virus solution
- ▶ Authored knowledge base articles, integrating into Systems used by the End User Support and systems support personnel
- ▶ Maintenance of approved anti-virus exclusions ensuring proper alignment with vendor recommendations, technology best practices, and consultation with appropriate subject matter experts
- ▶ An auditable approval process for anti-virus exclusions ensuring proper alignment with all applicable security policies
- ▶ A quarterly report including the number of exclusions, number of new exclusions, number of exclusions removed and business justification for all exclusions
- ▶ Documentation of troubleshooting steps for use by field associates in response to product issue
- ▶ Customized scripts to assist in malware remediation and detection
- ▶ A developed process to address malware protection requirements that are not provided by deployed anti-virus products in the Environment
- ▶ Analysis and recommendations from data, advising on corrective course of action
- ▶ Pro-active alerts to indicate potential malware activity based on definable triggers and rule sets
- ▶ Web portal allowing remote execution of multiple anti-virus engines on assets and deliver scan results back to the centralized data repository

### 3.2.4 Network Forensics/Full Packet Capture

Atos will use [REDACTED] as VITA's Network Forensics/Full Packet Capture tool. [REDACTED] consists of three components: the capture infrastructure, which consists of a highly configurable Decoder that captures and stores raw log and packet data; a Concentrator that stores and indexes metadata for fast queries and retrieving raw data; and a broker that facilitates queries across a multisite deployment of Concentrators and Decoders. The Event Stream Analysis (ESA) module is powerful analytics and alerting engine that enables correlation across multiple event types. Archivers manage long-term data storage. [REDACTED] can be deployed across diverse network typologies and geographies and scaled according to their data capture and performance requirements. [REDACTED]:

- ▶ Inspects every network, packet session and log event for threat indicators at time of collection and enriches this data with threat intelligence and business context.
- ▶ Automated behavior analytics provides insight into attacker tactics, techniques and procedures as they execute their attacks. Detect Command and Control (C2) lateral movement for logs and packets.
- ▶ Collects and examines multiple pieces of data in real time and over extended periods of time, detects deviations from normal behavior, and creates a probability-weighted risk score for alerts based on these results.

Atos' Network Forensics/Full Packet Capture solution will:

- ▶ Ensure that data is coming in at line speed and that there will be no delays with the system performance.
- ▶ Verify that the system is able to process the amount of data provided, with ability to expand.
- ▶ Provide a full packet capture solution with enough resources to capture and record data and can display collected data quickly.
- ▶ Provide a full packet capture solution that can easily be viewed by protocol, MAC, VLAN, geo-IP, and so on, and that data can be filtered.
- ▶ Provide a full packet capture solution that has the ability to perform network behavior analysis (NBA) and block traffic that doesn't meet a certain policy.
- ▶ Download sample packets for inspection using a protocol analyzer if needed, or if it will send them over to the authorities in accordance with the SMM.
- ▶ Retain and preserve the original timestamps. Timestamps will be synchronized to a common time zone.
- ▶ Ensure that full packet capture solution will not cause a single point of failure.
- ▶ Ensure that logs are saved and preserved.
- ▶ Ensure the security of the packet capture solution.
- ▶ Decrypt captured traffic when approved by VITA and as specified in the SMM.
- ▶ Acknowledge and understand relevant privacy laws and concerns regarding full-packet capture.

If VITA desires to have the [REDACTED] firewall incorporated into our overall security proposal, the [REDACTED] firewalls we will be able to detect threats within encrypted data via multiple methods:

- ▶ The header data such as the IP addresses, domains, etc. is not encrypted and can be used to determine if communication is occurring with an entity known [REDACTED] as malicious.
- ▶ If agreed upon and implemented by the relevant Agency, [REDACTED] can decrypt communications between endpoints and servers for the purposes of inspecting the payload contents for threats. This data is only in decrypted form within a secured enclave, either on the appliance performing the decryption or within a select group of other security appliances. All access to these devices will be restricted via role-based access control, and all data accessed, and policies modified will be logged for auditing purposes.

### 3.2.5 Data Loss Prevention (DLP)

Atos' Data Loss Prevention (DLP) solution utilizes [REDACTED] unified DLP to monitor and prevent confidential data loss. Unified DLP provides quick monitoring real-time events, centrally managed security policies to control how employees use and transfer sensitive data, and generates detailed forensics reports with minimal impact to daily business activities. This solution will prevent data loss and leakage when data is modified, copied, pasted, printed, or transmitted while enabling its flexible use. Atos will monitor data moving across Customer's network and create an audit trail of policy-violation incidents. Atos will also monitor Customer networks, including but not limited to routers, switches, intrusion detection systems (IDS), intrusion prevention systems (IPS), firewalls, etc. for evidence of threats, and to use this information in security and threat analysis.

Atos' solution utilizing [REDACTED] DLP will provide VITA:

- ▶ Integration of event logging into the SIEM solution in accordance with the SMM.
- ▶ Scalability capable of automatically detecting or blocking transmissions containing sensitive data, encrypting emails containing sensitive data, or quarantining messages that may need approval to exit Customer's network.



- ▶ Integration with a centralized Data Loss Prevention environment.
- ▶ A solution that is not limited to individual packets. The solution will decrypt captured information and intelligently assemble traffic streams into Application-layer sessions.
- ▶ Ability to understand, reassemble and review various protocols such as SMTP, HTTP, HTTPS, Instant Message, FTP, Telnet, P2P communications and applications. Network DLP will support the reassembly and investigation of Microsoft Word, Microsoft Excel, and Adobe PDF attachments.
- ▶ Ability to add additional scanning categories and content filters (e.g., adult content, credit card information, backdoors, key logger, P2P, personal information, Social Security numbers, violent acts).
- ▶ Definition of shared variables to be used by rules. This may include network address ranges, strings for pattern matching, etc.
- ▶ Ability to create custom signatures using pattern matching in conjunction with other defined rule parameters as specified in the SMM.
- ▶ Evaluation of network architecture, traffic patterns, protected system types and Customer DLP requirements to define custom rules and monitoring.
- ▶ Customized policy and signature settings
- ▶ Coordination with Customer and service providers to evaluate changes to network architecture, traffic patterns, protected system types and updated Customer security requirements at a minimum annually.
- ▶ Response to requests to provide detailed listings of all rules and logic.
- ▶ Response to requests to research and identify rule capabilities related to Customer perceived threats (e.g. new patch, internal investigation).
- ▶ The execution of, in accordance with Customer's security policies, annual security scans of attached data storage at Customer facilities to look for sensitive data.
- ▶ The capability for data to be scanned at Customer facilities.
- ▶ The capability to scan for sensitive data upon demand for any device located on Customer's network.
- ▶ Ability to scan UNIX, Linux and Windows computers, file shares, servers, databases, repositories such as SharePoint and any other systems identified in the SMM.
- ▶ Capability to add additional domestic and international regulatory classifications to scanning criteria.
- ▶ Ability to throttle the host's CPU utilization during scanning, such that scanning is non-impacting to production systems and Applications.
- ▶ A method for requesting scan reports upon demand.
- ▶ Scans will be conducted as directed by VITA and/or Customer (e.g. during non-business hours) providing the following in accordance with the SMM:
  - Export of scan results
  - Analysis of scan results
- ▶ Management of the validation scanning and Application configuration to remove false positives.
- ▶ Communication of the scan results and remediation options with VITA and/or the data owning agency.
- ▶ "Per scan" metrics on file deletion, file redaction, and file encryption and false positives.
- ▶ Online analysis and reporting of the remediation efforts to include "per scan" metrics on file deletion, file redaction, and file encryption and false positives.
- ▶ Continuous monitoring of scan progress to ensure that it is successfully completed.
- ▶ Customer trends and progress reports as listed below:
  - Monthly, quarterly and yearly metrics of all scans conducted to include scan dates

- name of server or shares, total number of Incidents
- number of file deletions
- number of file redactions
- number of file encryptions
- number of false positives across all content policies
- Any other metrics specified in the SMM.

### 3.2.6 Compliance Management

Atos security leverages process, technology and tooling with established baselines that support VITA's information assurance requirements. Once in place, these baselines follow a disciplined change management process to ensure security provisioning maintains the highest integrity—no arbitrary or unrecorded configuration changes. Although the broad spectrum of people, processes, and technologies that are fused together as part of this proposal collectively address compliance management across VITA, the key areas that address the majority of activity for compliance management are:

- ▶ [REDACTED] – Agentless Network Access Control (NAC)
- ▶ [REDACTED] – a dedicated GRC specialist that will focus on supporting security and compliance management tasks within RSA Archer.

### 3.2.7 Vulnerability Management

Atos recognizes the need and ability to consistently measure the effectiveness of a vulnerability management program. As such, Atos Cyber Security exercises a robust patch and vulnerability management program to proactively prevent the exploitation of vulnerabilities within VITA's environments. Our combination of tooling and process leverage an asset-based approach to vulnerability management that provides for maximum coverage of VITA's evolving assets.

Through the use of [REDACTED], Atos will serve as the central point for vulnerability management activities and will work with the MSI to coordinate remediation activities with other Service Provider's teams to:

- ▶ Ensure a current inventory of IT resources
- ▶ Monitor security sources for vulnerabilities,
- ▶ Vulnerability, by risk, prioritization
- ▶ Support VITA in conducting testing of patches and remediation
- ▶ Maintain a vulnerability and remediation information database
- ▶ Verify (through regular scanning) vulnerability remediation

The vulnerability management solution will be integrated with the [REDACTED] platform to automatically adjust threat risk score based on the assets known vulnerabilities.

### 3.2.8 Penetration Testing

Atos will partner with a 3<sup>rd</sup>-party penetration testing company to ensure an independent review of security. Atos will participate in the penetration testing program where identified and follow the procedures and requirements included in the SMM. Atos will make services available within the scope of the penetration testing program and will participate in the penetration testing program established for the environment. The penetration testing program will require participation where identified and following procedures and requirements included in the SMM.



### 3.2.9 Managed Firewall

Atos has partnered with ePLUS to provide a managed firewall solution through the use of [REDACTED]. ePLUS has both expertise and trained resources on [REDACTED], which is in use on the program today. To meet VITA's requirements, we are proposing [REDACTED] firewalls for the 1 GB and 10 GB service and [REDACTED] for the 100 MB service.

[REDACTED] firewalls can be deployed in High Availability to ensure no impact to the Supplier and Program environment. [REDACTED] firewalls can integrate into third-party change management solutions to ensure proper approval of changes prior to commits. Role-based access to the firewalls provides the ability to limit who can update rules, objects, network settings and other areas of responsibility.

[REDACTED] firewalls generate alerts for system level and service events that can be forwarded to third-party systems for incident management, monitoring, reporting and alerting. [REDACTED] identifies applicable vulnerabilities, software bugs, assesses the risk, and works to develop fixes in a timely manner. Major feature releases typically occur two times per year. Critical patches around vulnerabilities are released as needed to ensure customers are protected at all time. [REDACTED] support maintains a list of "Recommended" versions for each major and minor release of [REDACTED] that will be considered when scheduling routine maintenance.

All [REDACTED] firewalls are application aware and identify applications regardless of the port being used. If the application used does not show up in the database of known applications, port and protocols can be used or a custom application can be created. Whether using Application-based rules or port/protocols rules, Security profiles can be attached to policy to scan for and prevent both known and unknown threats.

[REDACTED] provides best practices for implementing security policies, profiles and other features to properly protect organizations. Those best practices translate into system level configurations and firewall security policies. As new threats or vulnerabilities are discovered, best practices are updated to ensure customers are properly protected. In addition to best practices, [REDACTED] addresses threats and vulnerabilities through the use of content updates. Content updates provide new signatures for Applications, IDS/IPS, Anti-Virus, Anti-Spyware, DNS, URL Categories, and 0-Day malware in update intervals as fast as five minutes. Content updates can be done automatically or manually in order to adhere with change control policy.

[REDACTED] firewalls provide:

- ▶ Stateful packet filtering (IPv6)—Maintain per-flow state table, allow packets matching criteria
- ▶ Packet inspection for a variety of IP values (for example, length, checksum, fragmentation)
- ▶ Higher layer state checks including TCP
- ▶ Detection and protection against a variety of types of attacks
- ▶ Tracking of "Top Talkers" based on sessions or bandwidth usage based on particular flows, src/dst IP addresses and endpoint pairs
- ▶ Anomaly tables for tracking sites under attack or potential hackers
- ▶ Support for application layer gateway (ALG) algorithms

Atos' Managed Firewall solution partnered with ePLUS will provide VITA the following:

- ▶ The capability and process to expedite firewall rule change requests
- ▶ Response to incidents and problems with Firewall Services



- ▶ Continuously monitored firewalls, and reports of any alerts or events to VITA and VITA Customers immediately, in accordance with the SMM and Customer's escalation and reporting procedures
- ▶ Program-wide and individual Customer firewall rule set reports and configuration information via real time reporting and immediately upon request
- ▶ Integration of firewall services with Internet Proxy services (e.g., integration with Content Delivery Networks (e.g., Akamai))
- ▶ Coordination of work with customers, following established change control policies, to test and validate firewall rules
- ▶ Audited firewall rules that have been created in response to security threats and business continuity at least quarterly, for their technical relevance and integrity
- ▶ Assurance that firewall components are performing within defined performance guidelines and assistance in all performance troubleshooting and testing activities
- ▶ Access to reports that will reflect on demand, daily, weekly, and monthly status of overall firewall operational and rule data
- ▶ Support of exception handling processes and improvement recommendations to Customer or the Third-Party Provider responsible for handling exception requests
- ▶ Maintenance of an auditable approval process for firewall rules ensuring proper alignment with all VITA and VITA Customer security policies and as established in the SMM
- ▶ Review of firewall events (alarms) to identify false positives and systems that need remediation
- ▶ A method to submit firewall change requests
- ▶ Review new firewall change requests at least daily and as specified in the SMM
- ▶ Integration of logging into the SIEM solution in accordance with the SMM
- ▶ A designed and engineered process or infrastructure that will allow the ability to audit and review all firewall rules based on the firewall request/exception process, and determine if the firewall rules are still valid, can be deleted, or need to be updated
- ▶ A portal and integration into a portal to allow VITA and Customers to review, approve, or identify for deletion firewall rules impacting the customer and/or the enterprise
- ▶ An electronic copy of the firewall rules implemented and available to Customer in accordance with the SMM
- ▶ Allowance granted for penetration testing and vulnerability scans to be performed against the Solution
- ▶ Atos will provide network security services utilizing a defense-in-depth approach through enclaves (zoning) of the Enterprise network with multi-layered internal protections. Solution will enforce Network Access Control (NAC) requirements on those enclaves identified in the SMM requiring this level of security. Firewalls will be managed at the network level to enforce a security policy between tenants, and sub-tenants. Firewalls will also be managed to protect at the host level where identified.

The following items are additional options that will be made available to VITA customers upon request in order to allow flexibility for various agency needs:

#### **Virtual Firewall**

The [REDACTED] virtualized form factor of next-generation firewall can be deployed in a range of private and public cloud computing environments based on technologies from VMware®, Amazon® Web Services, Microsoft®, Citrix® and KVM.

The [REDACTED] natively analyzes all traffic in a single pass to determine the application identity, the content within, and the user identity. These core elements can then be used as integral components of Commonwealth

security policy, enabling the Commonwealth to improve its security efficacy through a positive control model and reduce the incident response time through complete visibility into applications across all ports.

The following performance matrix will be utilized when sizing an appropriate virtual firewall:

Model	VF-50	VF-100	VF-300	VF-500	VF-700
	200 Mbps	2 Gbps	4 Gbps	8 Gbps	16 Gbps
	100 Mbps	1 Gbps	2 Gbps	4 Gbps	8 Gbps
	N/A	1 Gbps	1.5 Gbps	3 Gbps	N/A
	N/A	2 Gbps	4 Gbps	4 Gbps	4 Gbps
	N/A	1 Gbps	1 Gbps	1 Gbps	1 Gbps

#### **Sandbox**

As an option for enhanced security capabilities a license may be provided for an additional layer of threat protection to the . This provides protection from previously unknown threats (zero-day threats, APT) within five minutes and sandbox capabilities related to network.

#### **Firewall Self-service Enablement**

manages complex network security policies throughout their lifecycle— from discovering application connectivity requirements, through ongoing change management and proactive risk analysis, to secure decommissioning. With powerful visibility across all leading firewalls and cloud security controls, simplifies, automates and orchestrates security policy management to accelerate application delivery while ensuring security and continuous compliance across the enterprise. This tool and processes are utilized to provide management firewall services. In addition, the platform and licenses can be provided as an optional service for agencies who may want self-service / self-management capability for firewalls.

Delivers visibility and analysis of complex network security policies across on premise and cloud networks. It automates and simplifies security operations including troubleshooting, auditing and risk analysis. Using , agencies can optimize the configuration of firewalls, routers, web proxies and related network infrastructure to ensure security and compliance. Licensed for cluster.

automates the entire security policy change process — from design and submission to proactive risk analysis, implementation, validation and auditing. Its intelligent automated workflows eliminate guesswork and help agencies save time, avoid manual errors and reduce risk.

automates the entire security policy change process — from design and submission to proactive risk analysis, implementation, validation and auditing. Its intelligent automated workflows eliminate guesswork and help agencies save time, avoid manual errors and reduce risk. Licensed for cluster.



Delivers visibility and analysis of complex network security policies across on premise and cloud networks. It automates and simplifies security operations including troubleshooting, auditing and risk analysis. Using [REDACTED], agencies can optimize the configuration of firewalls, routers, web proxies and related network infrastructure to ensure security and compliance.

Discover, provision, maintain and securely decommission network connectivity for critical business applications. By automatically discovering and mapping application connectivity requirements to the underlying network infrastructure, [REDACTED] accelerates business application delivery, minimizes outages and enforces security and compliance across virtual, cloud and physical networks. [REDACTED] requires additional license for [REDACTED].

### 3.3 Internal Network Controls

### 3.3.1 Managed IDS/IPS

Atos will use [REDACTED] which discovers and blocks sophisticated threats in the network. [REDACTED] is firewall-native and provides multiple layers of prevention, confronting threats at each phase of an attack. In addition to traditional IPS capabilities, [REDACTED] has the unique ability to detect and block threats on all ports instead of invoking signatures based on a limited set of predefined ports.

To ensure holistic protection, [REDACTED], with its tight integration with combines multiple defensive mechanisms:

- Heuristic-based analysis detects anomalous packet and traffic patterns, such as port scans, host sweeps, and denial-of-service (DoS) attacks.
- Easy-to-configure, custom vulnerability signatures tailor intrusion prevention capabilities to Commonwealth network unique needs.
- Other attack protection capabilities, such as blocking invalid or malformed packets, IP defragmentation, and TCP reassembly, protect against evasion and obfuscation techniques.

██████████ employs natively integrated defensive technologies to ensure that, when a threat evades one technology, another catches it. The key to effective protection is to use security features that are purpose-built to share information and provide context around both the inspected traffic and the identified threats being blocked.

The [REDACTED] represents an industry first by inspecting and classifying traffic as well as detecting and blocking both malware and vulnerability exploits in a single pass. Traditional threat prevention technologies require two or more scanning engines and multiple rule bases that need to be managed separately, adding significant latency and management overhead while dramatically slowing throughput performance. [REDACTED] uses a uniform signature format for all threats to ensure rapid processing by performing all analysis in a single, integrated scan, eliminating redundant processes common to traditional solutions. [REDACTED] combs each packet as it passes through the platform, looking closely at byte sequences within both the packet header and payload. From this analysis, important details about a packet are identified, including the application used, its source and destination, whether the protocol is RFC-compliant, and whether the payload contains an exploit or malicious code. Beyond individual packets, [REDACTED] analyzes the context provided by the arrival order and sequence of multiple packets to catch and prevent evasion techniques. All of this happens within one scan, so Commonwealth network traffic will not be throttled.



Atos' Managed IDS/IPS solution provides the following:

- ▶ Expertise and participate in network design and change discussions
- ▶ Experienced and trained network security analysts to participate with the SOC in review of IDS/IPS alerts in real-time
- ▶ Custom dashboards for focused views of IDS/IPS data for the program, each individual customer and other authorized parties, as requested
- ▶ Evaluation network design, Systems and Applications, and traffic patterns when defining policy and rule settings
- ▶ Customized intrusion prevention System policy and signature settings
- ▶ Detailed listing of all active and inactive IDS/IPS signature and policy components upon request
- ▶ Incorporation of the SMM defined threat matrix scoring system into the alert review and escalation process
- ▶ An alert communication template to be used with notifications and escalations. The template will include:
  - An event summary
  - Summary of the threat matrix rating
  - An analyst brief on the signature fired, the source, target systems, vector and attack type as it relates to Customer exposure
  - An analyst brief of false positive analysis
  - An analyst brief of packet capture analysis
- ▶ Implementation of ad hoc requests to change signature and policy settings in accordance with the SMM
- ▶ Full packet captures for alerts upon request within format specified by SMM, an alert escalation process with VITA, Customer, authorized third-party contacts, and any other parties identified in the SMM
- ▶ An inline testing environment replicating key ingress/egress traffic to test and validate signatures. This traffic will simulate or mirror production traffic
- ▶ An upgrade to the network IPD/IPS devices and all associated rules, signatures, settings and software when upgrades are provided by the applicable vendor, when such upgrades are in accordance with industry best practices, or as required to maintain compliance with security requirement
- ▶ A risk exception for Customer approval for any network device that cannot be configured, maintained or updated
- ▶ Workflows will exist for both logical (Software) bypass and physical (cabling) bypass of inline traffic processing, bypasses will exist as emergency procedures in the event of perceived impact from IDS/IPS devices
- ▶ Prerequisites and workflows for restoring bypassed inline IDS/IPS devices. IDS and IPS devices establish a baseline of normal user pattern and anything that deviates from the baseline will be flagged as a possible attack

### 3.3.2 Web Content Filtering

██████ web protection & content filtering capabilities equip VITA with security controls which protect the agencies' inbound and outbound traffic, for every device, user and location. As illustrated below, ██████ integrated web protection capabilities will provide VITA with the ability to:

- ▶ Perform content inspection, which will safeguard users from unwanted URL's, categories, and media types

- ▶ Provide Application Visibility & Control, identifying all cloud applications, and preventing the high cost of supporting Shadow IT services
- ▶ Support an integrated end-to-end web protection solution, providing real-time integration into the SIEM
- ▶ Limit incremental latency (including incremental network latency) for Internet content to 60 milliseconds or as defined in the SMM

### **Content Filtering Policy**

- ▶ Provide ability to support filtering policies for a multi-tenant environment; content filtering policies will be defined by assigning dispositions to Web site categories
- ▶ Provide these options for each category:
  - Allow
  - Block
  - Continue: User presented with a message containing a click-through link; user will click the link in order to access the site
  - Quota: User permitted to access sites in specified category for a defined period of time and/or bandwidth consumption per day
- ▶ If a given URL is associated with multiple categories, the most restrictive option will win
- ▶ Provide ability to override default categorization: all users, one or more groups of users, and individual users
- ▶ Provide ability to assign content filtering policies at the user level (vice machine or Customer location level)
- ▶ Provide ability for the content filtering policy assigned to an on-network user to follow the user from one Customer location to another Customer location
- ▶ Provide ability for roaming users (those not connected to Customer network) to have a content filtering policy that may be different (e.g., more liberal) than when the same user is connected to the Customer network
- ▶ Provide the ability to apply content filtering policies per IP address
- ▶ Provide ability to use a custom block, continue, or quota page on a per-category basis
- ▶ Provide a multi-tenant solution with the ability to monitor browsing activity and provide reports - the activity reports will include an estimated browsing time, the number of requests for a site, the sites a User visited, and an overall dashboard showing summary information about this data for the program and each Customer

### **User Authentication**

- ▶ Allow for the option to require users to enter credentials in order to access Internet

### **Content Filtering Bypass**

- ▶ Provide ability to temporarily bypass the content filtering solution for an individual user when troubleshooting to confirm whether content filtering solution is the cause of an identified issue such as an Internet performance issue, or issue with an individual web site's functionality

### **URL Categorization/Content Scanning**

- ▶ Provide mechanism to request URL (re)categorization; mechanism will provide requestor with emailed response explaining action(s) taken on request and implementation timeframe as required in the SMM
- ▶ Provide ability to manually override URL categorization:
  - For all users on all content filtering policies
  - For all users on a single content filtering policy
  - For a subset of users within a single content filtering policy

- There cannot be a limit on the number of URLs that can have their default categorization overridden

### Centralized Policy Management

- ▶ Provide secure web-based portal(s) in accordance with the SMM and the MSI ITSM to manage and examine content filtering policy, run reports, look up URL categorizations, and submit URL re-categorization request
- ▶ Provide following access roles in portal(s) providing content filtering policy management and reporting functionality:
  - Read-only access to one or more policies
  - Read-write access to one or more policies
  - Access to management portal audit trail
  - Access to reporting for one or more policies/user group(s)

### Logging/Log Retention

- ▶ Audit trail will be maintained for all logins (both successful and unsuccessful); additions, modifications, and deletions; and reports run in the portal(s) providing content filtering policy management and reporting functionality
  - For logins, the IP address from which access was attempted will be logged, in addition to the username
  - For additions, modifications, and deletions, both the user making the change and the specific changes made will be logged
  - For reports, the user running the report as well as the report run (including applied filters) will be logged. Audit logs will be maintained for a minimum of 12 months
- ▶ Provide detailed logging of each user's Internet activity down to the individual object level
  - Detailed logs will include the following information: timestamp (UTC) – to at least a hundredth of a second, policy, username, machine name, machine LAN IP address, public IP address, category/categories, content type (examples: Application/JavaScript, Application/pdf, image/gif, image/jpeg, image/png, text/CSS, text/html, text/JavaScript, video, etc.), disposition (e.g., allowed, blocked), URI, request size, response size
- ▶ Retain detailed logs for 90 days in a state that is easily accessible/searchable by approved customers

### Reporting

- ▶ Provide for complete reports to be exportable in CSV, PDF, XML, and any other format identified in the SMM
- ▶ Allow all types of report to be saved (with selected report filters)
- ▶ Enable all reports to be run on a scheduled basis and the result emailed to one or more email addresses, and also delivered as identified in the SMM - scheduling options will include: now (on-demand), one-time at specified date and time in the future or on a recurring basis at specified time interval
- ▶ There will not be a limitation on the number of scheduled reports
- ▶ Reports showing trends and baselines will be available
- ▶ Provide multi-tenant and program-wide detailed and summary reporting of each user's Internet activity. Detailed level reports will include the following information: Timestamp (UTC) – down to a second, Policy, Username, Machine Name, Machine LAN IP Address, Destination IP, Category/Categories, Content Type, Disposition, URI, Request Size, Response Size
- ▶ At a minimum the following summary level reports will be available with the ability to drill down to supporting details:
  - Daily level of internet activity per user and IP
  - Activity by category



- Trend information for all summary level reports
- ▶ Provide reporting on Internet activity response time: Timestamp (UTC) – down to second, Policy, Username, Site, Number of Requests, Total Request Size, Total Response Size, User Proxy Round Trip Time (seconds/request), Proxy Internet Origin Round Trip Time (seconds/request), Total Response Time (seconds/request)
- ▶ All reports will support filtering by time period, username, user group(s), policy/policies, site(s), category/categories, disposition, IP address(es)
- ▶ Provide reporting on scanned and blocked file types
- ▶ Provide summary and detail level reporting on security threats blocked, by service and threat type
- ▶ Provide summary and detail level reporting on number of unique users/unique machines with activity. Also, need to be able to show trending as follows: Number of Unique Users/Unique Machines, Usernames/Machine name, Number of Requests, Total Request Size, Total Response Size, IP addresses, On-network or Off-network Location
- ▶ Report will support filtering by time period, time increment (e.g., x minutes, x hours, x days, x weeks), policy, IP address(es), total request size volume /total response size thresholds

#### **Test Environment/Phased Feature Deployment**

- ▶ Provide ability to test new code and features prior to production deployment
- ▶ Provide ability to phase in introduction of new features across user base
- ▶ Provide the capability for customers to manage their own users

### **3.3.3 Malware Protection**

The Atos solution for Malware Protection will provide VITA the following:

- ▶ Capturing and monitoring of context and system state changes that may be an indicator of attack (IoA), as well as attack components lying dormant, and send intelligence to analytics, operations, and forensic teams
- ▶ Ability to adjust to changes in attack methodologies, automate data collection, alerts and responses to objects of interest, and customize configuration to customer workflows
- ▶ Persistent collectors trigger triggers on detection of attack events, alerting people and systems to attack activity
- ▶ Verification that all anti-virus components are performing within documented performance characteristics, and assist in all performance troubleshooting and testing activities
- ▶ Understanding of Customer operating systems and Applications to effectively troubleshoot performance issues related to security products
- ▶ Submission of malicious URLs to Web security vendor to be classified as malicious
- ▶ Real-time malware monitoring at Internet access points, using Tools to pull binaries from the live Internet stream -actions performed on binaries include reverse engineering and exploding malware in supported operating systems and/or as defined in the SMM
- ▶ Monitoring of DNS traffic for DNS requests to known malicious Internet addresses, interrogation of URL and check for malware, phishing, and any other malicious activity
- ▶ The ability to re-route traffic to a central location and run the traffic through the real-time malware monitoring Tools
- ▶ Assessment of the scope of damage related to all malware events
- ▶ Arresting of the spread and progressive damage from the malware
- ▶ When recovering from a malware compromise, restoration all data and Software to its original state
- ▶ Documentation of troubleshooting steps that can be used by field associates to respond to malware outbreaks or product issues

- ▶ Proactive alerts for consumption by End Users regarding current threats in the Customer Environment or based on industry information
- ▶ Daily, weekly, monthly and quarterly reports in the Security Dashboard on malware infections and remediation
- ▶ Custom interface services, using standard APIs including those identified in the SMM, between approved anti-virus products and compliance, reporting and deployment Applications
- ▶ Interfaces using standard APIs including those identified in the SMM to provide a standard interface for other Tools to gather malware detection data in an automated fashion
- ▶ Monitoring of logs from Web filtering, firewall, anti-virus and proactive malware Tools for malware infections and possible zero-day infections
- ▶ Standard and custom reports to assist in Incident inquiry, correlation and response activities
- ▶ Authored, knowledge base articles, integrating into Systems used by the End User Support and systems support personnel
- ▶ Maintenance of an approved anti-virus exclusions ensuring proper alignment with vendor recommendations, technology best practices, and consultation with appropriate subject matter experts
- ▶ An auditable approval process for anti-virus exclusions ensuring proper alignment with all applicable security policies
- ▶ Auditing and reporting on anti-virus exclusions quarterly, including contacting the exclusion requester to validate that the need for the exclusion still exists
- ▶ Inclusion of the number of exclusions, number of new exclusions, number of exclusions removed and business justification for all exclusions in the quarterly report
- ▶ Custom scripts to assist in malware remediation and detection
- ▶ A developed process to address malware protection requirements that are not provided by deployed anti-virus products in the Environment
- ▶ Analysis and recommendations from data, advising on corrective course of action
- ▶ Pro-active alerts to indicate potential virus activity based on definable triggers and rule sets
- ▶ A web portal allowing remote execution of multiple anti-virus engines on assets and deliver scan results back to the centralized data repository
- ▶ A dedicated malware technology to detect and alert for malware attacks at the network perimeter

### 3.3.4 Full Packet Capture

Atos will use [REDACTED] as VITA's Full Packet Capture tool. [REDACTED] consists of three components: the capture infrastructure, which consists of a highly configurable Decoder that captures and stores raw log and packet data; a Concentrator that stores and indexes metadata for fast queries and retrieving raw data; and a broker that facilitates queries across a multisite deployment of Concentrators and Decoders. The Event Stream Analysis (ESA) module is powerful analytics and alerting engine that enables correlation across multiple event types. Archivers manage long-term data storage.

[REDACTED] can be deployed across diverse network typologies and geographies, and scale it according to their data capture and performance requirements. [REDACTED]:

- ▶ Inspects every network, packet session and log event for threat indicators at time of collection and enriches this data with threat intelligence and business context.
- ▶ Automated behavior analytics provides insight into attacker tactics, techniques and procedures as they execute their attacks. Detect Command and Control (C2) lateral movement for logs and packets.
- ▶ Collects and examines multiple pieces of data in real time and over extended periods of time, detects deviations from normal behavior, and creates a probability-weighted risk score for alerts based on these results.



- ▶ Atos will address Full Packet Capture with awareness of privacy concerns and will be familiar with and review the relevant privacy laws.

Highlights of the Network Forensics Platform include the following:

- ▶ Continuous, lossless packet capture with nanosecond timestamping at speeds of up to 20Gbps
- ▶ Real-time indexing of all captured packets using timestamp and connection attributes. Export of flow index in NetFlow v5, v9 and IPFIX formats for use with other flow analysis tools
- ▶ Session decoders for viewing and searching web, email, FTP, DNS, chat, SSL connection details, and file attachments
- ▶ Industry-standard data storage and export in PCAP format, which can be stored with flexible storage options; on the appliance, SAS-attached, or SAN-attached storage

### 3.3.5 Data Loss Prevention

Atos has teamed with [REDACTED] to implement a DLP solution quickly and effectively that protects VITA and VITA customer data. [REDACTED] DLP integrates with other solutions in our data protection portfolio to provide the ultimate protection for data at rest, data in use, and data in motion. The Atos DLP solution will:

- ▶ Monitor and filter data moving across Customer's network and creating an audit trail of policy-violation incidents
- ▶ Monitor customer networks, including but not limited to routers, switches, intrusion detection systems (IDS), intrusion prevention systems (IPS), firewalls, etc. for evidence of threats
- ▶ Utilize information gathered in security and threat analysis
- ▶ A highly scalable solution capable of automatically detecting or blocking transmissions containing sensitive data, encrypting emails containing sensitive data, or quarantining messages that may need approval to exit Customer's network
- ▶ A solution that is not limited to individual packets. The solution will decrypt captured information and intelligently assemble traffic streams into Application-layer sessions
- ▶ A solution that is able to understand, reassemble and review various protocols such as SMTP, HTTP, HTTPS, Instant Message, FTP, Telnet, P2P communications and applications. Network DLP will support the reassembly and investigation of Microsoft Word, Microsoft Excel, and Adobe PDF attachments
- ▶ A solution able to add additional scanning categories and content filters (e.g., adult content, credit card information, backdoors, key logger, P2P, personal information, Social Security numbers, violent acts)
- ▶ A solution able to define shared variables to be used by rules. This may include network address ranges, strings for pattern matching, etc.
- ▶ a solution able to create custom signatures using pattern matching in conjunction with other defined rule parameters as specified in the SMM
- ▶ evaluation network architecture, traffic patterns, protected system types and Customer DLP requirements to define custom rules and monitoring
- ▶ coordination with Customer and other service providers to evaluate changes to network architecture, traffic patterns, protected system types and updated Customer security requirements at a minimum annually with reporting to Customer summarizing the discussion and next steps
- ▶ experienced technical contacts to support development and implementation Customer custom rule requests
- ▶ Response to requests to provide detailed listings of all rules and logic.
- ▶ response to requests to research and identify rule capabilities related to Customer perceived threats (e.g. new patch, internal investigation)
- ▶ in accordance with Customer's security policies, annual security scans of attached data storage at Customer facilities to look for sensitive data



- ▶ capability for data to be scanned at Customer facilities
- ▶ capability to scan for sensitive data upon demand for any device located on Customer's network
- ▶ ability to scan UNIX, Linux and Windows computers, file shares, servers, databases, repositories such as SharePoint and any other systems identified in the SMM
- ▶ capability to add additional domestic and international regulatory classifications to scanning criteria
- ▶ the ability to throttle the host's CPU utilization during scanning, such that scanning is non-impacting to production systems and applications
- ▶ integration and management of event logging in to the SIEM infrastructure in accordance with the SMM

Scans as directed by VITA and/or Customer providing the following in accordance with the SMM will provide:

- A method for requesting scan reports upon demand
- Management of the validation scanning and application configuration to remove false positives.
- Continuous monitoring of scan progress to ensure that it is successfully completed
- Ability to export scan results
- Analysis of exported scan results
- Communication of the scan results and remediation options with VITA and/or the data owning agency
- "Per scan" metrics on file deletion, file redaction, and file encryption and false positives
- Online analysis and reporting of the remediation efforts to include "per scan" metrics on file deletion, file redaction, and file encryption and false positives
- Customer trends and progress reports as listed below:
  - Monthly, quarterly and yearly metrics of all scans conducted to include scan dates
  - Name of server or shares, total number of Incidents
  - Number of file deletions
  - Number of file redactions
  - Number of file encryptions
  - Number of false positives across all content policies
  - Any other metrics specified in the SMM.

### 3.3.6 Compliance Management

Atos security leverages process, technology and tooling with established baselines that support VITA's information assurance requirements. Once in place, these baselines follow a disciplined change management process to ensure security provisioning maintains the highest integrity—no arbitrary or unrecorded configuration changes. Although the broad spectrum of people, processes, and technologies that are fused together as part of this proposal collectively address compliance management across VITA, the four key areas that address the majority of activity for compliance management are:

- ▶ Network Access Control (NAC) using [REDACTED] (addressing non-windows non-OS, IoT)
- ▶ Vulnerability Scanning using [REDACTED]
- ▶ ISSO resource with operational expertise tracking activities on the [REDACTED] platform.

### 3.3.7 Vulnerability Management

Atos will use [REDACTED] as an internal vulnerability scanner for VITA's environment. [REDACTED] supports more technologies than competitive solutions, scanning operating systems, network devices, next generation firewalls, hypervisors, databases, web servers and critical infrastructure for vulnerabilities, threats and compliance violations. [REDACTED] key features include:

### Reporting and Monitoring

- ▶ Flexible reporting: Customize reports to sort by vulnerability or host, create an executive summary or compare scan results to highlight changes
- ▶ Targeted email notifications of scan results, remediation recommendations and scan configuration improvements

### Scanning Capabilities

- ▶ Discovery: Accurate, high-speed asset discovery
- ▶ Scanning: Vulnerability scanning (including IPv4/IPv6/hybrid networks)
- ▶ Un-credentialed vulnerability discovery
- ▶ Credentialed scanning for system hardening and missing patches
- ▶ Meets PCI DSS requirements for internal vulnerability scanning
- ▶ Coverage: Broad asset coverage and profiling
  - Network devices: firewalls/routers/switches (Juniper, Check Point, Cisco, Palo Alto Networks), printers, storage
  - Offline configuration auditing of network devices
  - Virtualization VMware ESX, ESXi, vSphere, vCenter, Microsoft, Hyper-V, Citrix Xen Server
  - Operating systems: Windows, OS X, Linux, Solaris, FreeBSD, Cisco iOS, IBM iSeries
  - Databases: Oracle, SQL Server, MySQL, DB2, Informix/DRDA, PostgreSQL, MongoDB
  - ~~Web applications: Web servers, web services~~, OWASP vulnerabilities (Application Scanning suspended on MOD 23 Effective Date)
  - Cloud: Scans the configuration of cloud applications like Salesforce and cloud instances like Amazon Web Services, Microsoft Azure and Rackspace
  - Compliance: Helps meet government, regulatory and corporate requirements
  - Helps to enforce PCI DSS requirements for secure configuration, system hardening, malware detection, ~~web-application-scanning~~ (Application Scanning suspended on MOD 23 Effective Date) and access controls
- ▶ Threats: Botnet/malicious, process/anti-virus auditing
  - Detect viruses, malware, backdoors, hosts communicating with botnet-infected systems, known/unknown processes, web services linking to malicious content
  - Compliance auditing: FFIEC, FISMA, CyberScope, GLBA, HIPAA/ HITECH, NERC, SCAP, SOX
  - Configuration auditing: CERT, CIS, COBIT/ITIL, DISA STIGs, FDCC, ISO, NIST, NSA, PCI
  - Control Systems Auditing: SCADA systems, embedded devices and ICS applications
  - Sensitive Content Auditing: PII (e.g., credit card numbers, SSNs)

### 3.3.8 Penetration Testing

Atos will partner with a 3<sup>rd</sup>-party penetration testing company to ensure an independent review of security. Atos will participate in the penetration testing program where identified and follow the procedures and requirements included in the SMM. Atos will make services available within the scope of the penetration testing program and will participate in the penetration testing program established for the environment. The penetration testing program will require participation where identified and following procedures and requirements included in the SMM.

### 3.3.9 Managed Firewall

#### “Enterprise” Firewall Vendor

The proposed firewalls provided can be deployed in High Availability to ensure no impact to the Supplier and Program environment. The firewalls can integrate into third-party change management solutions to ensure proper



approval of changes prior to commits. Role-based access to the firewalls provides the ability to limit who can update rules, objects, network settings and other areas of responsibility.

The firewalls generate alerts for system level and service events that can be forwarded to third-party systems for incident management, monitoring, reporting and alerting. The vendor identifies applicable vulnerabilities, software bugs, assesses the risk, and works to develop fixes in a timely manner. Major feature releases typically occur two times per year. Critical patches around vulnerabilities are released as needed to ensure customers are protected at all time. The vendor's support function maintains lists of "Recommended" versions for each major and minor release of operating systems that will be considered when scheduling routine maintenance.

The firewalls are application aware and provide the ability to identify applications regardless of the port being used. If the application used does not show up in the database of known applications, port and protocols can be used or a custom application can be created. Whether using Application-based rules or port/protocols rules, Security profiles can be attached to policy to scan for and prevent both known and unknown threats.

The firewall vendor provides best practices for implementing security policies, profiles and other features to properly protect organizations. Those best practices translate into system level configurations and firewall security policies. As new threats or vulnerabilities are discovered, best practices are updated to ensure customers are properly protected. In addition to best practices, the vendor addresses threats and vulnerabilities through the use of content updates. Content updates provide new signatures for Applications, IDS/IPS, Anti-Virus, Anti-Spyware, DNS, URL Categories, and 0-Day malware in update intervals as fast as five minutes. Content updates can be done automatically or manually in order to adhere with change control policy.

#### **Remote Location Firewall Vendor**

The remote location firewalls offer the following services:

- ▶ Stateful packet filtering (IPv6)—Maintain per-flow state table, allow packets matching criteria
- ▶ Packet inspection for a variety of IP values (for example, length, checksum, fragmentation)
- ▶ Higher layer state checks including TCP
- ▶ Detection and protection against a variety of types of attacks
- ▶ Tracking of "Top Talkers" based on sessions or bandwidth usage based on particular flows, src/dst IP addresses and endpoint pairs
- ▶ Anomaly tables for tracking sites under attack or potential hackers
- ▶ Support for application layer gateway (ALG) algorithms

Atos' Managed Firewall solution partnered with ePLUS will provide VITA the following:

- ▶ The capability and process to expedite firewall rule change requests
- ▶ Response to incidents and problems with Firewall Services
- ▶ Continuously monitored firewalls, and reports of any alerts or events to VITA and VITA Customers immediately, in accordance with the SMM and Customer's escalation and reporting procedures
- ▶ Program-wide and individual Customer firewall rule set reports and configuration information via real time reporting and immediately upon request
- ▶ Integration of firewall services with Internet Proxy services (e.g., integration with Content Delivery Networks (e.g., Akamai))
- ▶ Coordination of work with customers, following established change control policies, to test and validate firewall rules
- ▶ Audited firewall rules that have been created in response to security threats and business continuity at least quarterly, for their technical relevance and integrity



- ▶ Assurance that firewall components are performing within defined performance guidelines and assistance in all performance troubleshooting and testing activities
- ▶ Access to reports that will reflect on demand, daily, weekly, and monthly status of overall firewall operational and rule data
- ▶ Support of exception handling processes and improvement recommendations to Customer or the Third-Party Provider responsible for handling exception requests
- ▶ Maintenance of an auditable approval process for firewall rules ensuring proper alignment with all VITA and VITA Customer security policies and as established in the SMM
- ▶ Review of firewall events (alarms) to identify false positives and systems that need remediation
- ▶ A method to submit firewall change requests
- ▶ Review new firewall change requests at least daily and as specified in the SMM
- ▶ Integration of logging into the SIEM solution in accordance with the SMM
- ▶ A designed and engineered process or infrastructure that will allow the ability to audit and review all firewall rules based on the firewall request/exception process, and determine if the firewall rules are still valid, can be deleted, or need to be updated
- ▶ A portal and integration into a portal to allow VITA and Customers to review, approve, or identify for deletion firewall rules impacting the customer and/or the enterprise
- ▶ An electronic copy of the firewall rules implemented and available to Customer in accordance with the SMM
- ▶ Allowance granted for penetration testing and vulnerability scans to be performed against the Solution
- ▶ Atos will provide network security services utilizing a defense-in-depth approach through enclaves (zoning) of the Enterprise network with multi-layered internal protections. Solution will enforce Network Access Control (NAC) requirements on those enclaves identified in the SMM requiring this level of security. Firewalls will be managed at the network level to enforce a security policy between tenants, and sub-tenants. Firewalls will also be managed to protect at the host level where identified.

The following items are additional options that will be made available to VITA customers upon request in order to allow flexibility for various agency needs:

#### Managed Virtual Firewall

The virtualized form factor of next-generation firewall can be deployed in a range of private and public cloud computing environments based on technologies from VMware®, Amazon® Web Services, Microsoft®, Citrix® and KVM.

The [REDACTED] natively analyzes all traffic in a single pass to determine the application identity, the content within, and the user identity. These core elements can then be used as integral components of Commonwealth security policy, enabling the Commonwealth to improve its security efficacy through a positive control model and reduce the incident response time through complete visibility into applications across all ports.

The following performance matrix will be utilized when sizing an appropriate virtual firewall:

Model	VF-50	VF-100	VF-300	VF-500	VF-700
[REDACTED]	200 Mbps	2 Gbps	4 Gbps	8 Gbps	16 Gbps

	100 Mbps	1 Gbps	2 Gbps	4 Gbps	8 Gbps
	N/A	1 Gbps	1.5 Gbps	3 Gbps	N/A
	N/A	2 Gbps	4 Gbps	4 Gbps	4 Gbps
	N/A	1 Gbps	1 Gbps	1 Gbps	1 Gbps

### Sandbox

As an option for enhanced security capabilities a Sandbox license maybe provided for an additional layer of threat protection. This provides protection from previously unknown threats (zero- day threats, APT) within five minutes and sandbox capabilities related to network.

Atos has partnered with ePLUS to provide a managed firewall solution through the use of [REDACTED]. ePLUS has both expertise and trained resources on [REDACTED], which is in use on the program today. To meet VITA's requirements, we are proposing [REDACTED] firewalls for the 1 GB and 10 GB service and [REDACTED] for the 100 MB service.

[REDACTED] firewalls provided can be deployed in High Availability to ensure no impact to the Supplier and Program environment. [REDACTED] firewalls can integrate into third-party change management solutions to ensure proper approval of changes prior to commits. Role-based access to the firewalls provides the ability to limit who can update rules, objects, network settings and other areas of responsibility.

[REDACTED] firewalls generate alerts for system level and service events that can be forwarded to third-party systems for incident management, monitoring, reporting and alerting. [REDACTED] identifies applicable vulnerabilities, software bugs, assesses the risk, and works to develop fixes in a timely manner. Major feature releases typically occur two times per year. Critical patches around vulnerabilities are released as needed to ensure customers are protected at all time. [REDACTED] support maintains a list of "Recommended" versions for each major and minor release of [REDACTED] that will be considered when scheduling routine maintenance.

All [REDACTED] firewalls are application aware firewalls that provide the ability to identify applications regardless of the port being used. If the application used does not show up in the database of known applications, port and protocols can be used or a custom application can be created. Whether using Application-based rules or port/protocols rules, Security profiles can be attached to policy to scan for and prevent both known and unknown threats.

[REDACTED] provides best practices for implementing security policies, profiles and other features to properly protect organizations. Those best practices translate into system level configurations and firewall security policies. As new threats or vulnerabilities are discovered, best practices are updated to ensure customers are properly protected. In addition to best practices, [REDACTED] addresses threats and vulnerabilities through the use of content updates. Content updates provide new signatures for Applications, IDS/IPS, Anti-Virus, Anti-Spyware, DNS, URL Categories, and 0-Day malware in update intervals as fast as five minutes. Content updates can be done automatically or manually in order to adhere with change control policy.

[REDACTED] offers the following firewall services:



- ▶ Stateful packet filtering (IPv6)—Maintain per-flow state table, allow packets matching criteria
- ▶ Packet inspection for a variety of IP values (for example, length, checksum, fragmentation)
- ▶ Higher layer state checks including TCP
- ▶ Detection and protection against a variety of types of attacks
- ▶ Tracking of “Top Talkers” based on sessions or bandwidth usage based on particular flows, src/dst IP addresses and endpoint pairs
- ▶ Anomaly tables for tracking sites under attack or potential hackers
- ▶ Support for application layer gateway (ALG) algorithms

Atos’ Managed Firewall solution partnered with ePLUS will provide VITA the following:

- ▶ Enable stateful packet filtering (IPv6)—Maintain per-flow state table, allow packets matching criteria
- ▶ Allow packet inspection for a variety of IP values (for example, length, checksum, fragmentation)
- ▶ Higher layer state checks including TCP
- ▶ Detection and protection against a variety of types of attacks
- ▶ Tracking of “Top Talkers” based on sessions or bandwidth usage based on particular flows, src/dst IP addresses and endpoint pairs
- ▶ Anomaly tables for tracking sites under attack or potential hackers
- ▶ Support for application layer gateway (ALG) algorithms
- ▶ A secure, configured, multi-layer high availability firewall infrastructure with no single point of failure to support the Supplier and Program environment
- ▶ Where specified, different approved firewall manufacturers on separate layers to reduce exposure to any single manufacturer’s exploit
- ▶ Capability and process to expedite firewall rule change requests
- ▶ Response to incidents and problems with Firewall Services
- ▶ Continuously monitored firewalls, reporting of any alerts or events to VITA and VITA Customers immediately, in accordance with the SMM, Customer’s escalation and reporting procedures
- ▶ Program wide and individual Customer firewall rule set reports and configuration information via real time reporting and immediately upon request
- ▶ Cooperation with customers, following established change control policies, to test and validate firewall rules
- ▶ Audit of all firewall rules that have been created in response to security threats and business continuity at least quarterly, for their technical relevancy and integrity
- ▶ Confirmation that firewall components are performing within defined performance guidelines and assist in all performance troubleshooting and testing activities
- ▶ Access to reports that will reflect on demand, daily, weekly, monthly status of overall firewall operational and rule data
- ▶ Remediation methods for devices that are missing firewall services within the Customer Environment
- ▶ Exception handling processes and provide improvement recommendations to Customer or the Third-Party Provider responsible for handling exception requests
- ▶ An auditable approval process for firewall rules ensuring proper alignment with all VITA and VITA Customer security policies and as established in the SMM
- ▶ Review of the firewall events (alarms) to identify false positives and systems that need remediation
- ▶ Remediation of any of the systems that are in the error state and ensure that a firewall is installed and active
- ▶ A method to submit endpoint firewall change requests
- ▶ Review of new firewall change requests at least daily and as specified in the SMM



- ▶ Integration and management of the logging of administrative actions in to the SIEM infrastructure in accordance with the SMM
- ▶ Design and engineering of a process or infrastructure that will allow the ability to audit and review all firewall rules as based off of the firewall request/exception process, and determine if the firewall rules are still valid, can be destroyed, or need to be updated
- ▶ A portal and integration into a portal to allow Customers to review, approve, or identify for deletion firewalls rules impacting the customer and/or the enterprise
- ▶ Allowance for penetration testing and vulnerability scans to be performed against the Solution
- ▶ Atos will provide network security services utilizing a defense-in-depth approach through enclaves (zoning) of the Enterprise network with multi-layered internal protections. Solution will enforce Network Access Control (NAC) requirements on those enclaves identified in the SMM requiring this level of security. Internal firewalls will be managed at the network level to enforce a security policy between tenants, and sub-tenants. Firewalls will also be managed to protect at the host level where identified.

The following items are additional options that will be made available to VITA customers upon request in order to allow flexibility for various agency needs:

██████████ is a virtualized form factor of our next-generation firewall that can be deployed in a range of private and public cloud computing environments based on technologies from VMware®, Amazon® Web Services, Microsoft®, Citrix® and KVM.

The ██████████ natively analyzes all traffic in a single pass to determine the application identity, the content within, and the user identity. These core elements can then be used as integral components of Commonwealth security policy, enabling the Commonwealth to improve its security efficacy through a positive control model and reduce the incident response time through complete visibility into applications across all ports.

The following performance matrix will be utilized when sizing an appropriate virtual firewall:

Model	VF-50	VF-100	VF-300	VF-500	VF-700
██████████	200 Mbps	2 Gbps	4 Gbps	8 Gbps	16 Gbps
	100 Mbps	1 Gbps	2 Gbps	4 Gbps	8 Gbps
	N/A	1 Gbps	1.5 Gbps	3 Gbps	N/A
	N/A	2 Gbps	4 Gbps	4 Gbps	4 Gbps
	N/A	1 Gbps	1 Gbps	1 Gbps	1 Gbps

As an option for enhanced security capabilities a ██████████ license maybe provided for an additional layer of threat protection to the ██████████ Firewalls. This provides protection from previously unknown threats (zero- day threats, APT) within five minutes and sandbox capabilities related to network.

#### ██████████ Firewall Self-service Enablement

██████████ manages complex network security policies throughout their lifecycle— from discovering application connectivity requirements, through ongoing change management and proactive risk analysis, to secure decommissioning. With powerful visibility across all leading firewalls and cloud security controls, ██████████ simplifies, automates and orchestrates security policy management to accelerate application delivery while ensuring security and continuous compliance across the enterprise. This tool and processes are utilized to provide management firewall services. In addition, the platform and licenses can be provided as an optional service for agencies who may want self-service / self-management capability for firewalls.

██████████  
Delivers visibility and analysis of complex network security policies across on premise and cloud networks. It automates and simplifies security operations including troubleshooting, auditing and risk analysis. Using ██████████, agencies can optimize the configuration of firewalls, routers, web proxies and related network infrastructure to ensure security and compliance. Licensed for cluster.

██████████ automates the entire security policy change process — from design and submission to proactive risk analysis, implementation, validation and auditing. Its intelligent automated workflows eliminate guesswork and help agencies save time, avoid manual errors and reduce risk.

██████████ automates the entire security policy change process — from design and submission to proactive risk analysis, implementation, validation and auditing. Its intelligent automated workflows eliminate guesswork and help agencies save time, avoid manual errors and reduce risk. Licensed for cluster.

██████████  
Delivers visibility and analysis of complex network security policies across on premise and cloud networks. It automates and simplifies security operations including troubleshooting, auditing and risk analysis. Using ██████████, agencies can optimize the configuration of firewalls, routers, web proxies and related network infrastructure to ensure security and compliance.

██████████  
Discover, provision, maintain and securely decommission network connectivity for critical business applications. By automatically discovering and mapping application connectivity requirements to the underlying network infrastructure, ██████████ accelerates business application delivery, minimizes outages and enforces security and compliance across virtual, cloud and physical networks. ██████████ 50 requires additional license for ██████████.

## 3.4 End Point Security

### 3.4.1 Malware Protection

The Atos solution for Malware Protection will provide VITA the following:

- ▶ Capturing and monitoring of context and system state changes that may be an indicator of attack (IoA), as well as attack components lying dormant, and send intelligence to analytics, operations, and forensic teams
- ▶ Ability to adjust to changes in attack methodologies, automate data collection, alerts and responses to objects of interest, and customize configuration to customer workflows



- ▶ Persistent collectors trigger triggers on detection of attack events, alerting people and systems to attack activity
- ▶ Installation, update, upgrade, patch, operation and maintenance of malware Protection Software and systems in accordance with security requirements and VITA Rules for all Software and Equipment in the Environment, including all supported operating systems and platforms
- ▶ Update anti-virus components on all devices within 24 hours of release and testing or in accordance with SMM and work with appropriate third-party vendors to immediately resolve issues
- ▶ Verification that all anti-virus components are performing within documented performance characteristics, and assist in all performance troubleshooting and testing activities
- ▶ Understanding of Customer operating systems and Applications to effectively troubleshoot performance issues related to security products, technologies will be deployed with industry best practices to ensure performance
- ▶ Real-time malware protection scanning in accordance with security requirements, VITA Rules, and the SMM
- ▶ Continuous scans of all Workstations and servers according to the SMM and VITA Rules, Atos will monitor the status of the scans and remediate where necessary to avoid any performance or threat impact to the environment
- ▶ Upon detection of a malware infection, respond immediately as defined by the SMM and VITA Rules
- ▶ In the case malware is detected, analyze malware to determine the following:
  - Function of malware
  - Infection vector of the malware
- ▶ Determination what, if any, data was/is compromised due to the security event, including identified information in the security incident report
- ▶ Submission of new malware (zero-day) binaries to the anti-virus vendor for inclusion in the next pattern release
- ▶ Submission of malicious URLs to Web security vendor to be classified as malicious
- ▶ Real-time malware monitoring at Internet access points, using Tools to pull binaries from the live Internet stream - actions performed on binaries include reverse engineering and exploding malware in supported operating systems and/or as defined in the SMM and VITA Rules
- ▶ Monitoring of DNS traffic for DNS requests to known malicious Internet addresses, interrogate URL and check for malware, phishing, and any other malicious activity
- ▶ The ability to re-route traffic back to a central location and run the traffic through the real-time malware monitoring Tools
- ▶ Assessment of the scope of damage related to all malware events
- ▶ Arresting of the spread and progressive damage from the malware
- ▶ Eradication of malware through techniques such as reverse engineering, custom scripting in endpoint management system, and working with the anti-virus vendor, [REDACTED]
- ▶ When recovering from a malware compromise restore all data and Software to its original state
- ▶ Documentation of troubleshooting steps that can be used by field associates to respond to malware outbreaks or product issues
- ▶ Advanced Tools, including disassemblers, debuggers, tcpdump, and others as required
- ▶ Proactive alerts for consumption by End Users regarding current threats in the Customer Environment or based on industry information
- ▶ Daily, weekly, monthly, and quarterly reports in the Security Dashboard on malware infections and remediation activities
- ▶ Custom interface services, using standard APIs (including those identified in the SMM), between approved anti-virus products and compliance, reporting and deployment Applications



- ▶ Developed interfaces or standard APIs (including those identified in the SMM), to provide a standard interface for other Tools to gather malware detection data in an automated fashion
- ▶ Monitoring of anti-virus logs to detect any malware infections
- ▶ Monitoring of logs from Web filtering, firewall, anti-virus and proactive malware Tools for malware infections and possible zero-day infections
- ▶ Development, maintenance and administration of a centralized data repository and reporting framework that consolidates information from dissimilar security products
- ▶ Retention of data in centralized repository online for a minimum of one year
- ▶ Standard and custom reports to assist in Incident inquiry, correlation and response activities
- ▶ Correlation activities to identify ongoing threats based on data and reports from VITA, Customer, Supplier, authorized third parties and industry sources
- ▶ Installation instructions for the anti-virus solution
- ▶ Authored knowledge base articles and integrate into Systems used by the End User Support and systems support personnel
- ▶ Maintenance of license and support compliance for the anti-virus product(s)
- ▶ Maintenance of approved anti-virus exclusions ensuring proper alignment with vendor recommendations, technology best practices, and consultation with appropriate subject matter experts
- ▶ Maintenance of an auditable approval process for anti-virus exclusions ensuring proper alignment with all applicable security policies
- ▶ Audit and reporting on anti-virus exclusions quarterly, including contacting the exclusion requester to validate that the need for the exclusion still exists
- ▶ Quarterly report including the number of exclusions, number of new exclusions, number of exclusions removed, and business justification for all exclusions
- ▶ Rapidly deployed anti-virus component updates during critical Security Events, as directed by applicable security teams, policies, and VITA Rules
- ▶ Set up, monitoring and troubleshooting of backups of all anti-virus products
- ▶ Custom scripts to assist in malware remediation and detection
- ▶ Development of a process to address malware protection requirements that are not provided by deployed anti-virus products in the Environment
- ▶ The ability to discover and eradicate suspicious files across the environment based on hashes, file names, registry entries, paths, etc.
- ▶ The ability to blacklist or whitelist files based on names and/or hashes
- ▶ Standard and ad hoc reports from the solution that can be used for remediation, cleansing and correlation
- ▶ Proactively compare data from system to malware sites for hash verification of known malware
- ▶ Web portal allowing remote execution of multiple anti-virus engines on assets and deliver scan results back to the centralized data repository
- ▶ Clam AntiVirus (ClamAV) applies to legacy Unix servers and is an open-source antivirus software toolkit able to detect many types of malicious software, including viruses. The ClamAV virus database is updated at least every four hours.

### 3.4.2 Managed Host Intrusion Prevention

Atos' Managed Host Intrusion Prevention solution utilizes [REDACTED]  
[REDACTED] solution as well as [REDACTED]

██████ provides continuous monitoring of endpoint activity so we will know exactly what's happening - from a threat on a single endpoint to the threat level of the Commonwealth. ██████ delivers visibility and in-depth analysis to automatically detect suspicious activity and ensure stealthy attacks - and breaches - are stopped. Insight will provide more than intrusion prevention because it:

- ▶ Provides unparalleled visibility through continuous raw event recording
- ▶ Enables threat hunting - proactive and managed - with full endpoint activity details
- ▶ Unravels the entire attack in the easy-to-use Incident Workbench enriched with context and threat intelligence data
- ▶ Enables our analysts to see the big picture, in real time, delivering situational awareness on the current threat level of the Commonwealth, and how it's changing over time.
- ▶ Can share (if allowed) assessment scores with ██████ zero trust ecosystem partners for real-time conditional access enforcement.
- ▶ Detects and intelligently prioritizes malicious and attacker activity
- ▶ Possesses powerful response actions which will enable Atos to contain and investigate compromised systems, including on-the-fly remote access to take immediate action
- ▶ Searches very quickly – returning threat hunting and investigation query results in five seconds or less
- ▶ Maps alerts to the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) framework which helps Atos and VITA analysts to understand even the most complex detections at a glance

██████ is managed and controlled by ██████. The ██████ resides in the MSS enclave of the Secured Tools Domain.

- ▶ ██████ agents installed on each server are managed by a central hub which consolidates events and sends them to the SIEM.
- ▶ The ██████ also initiates active response actions.
- ▶ The ██████ client on each server would also be centrally managed by the ██████ is a single self-contained on-premise security solution that incorporates file integrity monitoring, policy enforcement, system hardening, intrusion detection, log management and active response.

### 3.4.3 Managed Firewall

Atos will provide an endpoint managed firewall solution through the use of ██████. Atos' Managed Firewall solution partnered with ██████ will provide VITA the following:

- ▶ Installation, update, upgrade, patch, operate and maintain host firewall protection Software and Systems in accordance with security requirements and VITA Rules for all Software and Equipment in the environment
- ▶ Maintenance, understanding and engineering of the architecture of the solution
- ▶ Recommendations for a host-based firewall security profile
- ▶ Engineered security profiles that contain a firewall module, to be used on Commonwealth network endpoints, including client-based Workstations and server OS
- ▶ Administration, configuration, customization and testing "out-of-the-box" firewall rules that have been identified applicable for a firewall security implementation
- ▶ Firewall rules built so that they will not disrupt business, while ensuring a secure platform
- ▶ Firewall rules which are used to identify malware or insecure Applications within Customer's network, data for the rules is derived from reverse engineering of malware and industry security information

- ▶ Engineered firewall rules that can be used to alert on malicious traffic from client-based Workstations and key server infrastructures
- ▶ Configured firewall rules so to fit into business Application models while protecting against emerging threats as they become known
- ▶ Firewall rule(s) as required by security threats, vulnerabilities, and industry best practices:
  - If a new threat (such as compromised devices or unauthorized and unmanaged software with a critical vulnerability) is discovered within the environment, write rules to secure the environment
  - Monitor custom rule deployment and address any of the ad-hoc troubleshooting or maintenance requests immediately
- ▶ Firewall rules that will cover the operating systems and Applications in the environment
- ▶ Installation and testing of rule updates that address known vulnerabilities or risks to endpoint systems, after such updates are identified by the vendor
- ▶ Firewall rules will not interfere with the function and operations of the environment
- ▶ Cooperation with Customers, following established change control policies, to test and validate firewall rules
- ▶ Installation of configuration updates to the endpoint systems as needed or directed, in accordance with the following:
  - All changes will be tested on a test, development or appropriate systems prior to implementation
  - Supplier will have intimate knowledge of Customer deployed assets and Applications to minimize possible risk to VITA, Customer and other Supplier Applications
- ▶ An audit of all firewall rules that have been created in response to security threats and business continuity at least quarterly, for technical relevancy and integrity
- ▶ Ensure that firewall components are performing within defined performance guidelines and assist in all performance troubleshooting and testing activities
- ▶ Results of routine review reporting metrics indicating number of systems to Customer containing the systems that:
  - Use host-based firewall solution
  - Are protected using a host-based firewall solution
  - Systems that are not using a host-based firewall (offline systems)
- ▶ On demand access to reports that reflect the daily, weekly, and monthly status of overall firewall operational and rule data
- ▶ Remediation methods for devices that are missing firewall services within the Customer Environment
- ▶ Identification of the ownership of the end point device
- ▶ Coordination with owner on a time for investigation for firewall services that are offline
- ▶ Scheduling a 'system change' to act on the end point that is offline once a solution has been identified
- ▶ System changes will be understood that prior notice is given to end point owner, unless otherwise identified as a security risk
- ▶ System changes will take place after business hours in the time zone of the end point, unless otherwise identified as a security risk
- ▶ Exception support handling processes and provide improvement recommendations to Customer or the Third-Party Provider responsible for handling exception requests
- ▶ Maintenance of an auditable approval process for firewall rules ensuring proper alignment with all security policies, VITA Rules, and as established in the SMM
- ▶ Maintenance of firewall rules ensuring proper alignment with recommendations, technology best practices, and consultation with subject matter experts.
- ▶ Ongoing tuning of firewall system rules, security profiles, and configuration to minimize false positives and false negatives



- ▶ Ensure that the host firewall solution supports all operating systems and major Applications defined by Customer, including Windows, Linux, HP-UX, AIX, Oracle, WebSphere, Apache, IIS, SQL Server or others as defined in the SMM.
- ▶ Standard and ad-hoc reports for Customer that include the following:
  - Number of devices installed
  - Number of devices failed
  - Health status:
  - Online for firewall
  - Offline for firewall
- ▶ Review of the firewall events (alarms) to identify false positives and systems that need remediation
- ▶ Remediation of any systems that are in the error state and ensure that a firewall is installed and active
- ▶ A method to submit endpoint firewall change requests
- ▶ Review of new firewall change requests at least daily and as specified in the SMM and VITA Rules.
- ▶ A designed and engineered process or infrastructure that will allow the ability to audit and review all firewall rules as based off of the firewall request/exception process, and determine if the firewall rules are still valid, can be destroyed, or need to be updated
- ▶ A portal to allow VITA/Customers to review, approve, or identify for deletion firewalls rules impacting the customer and/or the program-wide environment
- ▶ Firewall functions AEO will manage, depending on agency requirements comprise:
  - Enabling alerts to execute firewall actions on one system, a specific system, or every system (shared defense)
  - Setting dynamic firewall rules to expire (example: block an IP for 10 minutes, and then remove the block automatically)
  - Increasing block time to discourage repeat attackers
  - Acting on intelligence from external services (e.g. external firewall detects attack and AEO active response triggers a block the local server.)
  - Triggering ad-hoc firewall actions without an alert.

#### 3.4.4 Data Loss Prevention

████ Data Loss Prevention (DLP) Endpoint software instantly monitors and prevents confidential data loss. █████ DLP Endpoint protects the Commonwealth from the risks of financial loss, reputation damage, disappointed stakeholders, and regulatory noncompliance. █████ DLP Endpoint provides quick monitoring real-time events, centrally managed security policies to control how employees use and transfer sensitive data, and generates detailed forensics reports with minimal impact to daily business activities. Prevent data loss and leakage when data is modified, copied, pasted, printed, or transmitted while enabling its flexible use. █████ unified data loss protection provides protection for all potential leaking channels, to include removable storage devices, cloud, email, instant messenger, clipboard, printing, screen capture, etc.

████ Data Loss Prevention (DLP) Endpoint software will provide VITA:

- ▶ Comprehensive incident reporting and monitoring gathers all needed data, such as sender, recipient, timestamp, and network evidence, for proper analysis, investigation and audit, remediation, and risk assessment.
- ▶ Visibility of crawling of sensitive data at rest on local hard drives with granular targeting by user and network group.
- ▶ Flexible per-user policies for better control of the data flowing to shared terminals.

- ▶ Control and blockage of confidential data copied to USB devices, flash drives, Apple iPods, and other removable storage devices, including optical media and hard copy.

### 3.4.5 Network Access Control (NAC)

Atos will use [REDACTED] for Network Access Control. [REDACTED] interrogates the network infrastructure to discover devices as they connect to the network. [REDACTED] uses a combination of passive and active methods to classify the device according to its type and ownership. Based on its classification, [REDACTED] then assesses the device security posture and allows organizations to set policies that establish the specific behavior the device is allowed to have while connected to a network.

#### Network Security Risks and Blind Spots

Traditional network security has focused on blocking external attacks with firewalls and intrusion prevention systems. However, these security tools do nothing to protect the network against the deluge of insider threats that are increasingly causing security incidents and breaches. Threats include:

- ▶ Visitors: Guests and contractors bring their computers to the business. Both need Internet access, and contractors may require additional resources. If visitors are given unlimited access, it may expose the network to attack.
- ▶ Wireless and mobile (BYOD) users: Employees want to use their personally owned smartphones, tablets and notebooks on the network. Without adequate control, these devices can infect the network or be a source of data loss.
- ▶ Internet of Things (IoT) devices: Non-traditional devices continue to expand the attack surface by adding unmanaged devices such as IP-attached projectors, thermostats, lighting controls, security cameras and more.
- ▶ Rogue devices: Well-meaning employees can extend the network with inexpensive wiring hubs, departmental servers, routers and wireless access points that can cause network instability and vulnerability.
- ▶ Malware and botnets: Once the network is compromised, network attached devices can be used in “pivot attacks” in which outsiders scan the network and steal the data.
- ▶ Compliance: Misconfigured endpoints and virtual machines may include improper settings or inappropriate software. What’s more, they may be intentionally disabled by the user or by malware—deactivating security controls.

#### How [REDACTED] Works

[REDACTED] provides the unique ability to see IP-attached networked devices, control them and orchestrate information sharing and operation among disparate security tools.

The [REDACTED] deploys out of band on the network. From there, it continuously monitors network traffic and integrates with the networking infrastructure to identify devices as soon as they access the network. [REDACTED] has a unique ability to see a vast array of IP-attached endpoints, users and applications. In fact, [REDACTED]’s sophisticated technologies discover devices that are invisible to competitive products.

Next, [REDACTED] accurately classifies endpoints on the network through passive and active interrogation techniques. [REDACTED] can identify the device type, location, user, and whether the device is a member of the domain, as well as other basic information. It also obtains detailed information about the security posture of the device by using administrative credentials to query corporate-owned devices.



Once [REDACTED] discovers a security problem on an endpoint, its sophisticated policy manager can automatically execute a range of responses depending on the severity of the problem. Minor violations might result in a warning message sent to the end-user. Employees and contractors who bring their own devices can be redirected to an automated onboarding portal. Serious violations will result in actions such as blocking or quarantining the device, reinstallation of a security agent, re-starting of an agent or process, triggering the endpoint to fetch an operating system patch, or performing other remediation actions.

### Key Features

- ▶ Out-of-band deployment: Deploys out of band on the network without adding latency or a potential network failure point.
- ▶ Visibility: The Asset Inventory feature provides real-time, multi-dimensional network visibility and control, enabling tracking and control of users, applications, processes, ports, external devices and more (see Figure
- ▶ Open interoperability: [REDACTED] works with popular switches, routers, VPNs, firewalls, endpoints, operating systems (Windows, Linux, iOS, OS X and Android); patch management systems, antivirus systems, directories and ticketing systems—without infrastructure changes or equipment upgrades.
- ▶ Reporting: A fully integrated reporting engine helps monitor the level of policy compliance, fulfill regulatory audit requirements and produce real-time inventory reports.
- ▶ Scalability: Proven in customer networks exceeding 1,000,000 endpoints. [REDACTED] are available in a variety of sizes

Non-disruptive: Deploy without impacting users or devices. Automated control can evolve gradually, starting with the most problematic locations and choosing appropriate enforcement actions.

Policy management: Create security policies that are right for the enterprise. Configuration and administration are fast and easy thanks to built-in policy templates, rules and reports.

ControlFabric Architecture: Offers extensive third-party vendor interoperability and open integration architecture.

### Endpoint

Agentless: Identify, classify, authenticate and control network access without an agent. Perform deep endpoint inspection without an agent as long as [REDACTED] has administrative credentials on the endpoint. In situations where [REDACTED] does not have administrative credentials, such as BYOD, deep inspection can be performed with the help of our optional SecureConnector agent, which is included with [REDACTED] at no additional charge.

Endpoint compliance: Ensure that endpoints on the network are compliant with the antivirus policy, properly patched and free of illegitimate software. [REDACTED] automatically identifies policy violations, remediates endpoint security deficiencies and measures adherence to regulatory mandates.

Threat detection: Continuous monitoring provides more timely and accurate insights than point-in-time vulnerability scans, as some devices may drop on and off the network.

Rogue device detection: Detect rogue infrastructure such as unauthorized switches and wireless access points. [REDACTED] can even detect devices without IP addresses, such as stealthy packet capture devices designed to steal sensitive information.

### Access



Solution will perform a pre-connect compliance check to ensure only authorized users and devices connect to the network.

Guest registration: Allow guests to access the network without compromising the internal network security. Several guest registration options can tailor the guest admission process to the Commonwealth's needs.

Role-based access: [REDACTED] ensures that the right people with the right devices gain access to the right network resources. It leverages the existing directory where roles are assigned to user identities.

Flexible control options: Unlike "old school" NAC products that employ heavy-handed controls and disrupt users, [REDACTED] provides a full spectrum of enforcement options that tailor the response to the situation. Resolve low-risk violations by sending the end-user a notice or automatically remediating the security problem.

802.1X authentication, or not: Choose 802.1X or other authentication technologies such as LDAP, Active Directory, RADIUS, Oracle and Sun. Hybrid mode uses multiple technologies concurrently, which speeds NAC deployment in large, diverse environments.

Built-in RADIUS: A built-in RADIUS server simplifies rollout of 802.1X. [REDACTED] can also leverage existing RADIUS servers by configuring NAC to operate as a RADIUS proxy.

### 3.4.6 Endpoint Application/Process Whitelisting

The Atos solution for Application Whitelisting is based on the [REDACTED] product. [REDACTED] prevents zero-day and APT attacks by blocking execution of unauthorized applications. Using our inventory feature, application-related files can easily be found and managed. [REDACTED] will not only block but provide real-time alerts for applications/processes not authorized for use.

#### Key Advantages

- ▶ Protect against zero-day and APTs without signature updates.
- ▶ The solution technology directly enables a check against authorized processes at the endpoint.
- ▶ Strengthen security and lower ownership costs with dynamic whitelisting that automatically accepts new software added through trusted channels.
- ▶ Whitelisting Industry level standards and baseline capabilities include:
  - Integrity checks such as hashing to ensure the application/process is in fact the authorized application/process and not a malicious or otherwise inappropriate application with the same executable name.
  - Solution will prevent unauthorized processes from executing.
  - Solution will report activity to the SIEM and identified log collection points.
  - Solution will support multiple policies/profiles that include combinations of process blocking and allowing process execution.
  - Solution will support all software deployed within the environment in accordance with the SMM.
- ▶ Aligned with change control procedures for baseline environment handled through MSI ITSM platform, this solution will be capable of notifying designated parties for approval of applications/processes that are not part of the established environment baseline.
- ▶ Efficiently control application access with [REDACTED] software, a centralized platform for management [REDACTED].
- ▶ Reduce patch cycles through secure whitelisting and advanced memory protection.
- ▶ Keep systems current with the latest patches using trusted updates.
- ▶ Enforce controls on connected or disconnected servers, virtual machines, endpoints, fixed devices such as point-of-sale terminals, and legacy systems such as Microsoft Windows XP.
- ▶ Allow new applications based on application rating or self-approval for improved business continuity.
- ▶ Maintain user productivity and server performance with a low-overhead solution.
- ▶ Easily protect legacy systems and modern technology investments.

- ▶ Atos will interface as necessary with agencies and the MSI ITSM to establish baseline and determine authorized applications/processes at the endpoint.

### 3.4.7 Endpoint File Integrity Check

The Atos solution for File Integrity Control is based on the [REDACTED] product. [REDACTED] provides the awareness to identify who and what is on the Commonwealth network. With it, Atos can address potential blind spots in the Commonwealth security architecture to defend against attacks. This is accomplished with [REDACTED] three key capabilities:

- Application Inventory and Management: See what applications and which versions are running in the environment and be able to pinpoint suspicious applications that pose a threat to the Commonwealth. Asset Inventory: See all the devices on the network, including whether or not they are protected by the [REDACTED] platform. Drill down into which assets are managed, unmanaged, or unsupported by the [REDACTED] agent to identify blind spots in the security architecture. Account Monitoring: Have visibility into all the users active in the network, their admin privileges, logon history, and password update information.

[REDACTED] provides immediate visibility of all assets, applications, and accounts, real-time and historical insight, as well as unprecedented speed and coverage. VITA can ensure compliance for user applications and account usage, while Atos can address gaps in security and investigate suspicious users and applications.

- [REDACTED] allows Atos to identify what is being utilized to ensure the best possible readiness to face attacks. By reporting unauthorized systems and applications in the environment, [REDACTED] enables Atos to improve the security posture by addressing security issues ahead of attacks.
- Detect whether unpatched or vulnerable applications are being used, so application managers can patch them before an attacker can take advantage.
- The system inventory finds unmanaged systems and systems that could be a risk on the network, such as unprotected BYOD or third-party systems.
- Monitor the usage and creation of administrator credentials across the enterprise and detect if they are being used inappropriately and out of context.

#### 3.4.7.1 File Level Encryption

The [REDACTED] software provides file level encryption services for end user desktops and removable media such as USB drives.

In accordance with the SMM, Atos' solution for Endpoint File Integrity Check will provide VITA:

- ▶ Integration into the monitoring and logging solution
- ▶ Attribute and system information will be stored in the CMDB to identify necessary device characteristics
- ▶ A list of the file names, hash value (using a VITA-approved hash algorithm) and time stamp
- ▶ Support for multi-tenancy environments and is configurable to meet specific user needs and requirements
- ▶ Monitoring of files for tampering, modifications, and deletions as well as permission changes
- ▶ Checks on all files, processes, and a baseline to be monitored
- ▶ Checks on all files, processes, and system information on a device
- ▶ Alerts in real time of agency-specified files, folders, and registries

- ▶ Dedicated technology, change control and additional capabilities to supply full timeline, comprehensive file activity reports
- ▶ Technology components available to capture user information that will be correlated to file activity

### 3.4.8 Compliance Management

Atos security leverages process, technology and tooling with established baselines that support VITA's information assurance requirements. Once in place, these baselines follow a disciplined change management process to ensure security provisioning maintains the highest integrity—no arbitrary or unrecorded configuration changes. Although the broad spectrum of people, processes, and technologies that are fused together as part of this proposal collectively address compliance management across VITA, the four key areas that address the majority of activity for compliance management are:

- ▶ [REDACTED] – Agentless Network Access Control (NAC)
- ▶ [REDACTED] – a dedicated GRC specialist that will focus on supporting security and compliance management tasks within RSA Archer.

### 3.4.9 Vulnerability Management

Atos recognizes the need and ability to consistently measure the effectiveness of a vulnerability management program. As such, Atos Cyber Security exercises a robust patch and vulnerability management program to proactively prevent the exploitation of vulnerabilities within VITA's environments. Our combination of tooling and process leverage an asset-based approach to vulnerability management that provides for maximum coverage of VITA's evolving assets.

#### IoT

A key part in protecting IoT devices is following best practices to harden the IoT device itself. It is important to run vulnerability assessments against the IoT devices to look for possible areas of exploits. At times, traditional security tools cannot be installed on IoT devices because of their limited resources and operating systems constraints. Therefore, it's important to protect the perimeter around IoT devices leveraging tools such as firewalls and Intrusion Prevention Systems (IPS). We will deploy SIEM technologies to collect logs from IoT devices to detect patterns and malicious behaviors. Host Intrusion prevention technologies, sandboxing, threat intelligence and endpoint security tools can alert to malicious activities that occur on IoT systems

### 3.4.10 Penetration Testing

Atos will partner with a 3<sup>rd</sup>-party penetration testing company to ensure an independent review of security. Atos will participate in the penetration testing program where identified and follow the procedures and requirements included in the SMM. Atos will make services available within the scope of the penetration testing program and will participate in the penetration testing program established for the environment. The penetration testing program will require participation where identified and following procedures and requirements included in the SMM.

### 3.4.11 Full Disk Encryption (Attached Device)

Atos will utilize [REDACTED] to provide VITA with the ability to centrally manage an enterprise grade encryption suite for attached devices, which will in turn reduce the loss of sensitive and confidential information across the enterprise.



██████████ is the central management console used for deployments, configuration, and management of ██████████. The initial push of the ██████████ Agent can be accomplished a few different ways, ranging from deployment over the network from ePO to insertion of the Agent into system images used for deployment.

Once the ██████████ Agent is deployed, the deployment of the Drive Encryption GO (a pre-encryption tool), Agent, and Client will be handled by ePO as a Client Task. This task can be assigned to specific systems, groups of systems, or tags, and executed according to a schedule with an optional randomized timer to reduce strain on the environment.

After the deployment and a reboot of the system, the pre-encryption tool can verify there are no other incompatible encryption solutions on the system, the drive is in good health, and there are no issues with network communication. Following the pre-encryption tests, once the proper encryption policies are applied to the system, the Drive Encryption client will begin to encrypt the drive in the background so as not to interfere with the end user. If the system turns off during the encryption process, it will continue the encryption process from where it stopped before the shutdown.

██████████ can manage solutions for multiple operating systems and applications. The same infrastructure will manage both Windows and non-Windows systems without any special design/modifications.

The Atos solution for Full Disk Encryption (Attached Device) provides the following capabilities:

- ▶ Ensures that specific files and folders are always encrypted, regardless of where data is edited, copied, or saved.
- ▶ Uses the ██████████ software infrastructure for full-disk, files, folders, and removable media
- ▶ Is certified for FIPS 140-2 and Common Criteria EAL2+ certified
- ▶ The encryption system will use industry recognized secure algorithms with a minimum of a 256-bit key capability.
- ▶ Allows for the management of native encryption functionality, which includes support for Apple FileVault OSX and Microsoft BitLocker, directly from ██████████
- ▶ The ability to lock copying of files to a removable media device automatically
- ▶ Block copying of files to a removable media device automatically, on-the-fly encryption
- ▶ Read the encrypted device on a home computer that does not have ██████████ S/W installed
- ▶ Automatically encrypt entire devices without requiring user action or training or impacting system resources.
- ▶ Identify and verify authorized users using strong multifactor authentication.
- ▶ Allows for Remote, Out-of-Band Management which will reduce VITA's operational costs
- ▶ Automatic encryption is supported without requiring any user action or training
- ▶ Provides access to encrypted data anywhere, without the need for any local software installations or administrative privileges for end-users
- ▶ Only authorized personnel will be capable of removing or disabling the encryption Software.
- ▶ The encryption system will have the capability to encrypt media and devices attached to the encrypted device.
- ▶ Provides functionality for protection during boot up
- ▶ The encryption system will allow multiple users to access an encrypted device.
- ▶ The encryption system will support various authentication methods to include but not limited to common biometric identification hardware, passwords, USB tokens, smart cards.
- ▶ The encryption system will be capable of allowing an authorized administrator without an account on the system to decrypt the device.

- ▶ The encryption system will support the ability to perform a forensic analysis of the encrypted data. The device will be able to be decrypted within the forensic software to support the forensic analysis.
- ▶ The encryption system will integrate with the existing system logon process during authentication.
- ▶ The encryption system will directly authenticate to the existing authentication services, with the capability to, authenticate with a local account.
- ▶ The encryption system will support the environments device provisioning and de-provisioning process

## 3.5 Application Security

### 3.5.1 Source Code Scanning

The Atos Source Code Scanning Solution is based on [REDACTED]. The components of this solution include capabilities for Single Application Subscription, Static and Dynamic; Single Application Subscription, Static; Single Application Subscription, Dynamic; the [REDACTED]; Software Composition Analysis; Single eLearning Seat; and Technical Service Package.

[REDACTED] provides security testing at all stages of the SDLC, including at the very beginning in the prototype coding stage to the deployment stage with multiple scanning solutions, including static, dynamic, and manual testing.

Atos will work with a designated point of contact for the specific web application for provisioning the services as well as ongoing actions for tuning. This can be network, security, app developer groups etc. (or any combination of them) from the designated Agency. Designated Agency point of contact users also can have WAF violation information emailed to them daily, weekly, or monthly, if appropriate. Each service unit comes with a specified amount of SOC hours from the cloud-based service provider.

Agencies can leverage the tool with internal developers and third-party developers. Third-party developers can leverage the [REDACTED] platform, scan their coding, and leverage our platform to help mitigate and remediate any flaws or vulnerabilities. This solution can scan the integrated development environment and providing immediate feedback during the software development phase and is capable of scanning multiple development languages including but not limited to .NET, C, C++, Java, etc. Application source code will be scanned before deployment into production and after release into production on a quarterly basis or after a significant application change.

The Atos solution can be configured to whitelist the scanners to allow them to interact directly with the application back-ends for vulnerability assessments. These assessment tool results can also be provided to the cloud-based service provider SOC to assist with WAF policy creation and/or ongoing tuning.

### 3.5.2 Vulnerability Scanning (Application Scanning suspended on MOD 23 Effective Date)

Atos will use an automated web vulnerability scanner that scans any web application or website that uses HTTP or HTTPS protocols accessible through a web browser. The scanner audits and identifies vulnerabilities, such as SQL injection, cross site scripting, etc.

#### Reporting and Monitoring (Application Scanning suspended on MOD 23 Effective Date)

- ▶ ~~Flexible reporting: Customize reports to sort by vulnerability or host, create an executive summary or compare scan results to highlight changes~~
- ~~Native (XML), PDF, HTML and CSV formats~~

- ▶ ~~Targeted email notifications of scan results, remediation recommendations and scan configuration improvements~~

### Pre-Production (Application Scanning suspended on MOD 23 Effective Date)

Vulnerability scanning will be executed across the full lifecycle from Pre-production, production, including network scanning, ~~application scanning~~ and reporting for all vulnerability scanning. All scans and report will align with the SMM process and procedures. Once any vulnerability has been addressed, we will rescan the system and notify the owner of the results. Any required remediation will follow the SMM procedures and involve the MSI and other Service Providers. Scan will encompass any applicable new Systems, devices, ~~or Application Software~~ (or any Systems or Software to be deployed in a new project). Scans will include an operating system scan, a web vulnerability scan for Web servers, and any other applicable scan types identified in the SMM. Atos will conduct pre-production consulting with the teams responsible for the assets in question on an ad-hoc basis. Atos will ensure that no System ~~or Application~~ is moved into production until any identified vulnerability is corrected or an exception has been granted.

Atos will provide the following in accordance with the SMM:

### Production

- ▶ Perform security vulnerability assessments in accordance with security requirements.
- ▶ Document and communicate the scan results and recommend remediation activities to reduce security risks.
- ▶ Coordinate and track to completion any remediation tasks related to any vulnerabilities discovered.
- ▶ Perform scheduled vulnerability scans as required by policy, statute, federal requirements and VITA Rules.
- ▶ Review scan results and identify the vulnerabilities which require remediation.

### Scanning Capabilities (Application Scanning suspended on MOD 23 Effective Date)

- ▶ Discovery: Accurate, high-speed asset discovery
- ▶ Scanning: Vulnerability scanning (including IPv4/IPv6/hybrid networks)
  - Un-credentialed vulnerability discovery
  - Credentialed scanning for system hardening and missing patches
  - Meets PCI DSS requirements for internal vulnerability scanning
- ▶ Coverage: Broad asset coverage and profiling
  - Network devices: firewalls/routers/switches (Juniper, Check Point, Cisco, Palo Alto Networks), printers, storage
  - Offline configuration auditing of network devices
  - Virtualization VMware ESX, ESXi, vSphere, vCenter, Microsoft, Hyper-V, Citrix Xen Server
  - Operating systems: Windows, OS X, Linux, Solaris, FreeBSD, Cisco iOS, IBM iSeries
  - Databases: Oracle, SQL Server, MySQL, DB2, Informix/DRDA, PostgreSQL, MongoDB
  - ~~Web applications:~~ Web servers, ~~web-services~~, OWASP vulnerabilities
  - Cloud: Scans the configuration of cloud applications like Salesforce and cloud instances like Amazon Web Services, Microsoft Azure and Rackspace
  - Compliance: Helps meet government, regulatory and corporate requirements



- Helps to enforce PCI DSS requirements for secure configuration, system hardening, malware detection, **web-application-scanning** and access controls
- ▶ Threats: Botnet/malicious, process/anti-virus auditing
  - Detect viruses, malware, backdoors, hosts communicating with botnet-infected systems, known/unknown processes, web services linking to malicious content
  - Compliance auditing: FFIEC, FISMA, CyberScope, GLBA, HIPAA/ HITECH, NERC, SCAP, SOX
  - Configuration auditing: CERT, CIS, COBIT/ITIL, DISA STIGs, FDCC, ISO, NIST, NSA, PCI
- ▶ Control Systems Auditing: SCADA systems, embedded devices and ICS applications
- ▶ Sensitive Content Auditing: PII (e.g., credit card numbers, SSNs)

#### **Application Scanning (Application Scanning suspended on MOD 23 Effective Date)**

- ▶ Scan Applications as requested by Customer to evaluate, test and recommend security maintenance activities including upgrades, patches, and fixes.
- ▶ Work with the Application's owner or external vendor to remediate Application scan vulnerability issues.
- ▶ Scan Web Applications on a frequency defined by the SMM.
- ▶ Web application scans will be completed using an approved tool designed for web application scanning

#### **Network Scanning**

- ▶ Scan network devices to identify any deviations from specified configurations, misconfigurations, or device vulnerabilities.

#### **Vulnerability Scanning Reporting**

- ▶ Flexible reporting: Customize reports to sort by vulnerability or host, create an executive summary or compare scan results to highlight changes - Native (XML), PDF, HTML and CSV formats
- ▶ Targeted email notifications of scan results, remediation recommendations and scan configuration improvements
- ▶ Report detected vulnerabilities and non-compliance issues as defined in the SMM.
- ▶ Provide an updated vulnerability scan report once every calendar month.
- ▶ Report will be available via a portal that allows filtering on required reporting areas.
- ▶ Vulnerability scan report will at a minimum include the following fields. The report will be able to sort on each field.
  - The target IP address
  - The vulnerabilities discovered
  - CVSS scores and the CVE and where applicable CWE of the vulnerabilities discovered
  - Severity level of vulnerabilities discovered
  - Description of vulnerability
  - Affected software, firmware, and/or hardware
  - Indication of whether the vulnerability is confirmed by the tool or is a potential vulnerability
  - Vulnerability identifiers
  - List of the target's open ports

- Host information such as device name, MAC address, NetBIOS name, etc.
- ▶ Each vulnerability scan report will include corresponding recommendations for remediation.
- ▶ Supplier will work with the owner of vulnerable system to advise, complete, and develop remediation plans and take any approved steps necessary to correct the issue.

### 3.5.3 Web Application Firewall

Atos will manage and operate [REDACTED] Web Application Firewall (WAF) as part of our solution for VITA and its agencies. [REDACTED] delivers advanced, continuous protection for all web applications. [REDACTED] provides bi-directional traffic analysis, automated behavioral profiling, and multiple collaborative detection engines help to quickly identify abnormal behavior, improve threat blocking and prevent outbound data leaks [REDACTED] leverages our expertise in risk and compliance management, with pre-built best practice controls and reports for compliance mandates, including PCI DSS.

#### Cloud WAF Services

**Base SVC - FQDN - 125 Mbps - Unlimited DDoS** – Includes a fixed quantity of FQDN's, Unlimited DDoS Protection, and 125 Mbps of throughput, which is measured as the greater of clean inbound/outbound traffic that will flow through the WAF. Clean bandwidth is measured at the 95th percentile, meaning the WAF omits the top 5% of traffic peaks from the calculation.

**Note:** There is currently not a tool to measure the current traffic flow in the environment. The 125Mbps is an estimate used on averages across its customer base.

Each base service requires a 36-month commitment and a minimum quantity of FQDNs. The WAF “- ADD FQDNs” RU is prorated to the end of the original 36-month commitment.

WAF is a cloud-based, managed service that detects and mitigates general, automated and application-specific security threats. The WAF service protects organizations' internet facing web applications and data, and enforces compliance with industry security standards, such as PCI DSS. The WAF service is supported by highly specialized, application security experts in the Security Operation Center (SOC).

The WAF service will use a combination of techniques and sources to determine if traffic is malicious. Attack Signature Sets to block known threats, as well as defining and enforcing custom rules based on HTTP Headers, packet payloads or and other request parameters.

Below is a sample list from our extensive library of functions available for configuration:

- IP Blacklists/Whitelists
- Network layer firewall rules
- Layer 7 DOS Profiles
- WAF Policy enforcement
- WAF Rules
- IP Reputation (optional subscription)

The WAF SOC Analysts will determine which functions are appropriate for each Agency application. The WAF service provides mitigation for attacks, by virtually patching customers applications without the need for application code changes or patches, additionally provides the customer visibility into both legitimate and malicious traffic.

The WAF is a managed security service, meaning the SOC analysts will build and maintain WAF Policies. Agencies are required to provide initial input on the application, and web server technologies to aid the SOC analysts in policy creation. VITA will be responsible to perform the necessary configurations to direct traffic to the WAF Services platform (DNS configurations).

### **Portal Account**

Each agency that utilizes the WAF service will be required to have at least one (1) portal account. The WAF service offers access to the Agency portal, via the **Portal Account RU**, for configuration and visibility purposes. The customer portal provides detailed real-time information on WAF Violations, L7 DoS events, HTTP Statistics, HTTP Error codes and more. Portal users can also create 'Custom Dashboards' that showcase relevant info based on user persona / role.

### **WAF - 10 ADD FQDNs**

Prior to Mod 21, additional FQDNs above the base service were ordered in blocks of 10. Following Mod 21, FQDNs are ordered individually.

### **WAF BASE- FQDN-Unlimited DDoS 25Mbps ADD**

25 Mbps additive bandwidth to base service.

The WAF platform also provides comprehensive DDoS mitigation for both volumetric (OSI Layer 3 and 4) and application (OSI Layer 7) attacks. The WAF service provides protection for an unlimited number of attacks with up to 1.5Gbps of attack traffic. Additionally, WAF service provides protection for one attack per year of unlimited size. If a customer receives a second attack in excess of 1.5Gbps attack traffic per year and does not have a DDoS service subscription, we will reach out and work with the customer to ensure continued protection is deployed, however the SOC is not obligated to mitigate the attack. If unlimited DDoS is chosen, WAF will provide protection for an unlimited number of DDoS attacks, regardless of attack size.

The Security Operations Center (SOC) provides 24x7 global support from within the United States,. Our WAF SOC security analysts support the ongoing availability of applications. WAF DDoS Protection service guarantees bandwidth by leveraging direct network connections with Tier 1 carriers. Our global scrubbing centers reduce the risk of a single scrubbing center from being overwhelmed by intercepting the traffic closer to the source of DDoS attacks.

WAF DDoS Protection service offers mitigation against a wide variety of DDoS attacks targeted at L3-L7 protocols.

A few of the common DDoS attacks mitigated by the service are:

- ICMP flood
- TCP SYN flood
- UDP flood
- HTTP/HTTPS flood
- DNS reflection and amplification attacks

WAF DDoS Protection service scrubs customer traffic for large volumetric DDoS attacks, typically targeted at L3/L4 protocols, and is designed to permit only clean traffic to pass to the customer networks. This service also



rate-limits the clean traffic to avoid overwhelming the customer edge network devices. Granular detection and mitigation mechanisms provide customers with flexibility in mitigating L7 DDoS attacks, without impacting the user experience.

WAF DDoS Protection service includes firewall rules that proactively block traffic to certain networks and ports. Customers can also blacklist traffic they want blocked from specific IP addresses, or they can whitelist traffic to automatically traverse the platform without mitigation.

### **3.5.4 Compliance Management**

Atos security leverages process, technology and tooling with established baselines that support VITA's information assurance requirements. Once in place, these baselines follow a disciplined change management process to ensure security provisioning maintains the highest integrity; there will be no arbitrary or unrecorded configuration changes. Although the broad spectrum of people, processes, and technologies that are fused together as part of this proposal collectively address compliance management across VITA, the key areas that address most of the activity for compliance management are:

- ▶ Application Whitelisting supported by [REDACTED] – Agentless Network Access Control (NAC)
- ▶ Information Systems Security Officer (ISSO) – a dedicated GRC specialist that will focus on supporting security and compliance management tasks within RSA Archer

### **3.5.5 Vulnerability Management**

Atos recognizes the need and ability to consistently measure the effectiveness of a vulnerability management program. As such, Atos exercises a robust patch and vulnerability management program to proactively prevent the exploitation of vulnerabilities within VITA's environments. Our combination of tooling and process leverage an asset-based approach to vulnerability management that provides for maximum coverage of VITA's evolving assets.

Atos will participate in the vulnerability management program established for the environment. This participation may require deployment, implementation, and configuration of Supplier services to provide support the vulnerability management program. The Supplier may be required to take steps such as deploy software, modify configuration, integrate with a tool, etc. to support the vulnerability management program.

### **3.5.6 Penetration Testing**

Atos will partner with a 3rd-party penetration testing company to ensure an independent review of security. Atos will participate in the penetration testing program where identified and follow the procedures and requirements included in the SMM. Atos will make services available within the scope of the penetration testing program and will participate in the penetration testing program established for the environment. The penetration testing program will require participation where identified and following procedures and requirements included in the SMM.

### **3.5.7 Access Management**

Physical Access Management - The Atos solution for physical access management will follow the SMM for Supplier. Atos physical access standards and facility hardening measures to prevent unauthorized access or damage to

facilities that contain VITA data and information processing systems and equipment align with VITA standards or greater.

Logical Access Management - The Atos solution for logical access will follow the MSI requirements as defined in the SMM. Access to log, audit trails and other data as required will be provided in accordance with the SMM process and procedures.

## 3.6 Data Security

### 3.6.1 Managed Encryption (Managed Encryption Platform suspended on April 1, 2022)

Please reference section 3.4.11 for a description of the full disk encryption services. Atos' solution for managed encryption leverages the combined capabilities of the [REDACTED] platforms. This provides a layered set of technology to meet encryption requirements for various VITA agencies architecture. The Atos Managed Encryption Solution will provide the following in accordance with the SMM:

- ▶ A third party provider approved by VITA and the Customer that is a recognized and trusted authority in the industry to generate any certificates that are used for authentication.
- ▶ Web Applications containing Confidential Information will be transmitted over encrypted channels; attempts to use the Application without encryption will be rejected.
- ▶ Confidential Data at rest will be protected by encryption.
- ▶ Private keys will be kept confidential, key lifecycle management and protect all keys in storage or in transit will be implemented.
- ▶ Keys will be chosen randomly from the entire key space and ensure that encryption keys allow for retrieval for administrative and/or forensic use.
- ▶ VITA and the Customer will receive a complete set of decryption keys. All Commonwealth data will be recoverable.
- ▶ The Commonwealth will maintain control of the encryption keys that allow access to Commonwealth data, unless otherwise specified in the SMM.
- ▶ A multi-tenant solution based on industry standard encryption standards that supports:
  - Handling keys from every major encryption algorithm, plus all the communications and exchange standards (and proprietary methods) to manage keys inside and outside the system or service location where they are stored.
  - Entitlement decisions that are derived from the identities of the entities involved. Keys will have identifiable owners (binding keys to identities).
  - Lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions.
  - Strong encryption (e.g., AES-256) in open/validated formats and standard algorithms. Keys will be maintained in dedicated a Hardware Security Module (HSM) by VITA, the Supplier or trusted key management provider under management of the Supplier.
  - Hierarchical key deployment support to create a "manager of managers" to enforce consistent policies across individual-system boundaries and throughout distributed environments.
  - Keys will be accessible by the designated users within the data owning Customer.
  - Keys will be available for individual applications and accessible by designated user(s).
  - Backup and restoration will be achieved in a secure manner.
  - Data will be protected at motion and at rest.
  - 128-bit or larger key size encryption protocol supported.

- Encryption of Web applications containing confidential information.
- ▶ Role-based access to all tenants that supports:
  - A system-admin role for administration of the key manager itself, with no access to the actual keys.
  - Limited administrator roles that allow access to subsets of administrative functions such as backup and restore, creating new key groups, etc.
  - An audit and reporting role for viewing reports and audit logs with granularity of access to certain audit logs (e.g., specific applications).
  - System/application manager roles for individual system and application administrators who need to generate and manage keys for their respective responsibilities.
  - Sub-application manager roles which only have access to a subset of the rights of a system or application manager (e.g., create new keys only but not view keys).
  - System/application roles for the actual technical components that need access to keys.
- ▶ Auditing – types of activities to audit include:
  - All access to keys
  - All administrative functions of the key manager
  - All key operations – including generating and rotating keys
  - Support for logging of all activity to a centralized log management solution.
  - Support for the real-time exporting of raw audit logging information to customer maintained systems.
- ▶ Security controls over the encryption key management process:
  - A policy enforcement framework for controlling workflow processes as well as for controlling attributes such as key lengths, validity periods, and cryptographic hash types
  - Process to quickly identifying the misuse of keys
  - Controls that prevent key-based outages
  - Automated key replacement process for fast remediation if needed
  - Full support for key archiving and recovery
- ▶ All use, storage, and/or handling of Commonwealth Data occur within the contiguous United States.

The following [REDACTED] managed encryption platform licenses will be available to meet the various needs of VITA agencies:

#### **Encryption License – File Protection**

Provides transparent and automated file-system level encryption of server data-at-rest in the distributed enterprise, including Direct Attached Storage (DAS), Storage Area Network (SAN), and Network Attached Storage (NAS) servers using CIFS/NFS file sharing protocols. The solution encrypts unstructured, sensitive data on servers, such as credit card numbers, personal information, logs, passwords, configurations, and more in a broad range of files, including word processing documents, spreadsheets, images, database files, exports, archives, and backups, and big data implementations.

#### **Encryption License – Application Layer Encryption**

Provides an API and connectivity interface for key management operations, as well as encryption of sensitive data.



Once deployed, application-level data is kept secure across its entire lifecycle, no matter where it is transferred, backed up, or copied. Using ProtectApp APIs, both structured and unstructured data can be secured in multi-vendor application server infrastructures.

**Encryption License - Database Native**

Enables the encryption of sensitive data stored in application table columns or application tablespaces, the containers for all objects stored in a database.

**Encryption License - KMIP Connector**

Provides easy integration of KMIP functionality into many customer applications by supporting multiple computer platforms, languages and APIs. This license enables the Managed Encryption Platform services to be a single, centralized platform for managing cryptographic keys and applications from disparate encryption appliances and associated keys.

**Encryption License – ProtectV**

Provides a high-availability solution that encrypts sensitive data within instances, virtual machines, as well as attached storage volumes, in virtual and cloud environments. Once deployed, the solution enables enterprises to maintain complete ownership and control of data and encryption keys by keeping it safeguarded and completely isolated from the cloud service provider, tenants in shared environments, or any other unauthorized party.

**Encryption License – Protect DB**

Provides efficient and transparent column-level encryption of sensitive data, such as credit card numbers, social security numbers, and passwords, in multi-vendor database management systems.

### 3.6.2 eDiscovery/Preservation

Atos has partnered with ePLUS to provide an eDiscovery solution using EnCase. EnCase is the gold standard in forensic security and Guidance's field-tested and court-proven solutions are deployed on an estimated 33 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide.

**EnCase eDiscovery Overview**

**Early Predictability:** Gain the earliest possible insight into the costs and scope of potential litigation through early and continuous data assessment – all before any data is collected.

**Robust Automation:** Reduce time-consuming tasks by automating custom workflows designed to collect and process potentially relevant data in a forensically sound manner – without any disruption to the business.

**Unparalleled Collections:** Meet all reasonable preservation requirements by collecting data from wherever it's stored, including email servers and document repositories – both on premise and in the cloud.

EnCase eDiscovery provides everything needed to perform continuous case assessment, an optimized process whereby legal teams can quickly glean necessary facts, both pre-and post-collection. Designed for enterprise professionals, EnCase eDiscovery provides:

- ▶ Robust, defensible, and non-disruptive collection and preservation
  - Support for collection of multiple searches to place records into a legally defensible, secured location for each legal matter.

- Log and archive all real-time communications including Email, Email attachments, Instant Messaging, Social Media, voice mail, and associated metadata in a centralized, tamper-proof environment
- Search and discover all supported document types as described in the Managed Services Manual (for example, MS Office, Adobe, HTML, zip files, etc.)
- Full binary capture
- Capable to scan encrypted storage media.
- ▶ Agile, scalable e-discovery support for any combination of cases, users, and data volumes
- ▶ Intelligent and highly efficient Central Legal Repository for secure collaboration
  - Anti-tampering checksums for non-repudiation.
  - Retrieval of stored information based on granular searches of keywords, users, time frames, and complex Boolean searches.
- ▶ Simplified oversight and management of the entire e-discovery process
  - Supports searching on content containing international languages (Unicode).
  - Accounts for name changes, aliases, and different naming conventions that may relate to the custodians being searched.
- ▶ Integration with the existing infrastructure
- ▶ Implementing litigation holds/preservation orders in a multi-tenant environment that includes all platforms, file types, and storage locations.
- ▶ This solution, via integration with the Provider's end point services, provides scans to identify viruses or malware embedded in ESI.

### 3.6.3 Certificate/Key Management

Atos' Certificate/Key Management service will provide VITA with a multi-tenant platform based on [REDACTED] consisting of the [REDACTED] that will support server certificates and mobility/end-user device certificates.

The Atos solution:

- ▶ Ensures keys protecting Commonwealth data remain in control of the Commonwealth
- ▶ Supports standard protocols and provide unique solutions for integration with current IAM (Identity and Access Management) systems through SAML integration
- ▶ Implements controls that prevent certificate-based outages
- ▶ Provides the Commonwealth with processes and tools to quickly identifying the misuse of keys and certificates
- ▶ Automates and validates the entire issuance and renewal process with policy-enforced key generation and rotation
- ▶ Remediates across thousands of certificates in just hours in the event of a CA compromise or new vulnerability such as Heartbleed
- ▶ Provides full support for key archiving and recovery by generating key material and Certificate Signing Requests (CSR) for the user, the platform can securely store a copy of the key and cert. This enables for key recovery / key escrow by authorized users
- ▶ Provides a FIPS-certified solution for active certificate management
- ▶ Enforces configurable workflow capabilities for replacement, issuance, and renewal
- ▶ Establishes certificate ownership
- ▶ Enables termination of access, thereby revoking all certificates associated to a user from any integrated source

- ▶ Enables Delegated/self-service credential management through a web-based, policy enforced self-service portal for rapid certificate requests and renewals
- ▶ Provides a policy enforcement framework for controlling workflow processes as well as for controlling attributes such as key lengths, validity periods, and cryptographic hash types

The provided platform will integrate with other components such as Certificate Authorities (CA), multi-factor authentication (MFA), and Card Management Solutions (CMS) to address:

- ▶ Open Standards based with broad support for tokens and smart cards
- ▶ Support for strong ECC (Elliptic Curve Cryptography)
- ▶ Provide keys and certificates for browsers, Web servers, smart cards, network devices, etc.
- ▶ Complete electronic ID production process, from key generation and smart card profiling to the distribution of PIN codes to the end user.

Support for both soft and a wide assortment of physical tokens Integration with National Digital IDs or private Certificate Management of any required level of assurance (LoA).

### 3.6.4 Reserved

### 3.6.5 Data Loss Prevention

██████████ protects all kinds of sensitive data—from common, fixed-format data to complex, highly variable intellectual property. By combining the inputs from these object classification mechanisms; ██████████ DLP can build a highly accurate, multi-vector classification, which is used to filter and control sensitive information and perform searches that identify hidden or unknown risks. The DLP Manager provides the ability to scan data via encrypted and unencrypted communication channels. The Customer will be able to customize scan, data loss, and remediation policies based on business needs and in compliance with VITA rules. The DLP platform provides a centralized platform integrated with the security solution which enables the appropriate process across the enterprise.

Atos' solution provides a layered approach leveraging multiple technologies for DLP. As such, the DLP solution supports on premise and hosted environments and supports integration with cloud and mobile environments. The technologies in the layered solution enable scanning of structured and unstructured data including watermark/fingerprints. This solution will also offer exact data matching, pattern matching, regex, etc. The approach utilizes latest techniques for analyzing data at rest and data in transition.

Extensive flexibility to meet VITA compliance and business needs is available through Unified DLP. The width the converge end point and network DLP technologies include agent and agentless technologies. The DLP platform will be deployed to support the process in the SMM and interfaces with the IAM solution.

The object classification mechanisms in ██████████ DLP include the following:

- ▶ Multilayer classification – Covers both contextual information and content in a hierarchical format. Dictionary and regular expression patterns.
- ▶ Document registration – Includes biometric signatures of information as it changes.
- ▶ Grammar analysis – Detects grammar or syntax of anything from text documents to spreadsheets to source code.
- ▶ Statistical analysis – Tracks how many times a signature, grammar, or biometric match occurred in a particular document or file.
- ▶ File classification – Identifies content types regardless of the extension applied to the file or compression.



The [REDACTED] DLP tool set consists of two separate components:

1. DLP Discover, is a tool that permits scanning and classification of data stored anywhere on the network. Once the data is scanned, it is flagged based on pre-established rules. There are multiple levels of classification that can be applied to any given file.
2. DLP Endpoint, permits manual flagging and classification of data, but more importantly it applies rules at each network endpoint (server, laptop, desktop) regarding what specific actions can be performed on the flagged data. For example, a rule may state that data flagged as 'sensitive' may be opened by the application it was created with, but not copied locally, not copied to a USB thumb drive, or copied to a network share; it may also state that the file cannot be appended to an email as an attachment, and that cut and paste operations are not permitted on the data. In short, this is how Data Loss Prevention is enabled.

### Incident Manager

The incident manager has three tabbed sections:

- ▶ Incident List – The current list of policy violation events.
- ▶ Incident Tasks – A list of actions to mitigate violation events on the list. They include assigning reviewers to incidents, setting automatic email notifications, and purging all or part of the list.
- ▶ Incident History – A list containing all historic incidents. Purging the incident list does not affect the history.

The Incident List tab of the DLP Incident Manager has all the functionality needed to review policy violation incidents. Event details are viewed by clicking on a specific event. Filters to modify the view or use the predefined filters in the Group By pane may be created and saved. The view may be modified by selecting and ordering columns. Color-coded icons and numerical ratings for severity facilitate quick visual scanning of events. The Incident List tab works with [REDACTED] to create reports and display data [REDACTED] dashboards.

Operations which may be performed on events include the following:

- ▶ Case management – Create cases and add selected incidents to a case
- ▶ Comments – Add comments to selected incidents
- ▶ Email events – Send selected events
- ▶ Export device parameters – Export device parameters to a CSV file (data in-use/motion list only)
- ▶ Labels – Set a label for filtering by label
- ▶ Release redaction – Remove redaction to view protected fields (requires correct permission)
- ▶ Set properties – Edit the severity, status, or resolution; assign a user or group for incident review

### Integration

DLP incidents can be integrated with the existing incident management system, which will activate the incident response program and processes. If assistance is needed to build or validate the incident response program, Atos can assist with this. If assistance is required to integrate DLP with the incident management system, Atos can also assist with this as well.

The following item is an additional option that will be made available to VITA customers upon request to allow flexibility for various agency needs:

### Cloud Access Security Broker (CASB)

The Atos Managed Cloud Access Security Broker (CASB) Service provides a comprehensive approach to cloud access security, providing pervasive cloud brokerage services for any device from any location. For VITA, Atos has prepared a service program that consists of the foundational service component of Infrastructure as a Service (IaaS) Monitoring, Shadow IT and 5 supported Software as a Service (SaaS) applications.

The service architecture consists of the:

- Cloud Dashboard (Upper environment)– the single pane of glass for management of the CASB Service
- Enterprise Collector (EC) (Lower environment) - on-premises software service that provides an integration point between CASB provider and the enterprise network. The EC is deployed either centrally or distributed based on the network topology.

### **IaaS**

With Atos delivered Cloud IaaS Security Monitoring, Atos provides a comprehensive CASB service, providing visibility into user activity, compliance and governance policy enforcement, and threat protection.

With Cloud IaaS Security Monitoring, Atos will assist VITA with:

- Audit and Monitor IaaS Resources for Misconfiguration
- Automate Policy Corrections
- Prevent Data Loss with DLP
- Capture Custom App Activity and Enforce Controls
- Detect Malicious User Activity and Behavior
- Detect and Remove Malware
- Discover Rouge IaaS Services and Accounts
- Identify Provisioned User Risk (Over-Provisioned, Inactive)
- Enrich Native Cloud Platform Forensics
- Manage Multiple IaaS Providers

### **Shadow IT**

Shadow IT provides visibility into the cloud services employees are consuming. In most organizations, Cloud services have been provisioned by users or departments within an organization without the knowledge or consent of the IT department, the resulting application sprawl causes the enterprise considerable challenges from a risk and compliance standpoint. Atos CASB service assists by discovering Shadow IT and helping the enterprise understand their exposure.

With Shadow IT, Atos will assist VITA with:

- Discovery of all cloud services in use, their access counts, security risks, and usage trends over time,
- Gaining granular visibility into user activity with the ability to block high-risk activities,
- Detect and remediate policy enforcement gaps arising from proxy leakage
- Enforce acceptable use of cloud governance policies based on cloud service security risk.

### **SaaS**

With Atos delivered Cloud Sanctioned IT Software as a Service (SaaS), we provide a comprehensive CASB service, providing visibility into user activity, compliance and governance policy enforcement, and threat protection.

With Cloud Sanctioned IT, Atos will assist VITA with:

- Preventing the unauthorized sharing of sensitive data in SaaS outside the organization

- Detect and remediate compromised accounts, insider threats, and privileged user threats
- Prevent regulated data from being stored in SaaS to meet compliance requirements
- Capture a complete audit trail of all user and administrator activity for forensic investigations
- Block the download/sync of corporate data stored in SaaS to personal devices
- Enforce policies that permit access to corporate SaaS accounts while preventing personal access.

### 3.6.6 Data removal / device disposal

The Atos Cyber Security ISSO supports the VITA Information Security Program through adherence to NIST Special Publication 800-88 in meeting the challenges of data removal and device disposal. Atos follows SEC 501 for data removal and sanitization. The data removal and sanitization process will be subject to audit and in-person review. Data removal and sanitization will be performed according to the data classification requirements. Cyber Security resources, applications and tooling, by design, do not capture or host any customer data. Actionable threat and vulnerability hinges on searches and checks containing data points that are not sensitive in nature. Security activities centered on sensitive engagements are conducted on VITA owned/provided devices and by default fall inside of VITA's Data removal and device disposal.

Atos owned or hosted systems will be aligned to the VITA information system lifecycle and are labeled in reference to security categories (and as presented in FIPS Publication 199) of High, Medium or Low each system will receive the aligned requirement for media sanitization when being introduced or removed from the VITA environment. When media is repurposed or reaches end of life, it will be disposed of leveraging VITA's existing sanitization methodology (clear, purge or destroy) or Atos will undergo necessary steps to implement a methodology commensurate with Commonwealth security standards, VITA Rules, and the SMM. Commonwealth data will be removed and sanitized from any system containing the data; this includes wiping of virtual systems. All Atos leveraged media on behalf of VITA will be met with this requirement. This includes the careful deployment of "Cryptographic Erase" which, if leveraged "after" a device stores data is of little value. Documentation will be provided and made available documenting the data removal and sanitization.

### 3.6.7 Enterprise Remote Access

Enterprise Remote Access is a full-spectrum, cloud-based secure access service edge product. For remote users, Enterprise Remote Access provides secure remote access to applications and services based on zero trust network access control policies. For remote networks, Enterprise Remote Access provides access to both VITA enterprise resources and third-party resources.

Atos will provide the day-to-day monitoring and analysis as well as administrative services. The operations consist of the following discrete activities:

- ▶ Platform support
- ▶ Platform maintenance and upgrades
- ▶ Policy Management
- ▶ Report Generation
- ▶ Add, remove and change access based on tickets
- ▶ User based access
- ▶ Machine based access
- ▶ Application based access



- 
- ▶ Assist with incident resolution
  - ▶ Open Incident cases
  - ▶ Troubleshoot and resolve access issues
  - ▶ Execute current practices and procedures
  - ▶ Integration of the SIEM (Security Information and Event Management) with the [REDACTED] Data Lake event log repository
  - ▶ Support of Security Operations for incident investigation and response
  - ▶ Implement Site-to-Site VPN connections for VITA-approved Agency sites to provide secure connectivity in support of the Enterprise SD-WAN service.
  - ▶ For Clarity:
    - Agency Configuration Fee – This charge will only be applied to a new Agency that is not identified as part of the [REDACTED],
    - Connection Implementation Fee – This charge will apply for each agency, per connection implemented for the [REDACTED] connection. Request is required to be submitted for each connection an agency will require. If multiple [REDACTED] connections are required for an agency at a specific site, a request will be required and this charge will apply for each connection implemented.
    - Connection Change Fee – Is applicable, for a customer generated change, any time after the tunnel has been installed.
    - For clarification – All tunnels implemented as part of the SD WAN RFS are subject to the Third-Party Network Maintenance monthly charge which becomes effective at the time of installation.