StillSecure® VAM™

Eliminates risk through end-to-end vulnerability management.

Features, functions, and benefits

Feature	Function	Benefit
Device discovery/network mapping		
Autodiscovery™	▪ Discovers when new devices, applications, and operating systems are present on the network. ▪ Inventories discovered devices.	▪ Informs you when new devices are present on your network and allows these devices to be scanned for vulnerabilities. ▪ Discovers transient and rogue devices before they can compromise your network.
Ultra-fast initial device discovery	Through a multi-phased approach, places devices in the system quickly, even on networks that don't allow ICMP ping scans.	Large networks are scanned quickly.
TCP and UDP port scans for application accuracy	Scans TCP and UDP ports for applications.	Know which applications can create vulnerabilities.
Applications using non-standard ports identified	Scans multiple ports (rather than standard ports only) for applications.	Discovers hidden applications.
Accurately identifies devices and versions including: servers, desktops/laptops, infrastructure, IP phones, copiers, printers, DSL modems, cable modems, etc.	NMAP scans and characterizes the network.	Quickly and accurately identify almost 900 different systems, then use that information to efficiently scan for vulnerabilities.
Scheduled device discovery at user-determined intervals	Can be run regularly on a schedule of your choosing.	Device discovery occurs at your convenience.
On-demand device discovery	Quickly set up and run discovery on specific IP ranges.	Quickly respond to and assess network changes.
Configurable *Autodiscovery* parameters	▪ Supports multiple methods of detecting devices. ▪ Allows custom *Autodiscovery* settings for each *Distributed scanner* on the network.	Tailors host discovery to network configuration and environment.
Integration with third-party asset inventory systems	Import/export asset data from/to existing inventory system(s).	Leverage existing systems and data; maintain single source of asset data.
Vulnerability scanning		
Intelliscan™	Applies appropriate scan rules automatically to devices based on device type, OS, and applications.	▪ Delivers appropriate scans for range of devices. ▪ Ensures protection from specific vulnerabilities. ▪ Optimizes use of network and IT staff resources.
Automated, scheduled scanning	Systematically and continually scans for vulnerabilities without requiring monitoring 24x7x365.	Automated scanning saves IT resources and significantly reduces risk exposure.
On-demand scanning	Provides one-time scans focusing on specific vulnerabilities and/or IP ranges.	Efficiently respond to and assess network changes and new threats.
User-defined scanning schedule	Accommodates custom scan schedules.	Set up scanning convenient to your network/organization.
Pre-defined scanning schedules: hourly, daily, weekly, monthly	▪ Pre-defined scan policies install automatically with VAM. Can be easily modified to meet specific needs.	▪ Speeds setup and installation of the product. ▪ Optimizes scanning; saves time and network resources.
Scanning windows	Allows you set start and stop times for scheduled scans	Ensure minimal impact to production systems and users.
Custom scan policies	▪ Apply user-created custom scan policies to groups of devices or individual devices to test for a specific set of vulnerabilities. ▪ Implement custom schedules for all types of scans.	Optimize VAM to your network.
SANS Top 20 Internet Security scan policy	▪ Scans specifically for SANS Top 20 Internet Security vulnerabilities. ▪ Pre-defined, ships with VAM.	Ensures protection against the most commonly exploited vulnerabilities.
Integration with third-party vulnerability scanners and external sources of security data	Import data from third-party scanners and other sources.	Leverages existing systems and data; ensures comprehensive scanning coverage.
Scan rules		
Comprehensive .nasl-based *Scan rule* database	Protects against the widest variety of vulnerabilities.	Leverages the most popular scan rule format.

Dedicated 24x7 rule development and testing from StillSecure Security Alert Team (SAT)	Immediately creates, tests, and distributes scan rules for newly identified vulnerabilities.	Allows you to quickly identify where your network is vulnerable to new threats before they can be exploited.
Secure, quality-controlled, automated *Scan rule* updates	Automatic notification that tested *Scan rule* updates are available.	▪ No work required to stay current. ▪ Assurance that new scans are thoroughly tested before release.
Rule definitions	Provide a quick understanding of the affected software and operating systems, how the attack is launched, the impact on your system, and how to protect your system from future attacks.	Educates users; improves decision-making and repair efficiency.
Rule search	Quickly find and research specific rules.	Saves time and provides up-to-date rule information; improves understanding of rules and the vulnerabilities they address.
Per-vulnerability user notes	Enter notes for any vulnerability.	Ability to review reasons for actions on vulnerabilities.
Repair management		
Vulnerability Repair Workflow™	▪ Manages the repair process from vulnerability discovery to repair verification. ▪ Systematic means of tracking that repairs are being made by whom and when.	▪ Provides accountability and control over network security. ▪ Utilizes IT resources effectively throughout the remediation process.
Automatic assignment and verification of vulnerabilities	▪ Automatically assign repair tasks to the responsible IT staff member. ▪ Continually inform staff of repair status.	▪ IT can definitively show remediation progress and status. ▪ Clear ROI calculations. ▪ Accountability for status and solutions. ▪ Systematically ensures all vulnerabilities are assigned repair.
Multi-role remediation process	Assign roles in the remediation process to various individuals.	Manages differentiation of repair responsibilities.
Multi-state remediation process	Provides status of vulnerabilities.	▪ Accurately define where vulnerabilities are in the remediation process. ▪ Eliminate time and effort wasted responding to false-positives.
Automated notification of workflow status for administrators	Emails designated administrator with the status of the entire repair process.	Enhances accountability and improves vulnerability management.
Collections	Enables users to create sets of devices based on device attributes	▪ Organize devices into logical categories to better manage large numbers of devices. ▪ Create hierarchies of devices.
Integrated patch management	▪ Integrates with Microsoft® SMS to automate the vulnerability repair process. ▪ VAM manages the integrated process, tracking and logging all SMS activity.	▪ Automates vulnerability repair. ▪ Reduces burden on IT staff, saving time and resources. ▪ Repairs vulnerabilities quickly; improves security.
Ability to act on single vulnerability or many vulnerabilities at one time	'One-click remediation' for multiple vulnerabilities in the repair workflow.	▪ Simplifies and speeds managing the repair workflow. ▪ Reduces burden on IT staff; saves time and resources.
Fine-grained user permissions	▪ Supports multi-user access with appropriately defined roles. ▪ Assigns appropriate levels of access privileges.	▪ Tightly control access to highly confidential vulnerability information and changes to the repair process. ▪ Tightly control the levels of privileges based on company policy or roles. ▪ Facilitates appropriately distributed responsibility within repair process.
LDAP/AD integration	Synchronize with LDAP/AD database to create/update VAM user accounts.	Eliminates redundant account management activities; saves time on the creation and management of VAM user accounts.
Define business importance of assets	Assign importance level on a device-by-device basis.	Creates efficiency by focusing on the most critical devices first.
Escalation of repair based on criticality	Important devices are scheduled for repair before low-importance devices.	Critical vulnerabilities are given adequate focus.
Editable device profiles	▪ Maintain security information about each device such as discovery date, OS, applications, open and restricted ports, and scan schedules. ▪ Includes user-entered notes for additional information and context.	▪ Minimize manual efforts to track and maintain information about devices, their vulnerability history, and repair activities. ▪ Maintain a complete vulnerability audit trail for all vulnerabilities and their state of repairs.
Enterprise-scalable management of repair process	Centralizes management of vulnerabilities enterprise wide	Large organizations can efficiently secure their systems with clear accountability.

Advanced vulnerability filtering	Quickly pinpoint vulnerability(s) of interest.	Simplifies and speeds managing the repair workflow.
View repair workflow by vulnerability or by device	Toggle between vulnerability-centric or device-centric views.	Simplifies and speeds managing the repair workflow.
Reporting and compliance		
Security POV™	▪ Provides in-depth analysis of vulnerability lifecycle, repair management, risk management. ▪ Outputs both high-level and granular reports for auditors, managers, network and security staff. ▪ Provide details on specific vulnerabilities of interest.	▪ Correlates vulnerability risks from multiple sources. ▪ Assesses effectiveness and identifies trending in the vulnerability repair and management process. ▪ Provides actionable information and historical data for compliance.
Multiple report output formats	Selectable formats include HTML, PDF, CSV, XML, MS Excel.	Flexibility in report delivery.
Scheduled reporting	Automatically generates and emails reports to designated recipients.	Reduces administration time and keeps stakeholders informed.
Automatic report updates	Automatically updates reporting functionality and adds new reports to VAM via scheduled report updates.	Updates reporting capabilities without requiring the installation of software upgrades.
Drill-down capabilities	Pinpoints specific vulnerability/device/workflow data.	Enables in-depth analysis of data.
ODBC / SQL access to database	Standardized protocol allows custom queries and reports.	Allows you to customize reports and queries.
Report filtering	Filter reports on dozens of parameters including: *Collections* *Scan policies* Devices Device importance Vulnerabilities Vulnerability severity	Provide targeted, highly specific data for auditors, managers, and IT staff.
Integration with third-party reporting tools	Export data to third-party reporting tools.	Leverage existing systems and data; centralize management of vulnerability data.
Integration/extensibility		
Enterprise Integration Framework™	▪ Allows external systems to import data to, export data from, and act on data maintained in VAM through open Java/XML-based API.	▪ Centralizes management of all vulnerability data. ▪ Manages vulnerabilities across disparate systems. ▪ Leverages IT investments. ▪ Proactively mitigates risk.
Extensible Security Plug-in Architecture™	▪ Extends VAM functionality with user created plug-ins, which are run directly from VAM interface.	▪ Enables users to fine-tune VAM functionality to their business flows/environment. ▪ Reduces security administration.
Software development kit	Enables users to: ▪ Create connectors to external systems within the VAM API ▪ Write plug-ins	▪ Allows users to extend VAM functionality on their own.
On-request connector/plug-in development	Contract with StillSecure to write customer-requested connectors and plug-ins	▪ Takes advantage of StillSecure development expertise in extending functionality.
StillSecure suite integration	Natively supports integration of VAM with other solutions in the StillSecure suite including: ▪ StillSecure Safe Access™—network access control ▪ StillSecure Strata Guard™—intrusion prevention/detection	▪ Provides layered protection for the network. ▪ Maximizes efficiency of management and threat response through solution integration/data correlation. ▪ Leverages existing security investments through open architecture—enables integration with third-party security systems for centralized command and control. ▪ Simplifies administration with suite-wide common functionality, usability, and data management.
Deployment/scalability		

Scalable distributed architecture to scan enterprise, remote, and complex topologies	▪ Enables VAM to seamlessly scale to networks of any size and complexity. ▪ Centralizes data storage and management while distributing scanning. ▪ Allows local management/administration of repair workflow in distributed environment, based on centrally assigned permissions.	▪ Tailors deployment to specific environment. ▪ Enables responsibilities for vulnerability management to be assigned both centrally and locally in accordance with organizational structure/hierarchy.
Distributed scanning	*Distributed Scanners* (DSs) distribute the workload, enabling coverage of larger, more complex networks.	▪ Scan large network environment easily. ▪ Tailored scanning and performance parameters for each scanner with no on-site maintenance.
Centralized administration and data warehousing	▪ *Central Server* controls all local and distributed scanning activities. ▪ Provides central repository for all scanning and repair data.	Provides centralized administrative control over distributed scanning environment.
System management		
Anywhere, anytime access	Web-based interface.	Management flexibility.
Supports multiple browsers	Management console accessible through IE 6.0, Firefox 0.9, and Mozilla 1.7.	Provides management flexibility.
Authenticated proxy server support	Receive VAM license validation and rule updates through proxy server.	Saves time; allows easy integration into existing network environments.
Getting started tab	Helps new users become familiar with core VAM functionality.	Provides rapid time to value; allows scanning, remediation, and reporting activities to begin immediately.
Automated *Distributed Scanner* (DS) upgrades	Automatically updates DSs with software upgrades and patches as they become available.	Saves the time and resources; ensures product updates/upgrades installed.
Automatic data archiving	Archive historical data by offloading to external media or install a commercial back-up client on the VAM machine.	▪ Store appropriate amount of historical data. ▪ Easily keep historical data for compliance/audit purposes. ▪ Ensures system integrity. ▪ Reduces/eliminates system downtime.
Commercial data back-up	Compatible with leading back-up solutions for long-term data archiving.	Helps meet regulatory or audit requirements in addition to protecting against data loss.
Historical per-device data	Maintains a log of all actions by device.	Supports audit and reporting requirements.
Availability		
Software appliance	Provides implementation options as software solution installed on user-provided equipment.	▪ Flexible delivery options. ▪ Lets you select the implementation appropriate for your environment.
Hardware appliance	Provides implementation option as a high-performance hardware appliance.	Pre-configured and standardized.
Distributed scanners	DSs are delivered as software or hardware appliances, complete with a hardened OS and managed through the VAM console.	▪ One product to scan enterprise wide. ▪ Distributed scanners can be placed across the enterprise for efficient scanning. ▪ Plug-and-play hardware-based appliance to scale scanning capabilities.
Secure locked-down OS	Customized, hardened Linux® operating system.	Ensures vulnerability and management system is secure.
Subscription-based payment or purchase-plus-maintenance payment structures	Includes vulnerability updates, software updates, report updates, and engineer-delivered technical support.	▪ Provides affordable, cost-effective protection; low cost of entry. ▪ Provides all-inclusive, fixed cost of ownership.

StillSecure
361 Centennial Parkway
Suite 270
Louisville, CO 80027
P: [303] 381-3800
F: [303] 381-3880
www.stillsecure.com

Reducing your risk has never been this easy.