SUPRTEK

Continuous Monitoring Product and Capabilities

January 2013

PANOPTES

Contents

- What Are the Challenges?
- How Continuous Monitoring Can Help
- SuprTEK's Continuous Monitoring Experience
- Overview of SuprTEK's PanOptes Continuous Monitoring Platform

What are the Challenges?

Today's system owners have 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:

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

Certification and Accreditation Challenges

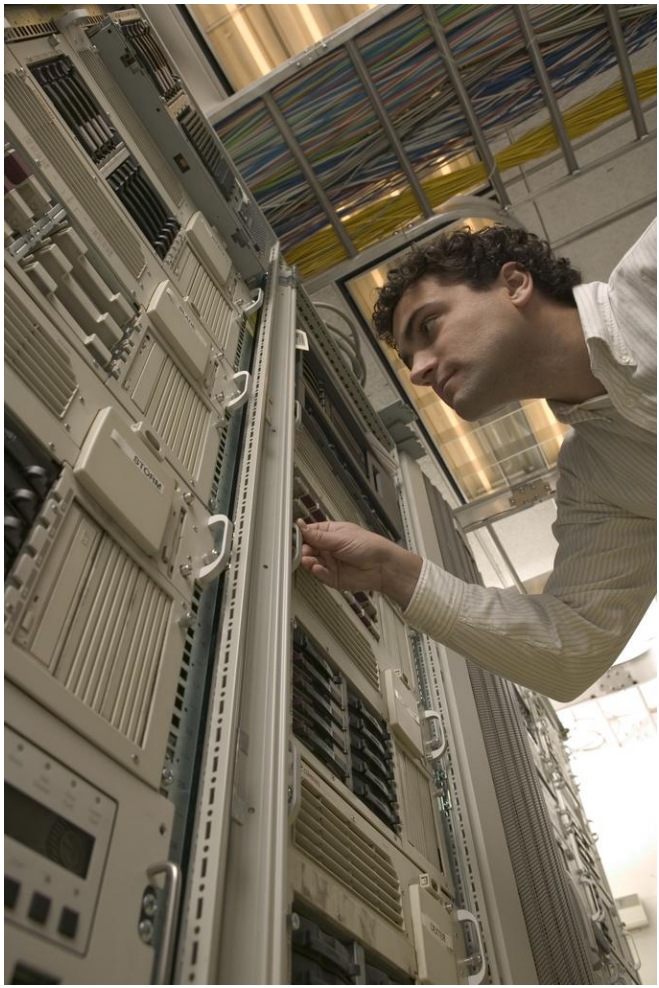
- *Hundreds of man-hours spent each year on a system to select, assess, and monitor against security controls*
  - NIST 800-53
  - DISA STIGs
  - CAG Top 20
  - Etc. …
- *How often do you actually monitor and reassess against selected controls?*
- *Dysfunctional POA&M processes*

Vulnerability Management Challenges

- *Hundreds of vulnerability alerts issued each day …*
  - Which ones need immediate attention?
  - How pervasive is this vulnerability across my enterprise?
  - What's the potential operational impact?
- *Time intensive manual tracking and reporting*
  - Affected assets
  - Remediated assets
  - Mitigated assets
  - Open assets

Inventory and Configuration Management Challenges

- *What's really deployed across the enterprise?*
  - Hardware
  - Software
  - Patches
- *How are the systems configured?*
- *System administrators constantly inundated with requirements to lock down and patch*
  - Operating systems
  - Databases
  - Applications
  - Network devices



Compliance and Reporting Challenges

- *Endless directives, policies, and regulations for reporting and compliance*
- *Manual reporting procedures that are resource intensive, slow, and inaccurate*

- *Lack of unified enterprise-wide visibility into security posture of systems and networks*
- *Too much time spent on reporting rather than actually trying to respond to threats on the networks*

Continuous Monitoring to the Rescue …

SUPRTEK

NIST SP 800-137:

"Information security continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."

NIST IR 7756:

"Continuous security monitoring is 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."

SuprTEK's Continuous Monitoring Experience

- 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)

- Since 2010 SuprTEK has been working with DISA PEO-MA to develop and field the Department of Defense's Continuous Monitoring and Risk Scoring (CMRS) system 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.

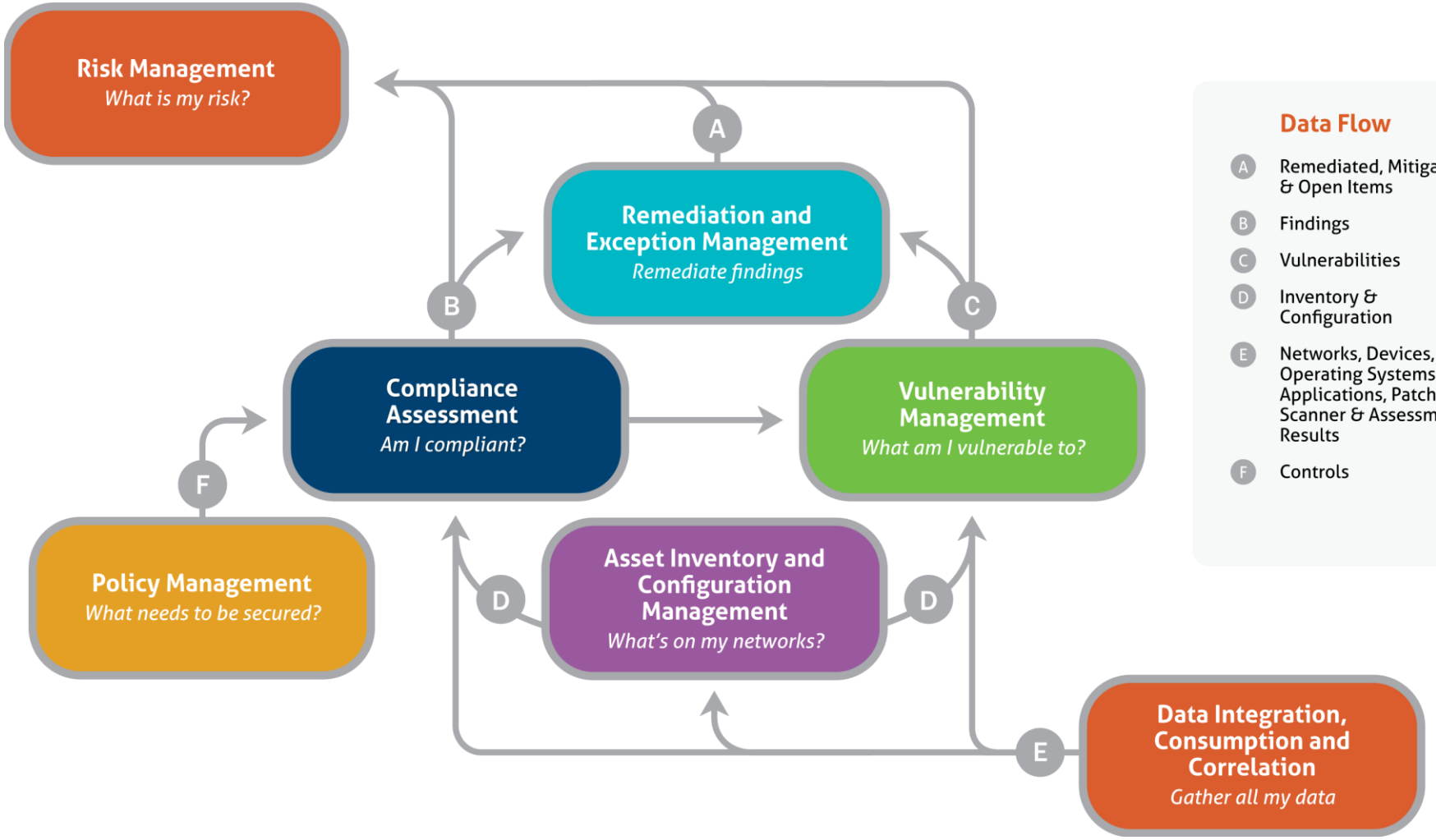
Transforming and improving the DoD's cyber security processes …

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

Improving security posture and reducing costs through continuous monitoring automation.

- CMRS utilizes SCAP standards such as XCCDF, OVAL, CPE, and CVE to continuously and automatically determine whether an asset is susceptible to vulnerabilities, its compliance level against required patches, and compliance against IAVAs, STIGs, and other enterprise security policies.

SuprTEK's Continuous Monitoring Reference Model



Reference Model Capabilities

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.*
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.*
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.*
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.*
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.*
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 f what's deployed on the networks.*
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.*

Introducing SuprTEK PanOptes

- A highly scalable platform developed specifically to address Defense, Intelligence, and Federal agencies' requirements for continuous monitoring; e.g. risk, vulnerability, compliance, inventory and configuration management

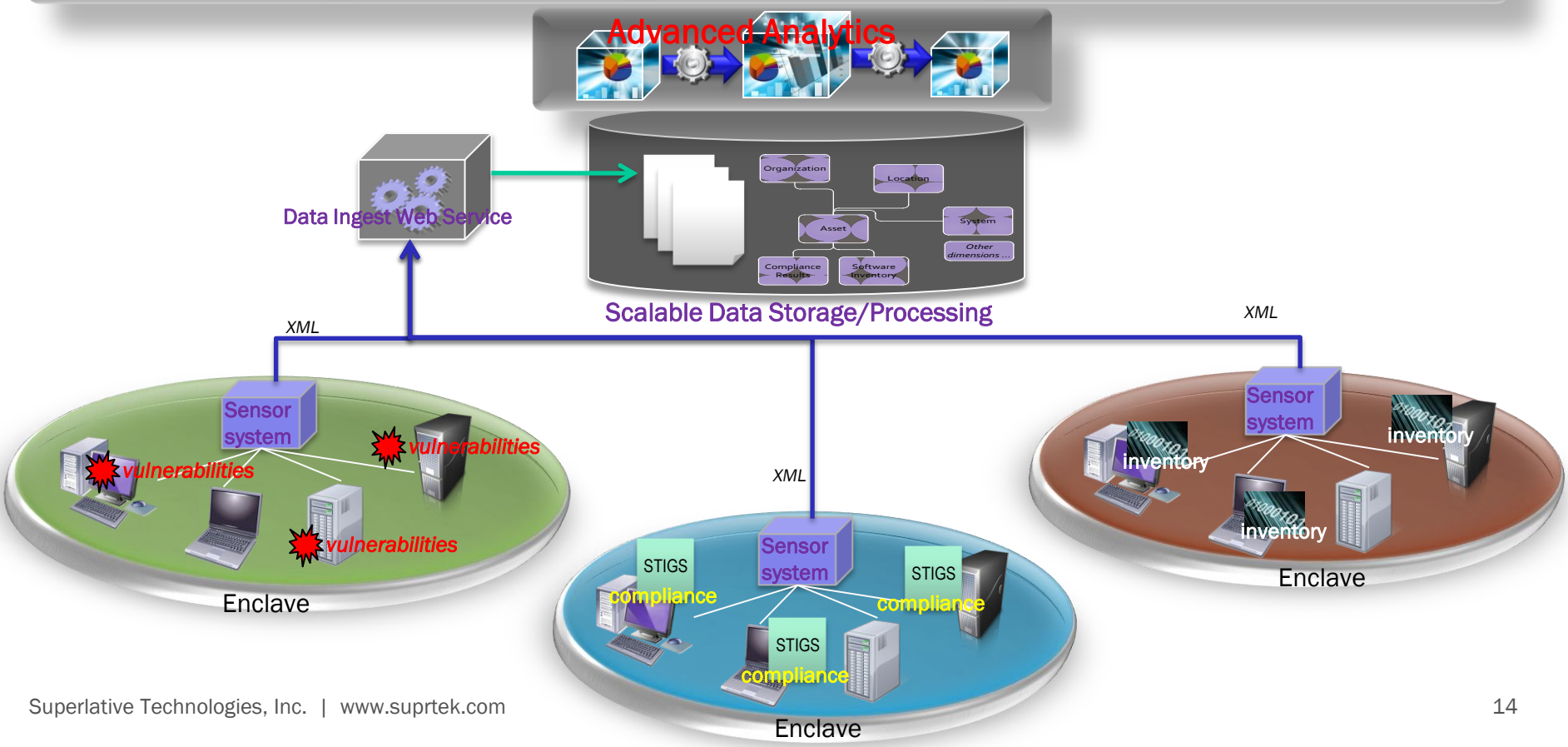
- Developed leveraging expertise and technologies incubated from collaboration with pioneers in continuous monitoring
  - Defense Information Systems Agency (DISA)
  - United States Cyber Command (USCYBERCOM)
  - National Security Agency (NSA)
  - Department of State (DoS)

PANOPTES

Unique Features and Benefits

- **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 policies for continuous monitoring**
  - As we work with USCYBERCOM and DISA to define and pilot the policies and processes, we'll build the capabilities to support them directly into the product
- **Seamless integration with other DoD enterprise cyber security tools**
  - E.g. HBSS, ACAS, Flying Squirrel, eMASS, VMS, 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
- **Support for federated compliance reporting requirements common in government organizations**
  - Summary- and metrics- level reporting at the enterprise and device-level details for internal tracking

PanOptes Continuous Monitoring Architecture



PanOptes' Capabilities

SUPRTEK

Policy Management	• Custom policy builder • Import policies and vulnerability alerts from other sources • Assign relevant policies to selected assets
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, and raw scores • Customizable risk scoring algorithms
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
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
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
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	• 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 • Scalable backend architecture to support processing and reporting on millions of devices

Advanced Risk Scoring Algorithms

SUPRTEK

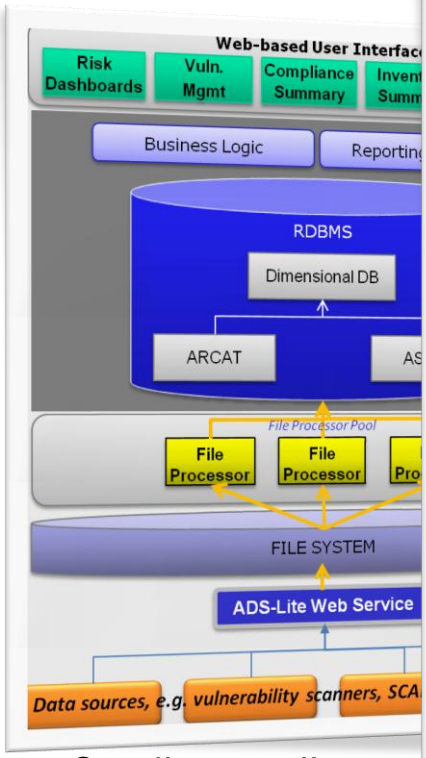
Eight score components across four categories of security controls

Security Control	Score Component		Description
Malware Defenses	AVR	Anti-Virus Reporting	Score based on how recently the device has completed and reported an anti-virus scan
	AVS	Anti-Virus - Up-to-date	Score based on currency of .DAT file versions on anti-virus software
Vulnerability Mgmt	IAR	IAVM Reporting	Score based on how recently the device has completed and reported a vulnerability scan
	IAV	IAVM Compliance Results	Score based on calculated IAVM compliance of the device
Secure Configuration	SCR	Security Compliance Reporting	Score based on how recently the device has completed and reported a policy scan
	SCM	Security Compliance	Score based on Benchmark/STIG and Benchmark/IAVM compliance of the device
Standard Operating Environment	SOR	SOE Reporting	Score based on how recently the device has completed and reported a SOE compliance scan
	SOE	Standard Operating Environment Compliance	Score based on compliance of the device against SOE product and version

- Based on Department of State's risk scoring best practices
- Adapted to support DoD requirements
- Highly customizable
  - Additional score components
  - Scoring formulas
  - Risk weights
  - Grade ranges
- Calculated at the device level, can be aggregated up multiple hierarchies to any level
- Slice and dice against multiple dimensions (*owning/administrating/ defending orgs, location, time, etc.*)

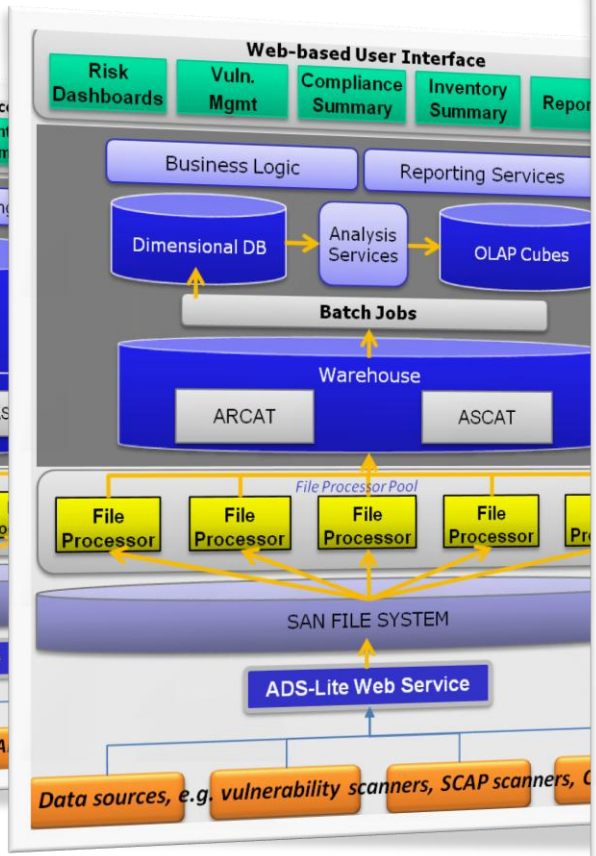
Scalable Architecture

Multiple architectural options to support organizations of various sizes



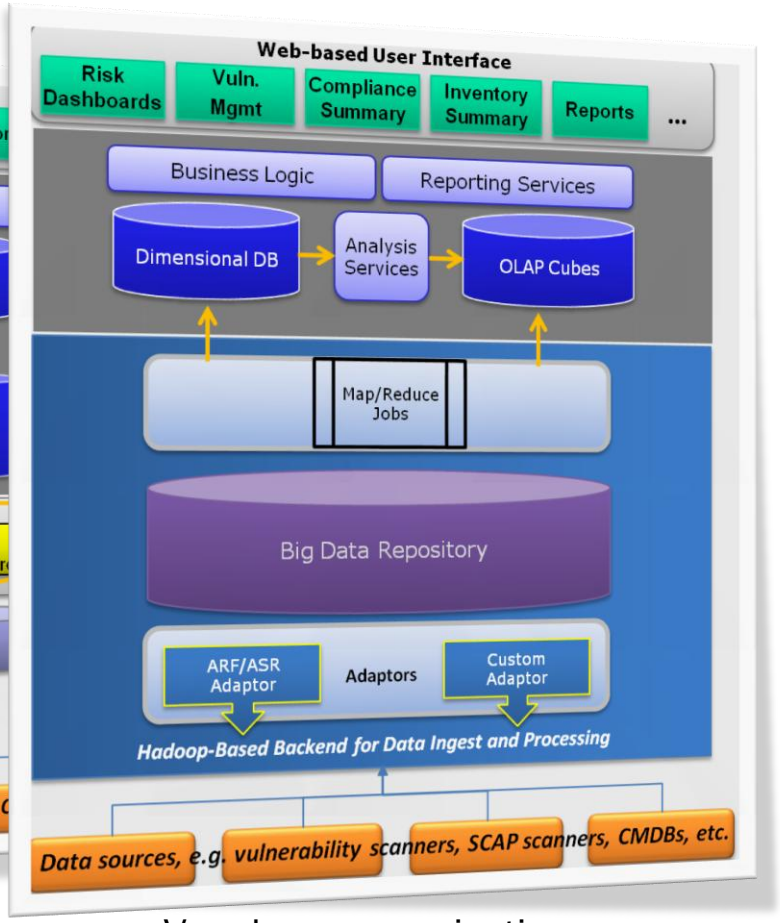
Small to medium organizations

(less than 100,000 devices)



Large organizations

(100,000 to 2M devices)



Very large organizations

(Over 2M devices)

45195 Research Place, Ashburn, VA 20147

Phone: 703.564.2012 | Fax: 703.840.0501

Continuous.monitoring@SuprTEK.com

PANOPTES