StillSecure® VAM™

Eliminates risk through end-to-end vulnerability management | Datasheet

The StillSecure® VAM™ vulnerability management platform identifies, tracks, and manages the repair of network vulnerabilities across the enterprise. VAM mitigates the risk of network exploitation through end-to-end vulnerability lifecycle management.

VAM serves as your vulnerability command and control center, delivering:

- Systematic vulnerability scanning: fast, accurate, comprehensive, with minimal network impact
- Automated, scheduled device discovery and network mapping; fully configurable, tunable
- Extensible *Vulnerability Repair Workflow*™: automatic assignment of repairs and scheduling, lifecycle tracking, automated repair verification, detailed device histories
- Technical and management reporting
- Trending and workflow analysis
- Multi-user, role-based permissions/access
- Distributed architecture for large organizations; centralized data warehousing
- Full integration with existing IT systems through the *Enterprise Integration Framework*™ suite of open APIs

As an integrated vulnerability management platform, VAM goes well beyond the routine scanning and reporting offered by simple vulnerability scanners. Effective vulnerability management must take into account regulatory/compliance requirements, the diminishing time between the identification of a vulnerability and its exploitation, and the need to maximize the efficiency of finite IT resources. VAM meets the challenges of today's demanding security environment, offering:

- Regulatory compliance: VAM ensures and demonstrates (through comprehensive reporting and device histories) the integrity of systems housing sensitive information
- Integration with existing IT systems and processes, such as trouble ticketing, patch management, network management, and other security-related systems
- Extensibility to accommodate organization-specific requirements and business flows
- An open, distributed architecture that scales seamlessly to global, enterprise-wide deployments, yet offers centralized Web-based management (shown at right).

VAM is available as software or as preconfigured hardware appliance. VAM can be deployed as a turnkey vulnerability management system or as a management platform integrated with existing IT systems.

SECURE ENTERPRISE

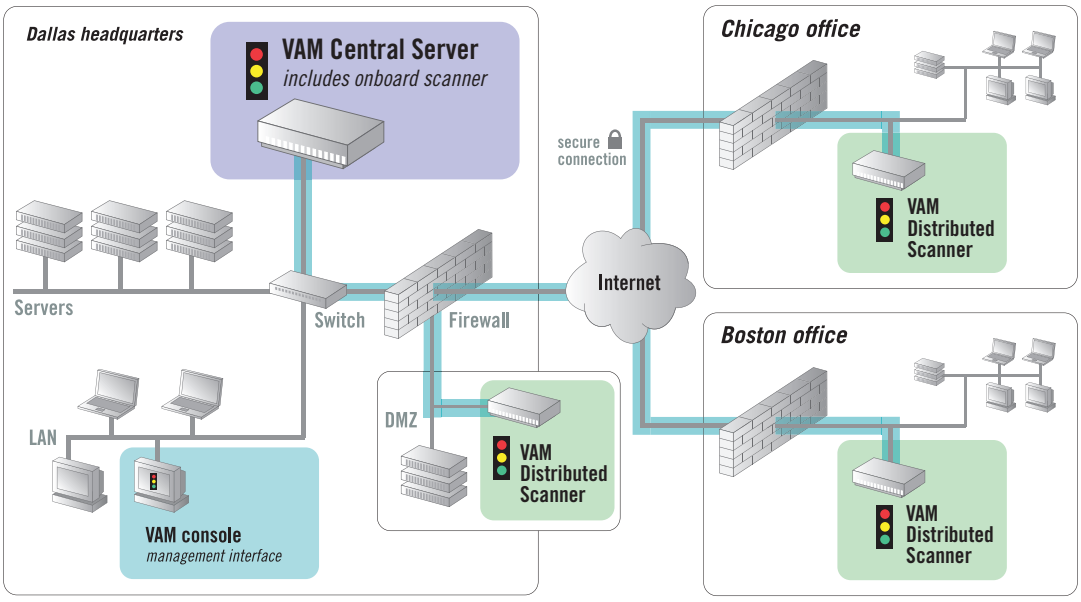
"StillSecure VAM's workflow process shined. Our options changed as a vulnerability moved from stage to stage, and we could see our overall schedule of tickets by day or month."

Secure Enterprise magazine

PROCESSOR

"VAM provides a fast and powerful command center for managing vulnerabilities throughout the enterprise."

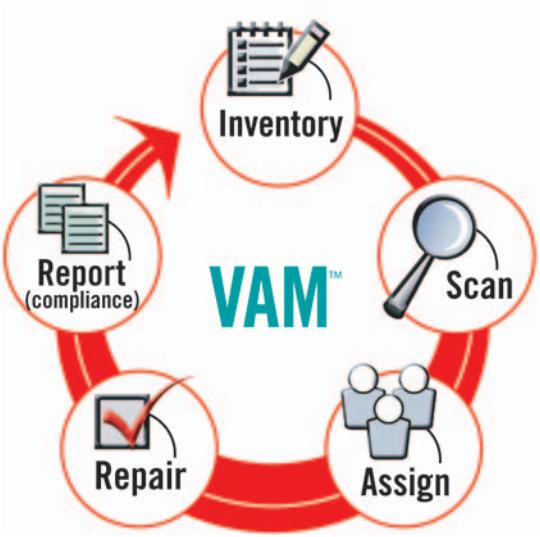
Processor magazine



VAM employs a distributed scanning architecture. All scanning and repair activities are securely controlled and coordinated through the VAM Central Server. Distributed Scanners are deployed as needed to load balance and to scan remotely. Access to the Central Server is through the Web-based VAM console, providing flexible 'anytime, anywhere' management. Where appropriate multiple Central Servers can be managed through a single 'master' Central Server.

The extensible VAM vulnerability management process

The VAM vulnerability management process, shown at right, provides a repeatable, systematic, turnkey approach for finding, tracking, and repairing vulnerabilities. Built on a device- and vulnerability-centric workflow, the process is engineered to meet the complex requirements of enterprise-scale vulnerability management.



Network inventory

- Inventory scanning – Scheduled scanning and on-demand scanning
- Device fingerprint – OS, services, and applications
- Fast device inventory – Tens of thousands of hosts discovered in minutes
- Rogue device identification – Protects against unauthorized devices

Systematic vulnerability scanning

- Systematic scanning – *Intelliscan*™ automatically determines appropriate scans for each device
- Maximized scanning efficiency – Minimal impact on network resources
- Scheduled scanning – Pre-defined hourly, daily, weekly, and monthly scanning schedules; user-customized schedules
- On-demand scanning – Efficiently assess network changes and new threats
- Custom scanning profiles – Meet organization-specific requirements
- Automatic scan rule updates – Up to hourly updates for zero-day protection

Automatic assignment and notification

- Automatic assignment – Vulnerabilities assigned to individual(s) responsible for repair
- User-specified notifications – Management, others notified of repair status
- LDAP integration – Synchronize VAM user accounts with LDAP database

Managing the repair process

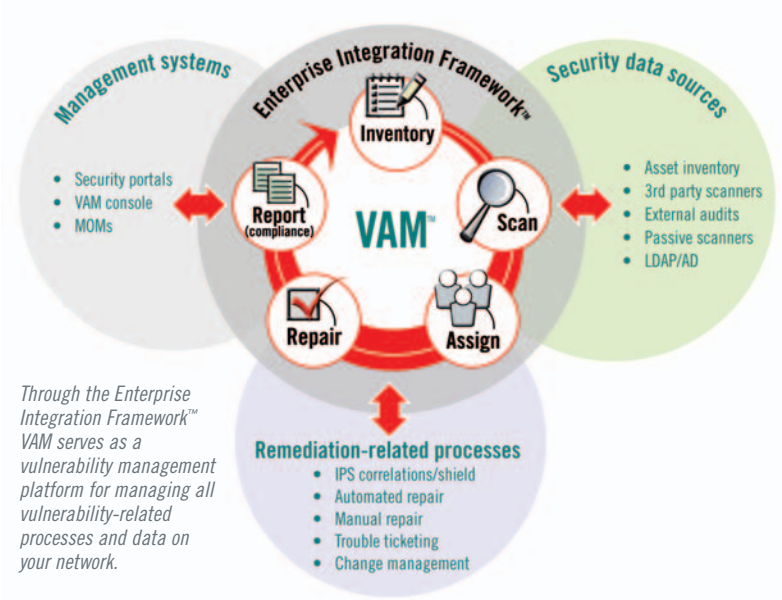
- *Vulnerability Repair Workflow*™ – Tracks repair progress from the time a vulnerability is discovered until the repair is verified
- Prioritized repair schedules – Driven by importance of the host device and criticality of the vulnerability
- Automated patch installation – Through integration with Microsoft® SMS and others
- Verification scans – Automatically performed on reported repairs
- Complete device history – For meeting compliance and auditing requirements
- Extensible, customizable workflow – Create organization-specific functionality through *Extensible Security Plug-in Architecture*™

Targeted reporting and compliance: Security POV™

- Comprehensive, targeted threat and workflow analysis
- Multi-level reporting – Generated on a corporate or workgroup level
- Actionable – Provide concise security status information and specify responsibilities for updates and repairs
- Filterable – By workgroup, device, vulnerability, scan activity, and dozens of other criteria
- Targeted for multiple audiences – Specific reports for managers, auditors, and IT staff

Integration within the enterprise IT environment

The optional *Enterprise Integration Framework*™ (EIF) module facilitates the complete integration of the vulnerability management process within the IT environment. The EIF is a set of open APIs (available both in Java and XML) that allows external systems to execute commands, import data to, export data from, and act on vulnerability data within VAM's core vulnerability management process (shown below).



Through the Enterprise Integration Framework™ VAM serves as a vulnerability management platform for managing all vulnerability-related processes and data on your network.

Through this open architecture, VAM serves as a network vulnerability command center, providing a common view of all vulnerability data and consolidating data and processes from other vulnerability-related systems, such as third-party scanning tools and patch managers. For example, VAM can create, update, or close out a trouble ticket in a third-party system such as Remedy or Peregrine (see example below). Likewise, VAM can import data from other vulnerability scanners, such as Nessus, ISS Internet Scanner, Harris STAT® and others.

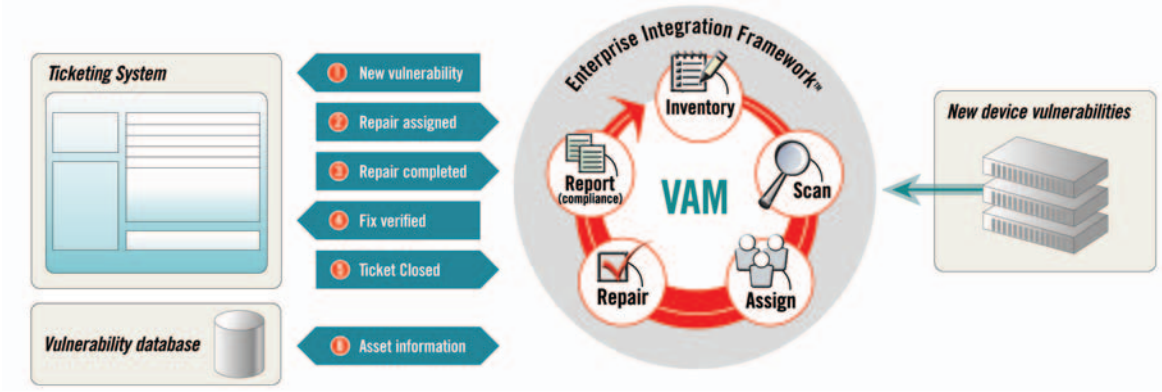
The VAM Enterprise Integration Framework provides:

- Centralized management of all vulnerability data – A single, integrated, end-to-end repository where all vulnerability information, activities, and data are managed.
- Vulnerability management across disparate systems – Integrates with third-party and internal systems to provide an auditable workflow.
- Leveraging of IT investments – Increases the value of existing IT systems and processes, streamlines security administration, and reduces training and management costs.
- Proactive risk mitigation – Requires less overhead and provides a repeatable means to continually mitigate the risk of an attack on the network.

The EIF also includes the *Extensible Security Plug-In Architecture*™ (ESPA), an open architecture that enables users to extend VAM's functionality by fine-tuning the workflow to meet specific organizational requirements. Executed directly from the VAM interface, plug-ins perform business operations unique to the enterprise's needs, such as sending data to business-critical systems or home-grown IT systems. Users can also build plug-ins to modify VAM; for example, customizing workflow prioritization or changing device profile information. Highly flexible, plug-ins can be developed using any programming or scripting language that can parse XML.

VAM business benefits

- Secures digital assets and reduces administrative overhead through highly automated scanning, repair management, and reporting process
- Ensures vulnerabilities are prioritized and fixed through an auditable, accountable process
- Maintains detailed compliance audit trail and reporting capabilities
- Leverages existing IT investments by integrating vulnerability data and processes from third-party IT systems for centralized security management and control
- Flexible deployment options: turnkey vulnerability management system or enterprise-integrated vulnerability management platform



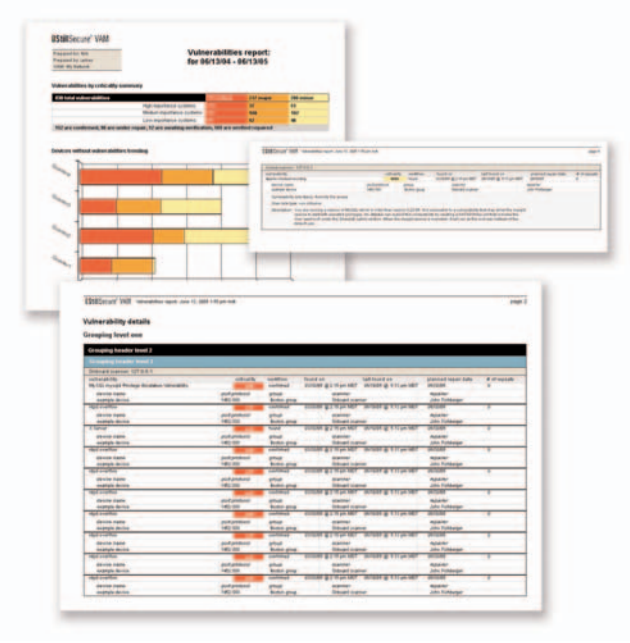
Example VAM integration with trouble ticketing system.

Reporting and compliance with Security POV™

Security POV consolidates all vulnerability data points from across the enterprise and provides a single view of an organization's risk. Available as an optional security management analysis module, Security POV analyzes the vulnerability lifecycle, repair management, and risk management posture. It generates both high-level and in-depth, granular reports tailored to auditors, managers, security staff, and system administrators.

Security POV analyzes all affected elements, correlates vulnerability risks from multiple sources, assesses the organization's effectiveness at eliminating and reducing security risks, and identifies positive and negative trends in the vulnerability management process.

Security POV's enterprise-class reporting capabilities include complete customization (including look and feel), scheduled and emailed reports, public and private reports, and five output formats including HTML, PDF, and XML.



Security POV provides vulnerability management, repair management, and security posture analysis.

Enterprise scalability and management

VAM scales seamlessly, from simple LAN deployments to enterprise-level networks. Managed from a single Central Server, multiple Distributed Scanners (DSs) can be deployed to provide the coverage required (see figure on page 1). DSs enable VAM to scan through or behind firewalls (and other access control measures) and across geographically dispersed networks.

Additionally, VAM's Groups, Collections, and role-based permissions features provide enterprise-level management of devices, user access, and reporting. Using Groups and Collections, you can create a hierarchical structure tailored to your organization and assign role-based, need-to-know access to VAM. Enterprise features include:

- Centralized, in-house, secure management of all vulnerability data
- Centralized configuration and control of Distributed Scanners
- Optimized interface for high-volume, complex enterprise environments.

Zero-day protection with automated rule updates

VAM scan rules are created, tested, and released by the StillSecure Security Alert Team (SAT), which operates on a 24x7 basis to monitor and respond to network threats. In addition to writing and releasing GPL rules in-house, SAT compiles rules from multiple sources including the Open Security Scanner Association (OS2A) and other organizations operating under the GPL.

VAM rules conform to the open-source .nasl format. VAM can be configured to check for updated SAT rules as frequently as every hour, or users can download rule updates on demand, ensuring up-to-the-minute protection against newly released threats. Custom rules can be easily created to address organization-specific threats and policy compliance.

Integration within the StillSecure suite

VAM is part of the integrated StillSecure suite of layered security solutions for the network. In addition to VAM, the suite includes:

- StillSecure Safe Access™ – network access control solution
- StillSecure Strata Guard™ – intrusion detection/prevention system

Through the StillSecure *Enterprise Integration Framework* (EIF) security data is shared among suite solutions and with existing IT systems, greatly enhancing network protection and operational efficiencies. The EIF enables data import/export and process integration with a wide-range of security and IT systems, as discussed above.

The integrated StillSecure suite offers organizations the following benefits:

- Layered security from a single provider
- Enhanced security through solution integration/data correlation
- Leveraging of existing security investments through an open architecture
- Simplified administration with suite-wide common functionality, usability, and data management

We invite you to try a free demonstration. Contact 303-381-3830, sales@stillsecure.com, or visit www.stillsecure.com.

StillSecure
100 Superior Plaza Way
Suite 200
Superior, CO 80027
P: [303] 381-3800
F: [303] 381-3880
www.stillsecure.com