PANOPTES

SuprTEK PanOptes™ Continuous Monitoring Platform

Superlative Technologies, Inc. dba SuprTEK | 45195 Research Place, Ashburn, VA 20147 | www.suprtek.com

Introduction

Today's government IT system owners are faced with having to manage the security posture of their systems and maintain acceptable levels of risks in a constantly evolving environment with limited time and resources.

Valuable time and resources are spent using manual processes and disparate tools to support four major functional areas that form the foundation for government information systems security practices:

- Inventory and Configuration Management
- Certification and Accreditation
- Vulnerability Management
- Compliance and Reporting

INVENTORY AND CONFIGURATION MANAGEMENT

Within large organizations, system owners often struggle with an inability to determine what is really deployed across the organization's enterprise IT landscape due to a lack of comprehensive and up-to-date inventory and configuration management of IT assets, e.g. devices, software, systems, and networks.

As a result, system accreditations are not properly maintained as the systems change and configuration management is rarely accomplished in a manner that maintains the security posture of the systems or updates the system security artifacts when changes are made. These problems are further exacerbated when system operators and administrators are inundated with requirements to securely configure and patch operating systems, applications, peripherals, and network devices without the necessary insight to plan and prioritize these actions.

CERTIFICATION AND ACCREDITATION

The Federal government's certification and accreditation processes that approve systems to go live on production networks is a lengthy and arduous endeavor with hundreds of man-hours spent each year on a system to select and validate against government and industry best practice-based security controls, e.g. NIST 800-53, DISA STIGs, CAG 20 Critical Security Controls, etc.

Systems are only reassessed annually or when there are significant system modifications, leaving system owners with out-dated and oftentimes inaccurate information to gauge compliance and the overall system security posture, putting their enterprises at risk. This problem is further compounded when Plans of Actions and Milestones (POA&Ms) are created on those security controls allowing system owners to defer corrective actions. The POA&Ms further obscure the true security posture of a system since they are often extended and are infrequently updated.

VULNERABILITY MANAGEMENT

Each day hundreds of vulnerability alerts and security advisories are issued by hardware and software vendors as well as various Computer Emergency Response Team (CERT) organizations but system owners and administrators lack the ability to properly prioritize these vulnerabilities based on how pervasive they may be across the enterprise and their potential operational impact.

As a result they're left trying to patch everything and are continuously playing catch-up with patching their systems against newly discovered vulnerabilities. In addition, countless hours are spent manually creating reports, which are often inaccurate and out-of-date, to identify assets that are vulnerable vs. those that have been remediated or mitigated.

COMPLIANCE AND REPORTING

System owners are faced with many directives, policies, and regulations to continually report compliance results and other security posture-related information. Many organizations still use processes that rely on manual reporting procedures that are resource intensive, slow, and inaccurate.

As a result, valuable system and security engineers' time spent on manual reporting processes detract from their ability to rapidly respond to threats on the network.

Continuous Monitoring Overview

To alleviate these challenges, information assurance and cyber security practioners have been converging around and evolving a set of best practices known as "Continuous Monitoring".

The National Institute of Standards (NIST) defines Continuous Monitoring as "***… a risk management approach to Cybersecurity that maintains an accurate picture of an organization's security risk posture, provides visibility into assets, and leverages use of automated data feeds to measure security, ensure effectiveness of security controls, and enable prioritization of remedies.***"

This is oftentimes supported through the use of tools and techniques that leverage NIST's Secure Content Automation Protocol (SCAP) standards such as the eXtensible Configuration Checklist Description Format (XCCDF), Open Vulnerability and Assessment Language (OVAL), Common Platform Enumeration (CPE), and Common Vulnerabilities and Exposures (CVE) to continuously and automatically capture inventory and configuration data, determine exposure to vulnerabilities, and assess compliance against required patches and security policies. These capabilities capture the necessary information on system security posture to support certification and accreditation and enable automated reporting.

SuprTEK has been at the forefront of Continuous Monitoring, working with and integrating technologies and standards from organizations such as the Defense Information Systems Agency (DISA), National Institute of Standards (NIST), National Security Agency (NSA), United States Cyber Command (USCYBERCOM), and Department of State (DoS)—all of whom have been pioneering advances in Continuous Monitoring approaches and technologies.

From this experience we have developed a Continuous Monitoring Reference Model that defines the supporting capabilities at both the operational and system perspectives, depicted in Figure 1 and described in Table 1.

PANOPTES

FIGURE 1

Continuous Monitoring Reference Model

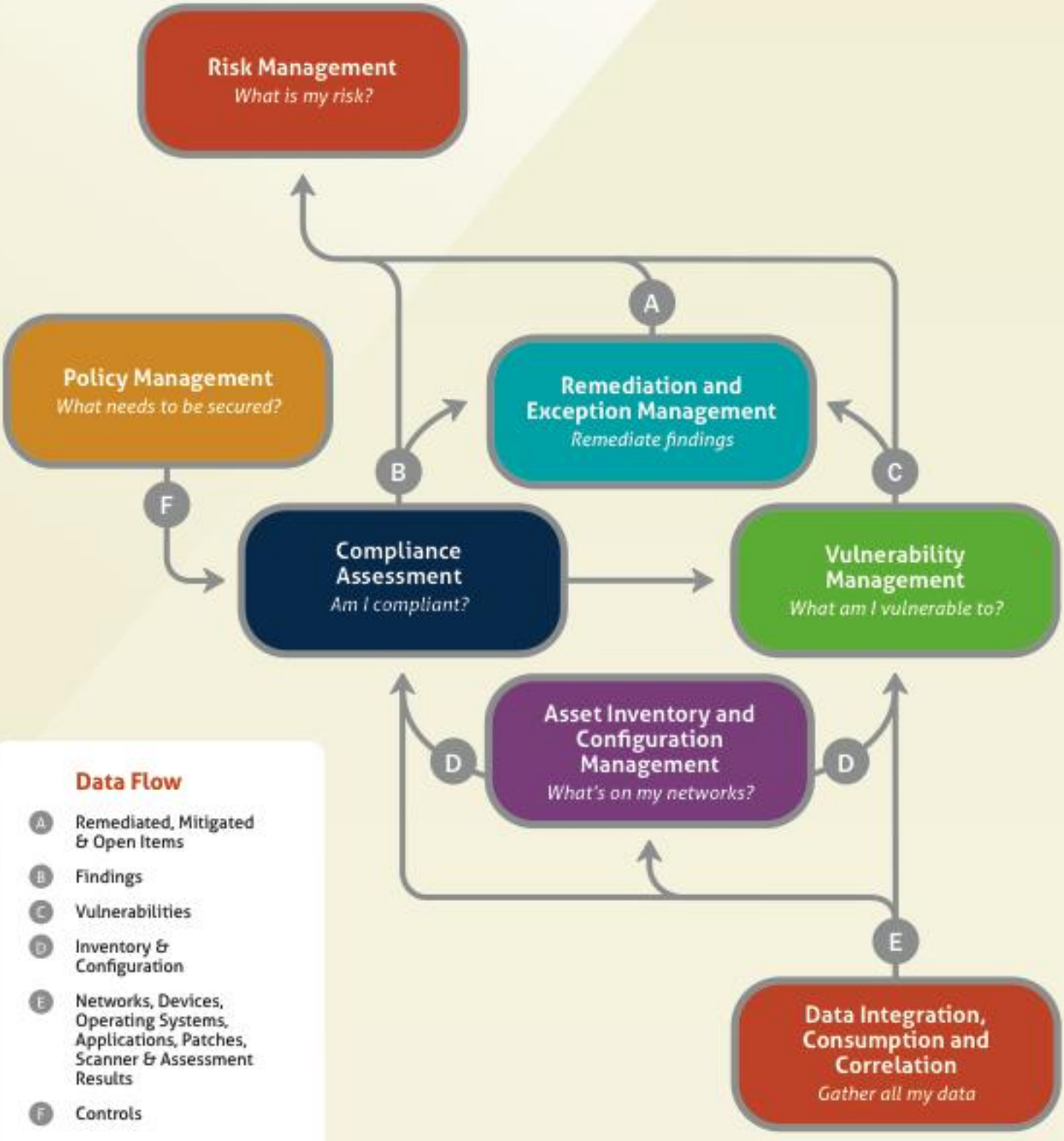

TABLE 1

Supporting Capabilities in the Continuous Monitoring Reference Model

SYSTEM / OPERATIONAL CAPABILITY	DESCRIPTION
Policy Management *What Needs to Be Secured*	Policy management supports creation and management of the policies that define what needs to be secured across the enterprise.
Data Integration, Consumption, and Correlation *Gather All My Data*	Data integration, consumption, and correlation supports gathering information about an enterprise's IT assets that often reside in a variety of disparate systems.
Asset Inventory and Configuration Management *What's On My Networks*	Asset inventory and configuration management utilizes all the data that has been gathered to provide an accurate and up-to-date understanding of what's deployed on the networks.
Compliance Assessment *Am I Compliant*	Compliance assessment utilizes asset inventory and configuration management as well as other audit and scan data to determine if assets are compliant against enterprise security policies.
Vulnerability Management *What Am I Vulnerable to*	Vulnerability management identifies which assets are exposed to what vulnerabilities and helps to prioritize vulnerabilities based on their potential impact to the enterprise.
Remediation and Exception Management *Remediate Findings*	Remediation and exception management supports the remediation/mitigation of non-compliant items and vulnerabilities as well as providing the capabilities to define exceptions and defer fix actions, e.g. POA&Ms.
Risk Management *What's My Risk*	Risk management scores the enterprise based on overall security posture and risk using information on what's been fixed, what hasn't been addressed, and operational impact as well as taking into account what's unknown.

DoD-Wide Continuous Monitoring Solution

During the past several years SuprTEK has been working with DISA's Program Executive Office for Mission Assurance (PEO-MA) to develop and field a highly scalable Continuous Monitoring platform that enables USCYBERCOM and other DoD Enterprise level users to monitor and analyze the security posture of millions of devices deployed across the DoD's networks.

Our solution provides comprehensive capabilities based on the Continuous Monitoring Reference Model described above, leveraging expertise and technologies incubated from pioneers in Continuous Monitoring, e.g. NSA, DoS, NIST.

This system supports PEO-MA's objectives of enabling a defendable Global Information Grid (GIG) and improving cyber readiness by automating the processes to securely configure the assets on the GIG, enhancing perimeter defenses through secure configuration of perimeter devices such as firewalls and routers, and providing the accurate up-to-the-minute insight necessary for cyber situational awareness and command and control (C2).

PANOPTES

FIGURE 2

Continuous Monitoring and Risk Scoring System Architecture

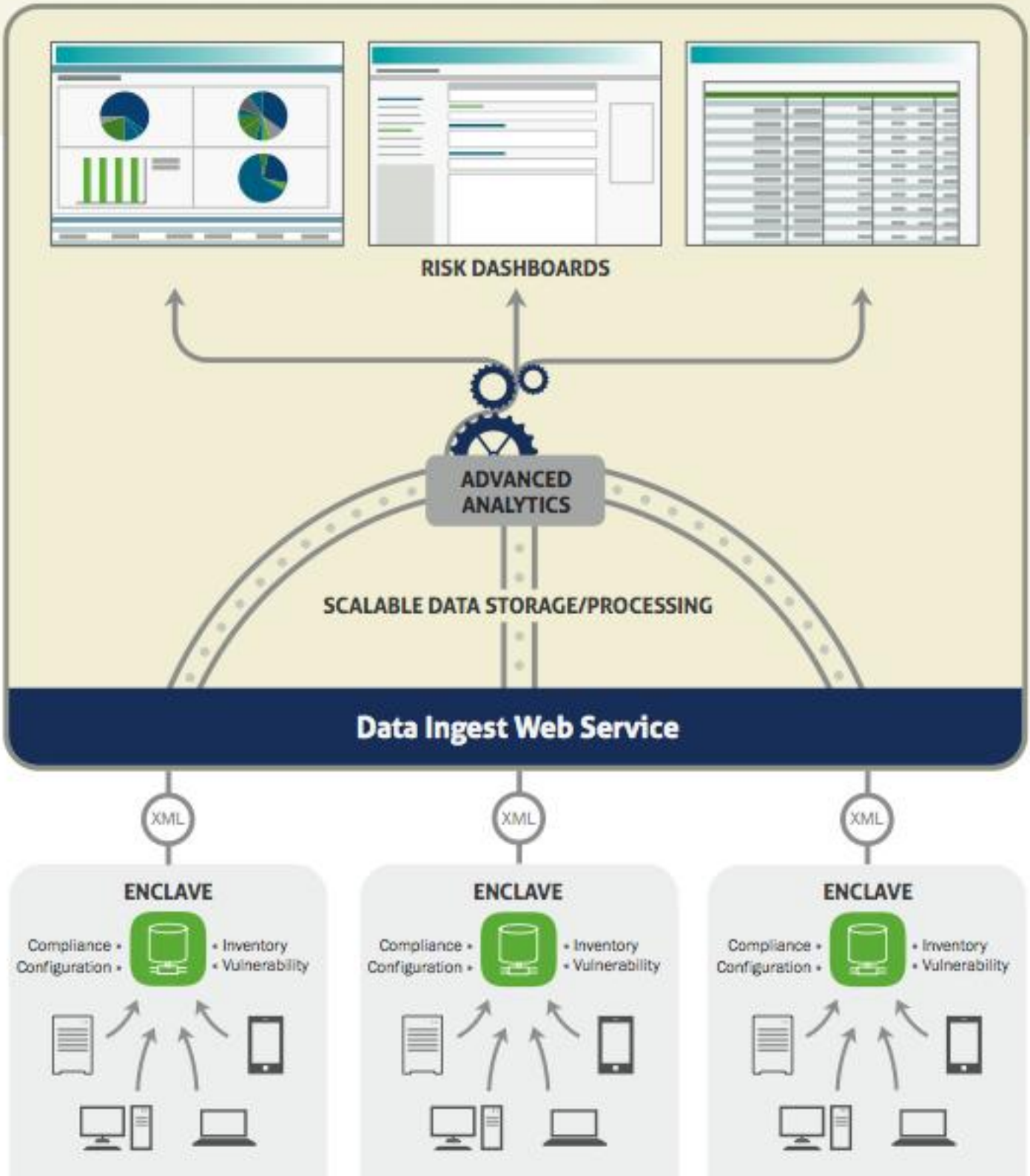

TABLE 2

Unique Features of SuprTEK's DoD Enterprise-Wide Continuous Monitoring Solution

UNIQUE FEATURES	EXAMPLES
State of the Art Capabilities *Developed from U.S. Government pioneers in continuous monitoring technologies*	NIST SCAP; DOS iPost/PRSM; DHS CAESARS; NSA/DISA ARCAT, ARF, ASR
Direct Support *For DoD/Federal policies for continuous monitoring*	Support for current and upcoming USCYBERCOM, DoD, DISA, and other Federal policies and processes built directly into the solution
Seamless Integration *With other DoD enterprise cyber security tools*	E.g. Host-Based Security System (HBSS), Assured Compliance Assessment Solution (ACAS), Vulnerability Management System (VMS), Digital Policy Management System (DPMS), etc.
Breadth and Depth *Of monitoring and reporting*	Ability to monitor at a macro-level across an enterprise (millions of devices) to detect patterns and systemic problems and drill down to individual devices for remediation
Federated Model *To support hierarchical compliance reporting requirements common in government organizations*	Summary- and metrics- level reporting at the enterprise level and device-level details for internal reporting and tracking

SuprTEK's Continuous Monitoring Platform: *PanOptes™*

PanOptes™ from SuprTEK is a commercial Continuous Monitoring platform that we have developed leveraging the best practices, lessons learned and technologies from our experience developing and fielding the DoD's solution for Continuous Monitoring.

The result is a product with capabilities that are unparalleled in:

- Scalability to monitor millions of assets
- Breadth and depth of situational awareness
- Advanced analytics to identify systemic issues and pinpoint problematic assets
- Support for stringent DoD-level security requirements
- Alignment with the Federal Government's policies and best practices for Continuous Monitoring

Subsequent paragraphs below describe the key capabilities of SuprTEK's PanOptes™ in the context of the Continuous Monitoring Reference Model.

RISK MANAGEMENT

PanOptes™ provides Risk Management by scoring an enterprise's overall risk level based on risk scoring best practices developed at Department of State and refined at the DoD.

Quantify the risk across enterprise IT assets by scoring them based on key metrics such as how many vulnerabilities they're potentially exposed to, how many

Risk Management

- Hierarchical risk scoring based on best practices established at Department of State
- Rollup and drilldown scores along multiple custom-defined hierarchies
- Rich visualization risk scoring dashboards showing graded, average, raw scores, and historical trending
- Customizable risk scoring algorithms

vulnerabilities have been remediated/mitigated, how current the anti-virus signature files are, number of open findings against enterprise security policies, how often scans are executed and results being reported.

POLICY MANAGEMENT

PanOptes™ enables an enterprise to define how its assets should be secured through Policy Management. Import standard security policies from DoD, NIST, and others using the XCCDF standard. Build custom policies to support unique security requirements of an enterprise. Not all policies apply to all assets so PanOptes™ provides rich selection criteria to assign specific policies to selected populations of an enterprise's assets.

REMEDIATION AND EXCEPTION MANAGEMENT

Identifying enterprise risks, compliance issues, and vulnerabilities is only half the battle. These findings have to be remediated or mitigated. PanOptes™ provides the capabilities to disseminate guidance and directives to address the findings as well as to track that the necessary corrective actions have been executed. In some cases, the amount of effort to fix a non-compliance finding or remediate a vulnerability far outweighs the risk that they pose, thus organizations need to be able to accept the risk and move on. In other cases, some security controls may not apply to certain assets due to some unique characteristics about that asset and thus organizations need to mark those as exceptions so that those assets aren't inaccurately assessed against those controls. PanOptes™ provides the capabilities for both risk acceptance and defining exceptions for policies.

Policy Management

- Custom Policy Builder
- Import policies and vulnerability alerts from other sources
- Assign relevant policies to selected assets

Remediation and Exception Management

- Disseminate information on remediation guidance and desired state across the enterprise
- Track and report on remediation actions
- Define exceptions for policies and compliance findings
- Report on exceptions at the enterprise, organizational or asset level

COMPLIANCE ASSESSMENT

Assess how well the enterprise and individual departments are implementing security policies using comprehensive Compliance Assessment capabilities provided by PanOptes™. Assess against standard security policies that have been imported or custom policies defined using Policy Management. PanOptes™ consumes assessment results from SCAP-compliant scanners and provides rich visualizations and reports to reveal enterprise compliance levels as well as identify non-compliant departments and assets.

VULNERABILITY MANAGEMENT

Organizations are flooded with a deluge of vulnerability alerts daily. PanOptes™ provides the capabilities to prioritize them and address them in a systematic manner by assessing the potential exposure across an enterprise's asset population. Thus enterprise's can first address the vulnerabilities that impact the largest population of assets or the ones that impact the assets that are most critical to the enterprise's mission. In addition, issue guidance to remediate or mitigate such vulnerabilities, track that these actions are executed across the enterprise in a timely manner, and use metrics gathered on affected and fixed assets to calculate the enterprise's overall risk.

ASSET INVENTORY AND CONFIGURATION MANAGEMENT

Know exactly what is deployed across the enterprise with PanOptes™' Asset Inventory and Configuration Management capabilities. When a zero-day vulnerability is discovered that affects a specific version of a popular program, determine your potential exposure by pinpointing exactly what assets across the enterprise are running that program. Use operational metadata tagged to those assets to determine how mission critical those assets are as well as to identify the departments and administrators responsible for securing them.

Compliance Assessment

- View enterprise, organizational, and specific asset compliance against security policies
- Custom reports and ad hoc queries against policy compliance results
- Pinpoint problematic organizations and assets
- Integrates with any SCAP-compliant policy scanner using XCCDF/OVAL standards
- Calculate risk based on compliance results

Vulnerability Management

- View enterprise, organizational and specific asset vulnerability metrics
- Import vulnerability alerts
- Identify affected and fixed assets
- Custom reports and ad hoc queries against vulnerability metrics
- Pinpoint problematic organizations and assets
- Calculate risk based on vulnerability metrics

Asset Inventory and Configuration Management

- View enterprise, organizational and asset-level details on hardware/software inventory and configurations
- Manage inventory by custom-definable hierarchies
- Custom reports and ad hoc queries against inventory and configuration data
- Assign operational metadata to assets

DATA INTEGRATION, CONSUMPTION, AND CORRELATION

Enterprises use a variety of tools to manage their IT assets and infrastructure and all of them contain valuable data that plug into the equation of "how risky is my enterprise?" PanOptes™ provides a massively scalable SOA-based integration framework for consuming and correlating that data. This framework provides the underlying foundation for the higher level capabilities that answer questions regarding inventory and configuration management, vulnerabilities and compliance, and ultimately overall risk for the enterprise.

Data Integration, Consumption, and Correlation

- Service-Oriented Architecture (SOA)-based publish/subscribe framework for data integration
- Integrates with SCAP-compliant data sources using XCCDF, OVAL, CPE, CVE, ASR, ARF standards
- Correlation of asset data from multiple sources

TABLE 3

Why PanOptes?

PanOptes™ provides improved time to value and rapid return on investment by lowering your enterprise security costs through automated continuous monitoring and enabling you to prioritize your investments to focus on the most critical risk areas. Table 3 summarizes the key features and benefits of the PanOptes™ Continuous Monitoring Platform.

FEATURES	BENEFITS
Scalability to monitor millions of assets	Multiple architectural options to support organizations of various sizes – from small to medium (less than 100,000 devices) to very large (over 2 million devices)
Breadth and depth of situational awareness	Visibility into risk metrics at the enterprise, department, and individual asset level Detect patterns and systemic problems across the enterprise and drill down to individual devices for remediation
Advanced analytics	Risk scoring algorithms customized to your enterprise environment presented through rich dashboards, ad hoc queries, and reports Slice and dice risk metrics across multiple dimensions for root cause analysis
Support for stringent DoD-level security requirements	Up-to-date compliance policies and vulnerability alerts imported from multiple sources Current and forthcoming USCYBERCOM, DoD, DISA and other Federal polices and processes built directly into the solution
Alignment with Federal Government policies and best practices for continuous monitoring	Leverage state-of-the-art continuous monitoring technologies pioneered by key US Government security experts to improve the security posture of your enterprise

Conclusions and Summary

Maintaining a strong security posture and managing the risks of IT systems in today's environment present many challenges. Continuous Monitoring is emerging as a set of best practices that promise to alleviate many of these challenges and streamline the processes that system owners have to undertake to secure their systems.

SuprTEK's PanOptes™ Continuous Monitoring Platform built leveraging the best practices, lessons learned and technologies from our experience developing and fielding an enterprise-wide solution for the DoD provides the robust capabilities that your organization needs to implement your own Continuous Monitoring program. In addition, SuprTEK's Information Assurance specialists and security architects have the necessary experience and expertise to provide the support services that will help you get your continuous monitoring program off the ground, improve existing processes that you have in place, or provide targeted support with specific phases of the continuous monitoring lifecycle.

About SuprTEK

Since 1996, SuprTEK has provided innovative services in technology strategy and architecture, cyber security, enterprise IT solutions engineering and delivery, managed IT service operations, and healthcare IT solutions.

SUPRTEK

SuprTEK supports over a dozen enterprise cyber security solutions for Department of Defense (DoD) customers, some implemented across more than 4 million systems and devices. SuprTEK continuously engages in the research and development of new and emerging solutions focused on improving the security posture of our clients' critical IT assets.

PANOPTES

For more information on the PanOptes™ Continuous Monitoring Platform or how SuprTEK can assist you with your Continuous Monitoring program, contact us at:

Phone: (703) 564-2012 | Email: continuous.monitoring@suprtek.com