

Device discovery/inventory

- Multi-phased scheduled and on-demand discovery scanning
 - Proprietary discovery capabilities
 - NMAP
 - Fully tunable
 - XProbe
- Fingerprints OS, available hosts, services (i.e., ports), and applications
- Fully configurable scan parameters:
 - *Phased discovery approach*
 - *Default configuration optimized for high speed and accurate OS and port discovery*
 - *Seven discovery phases, fully configurable/customizable*
 - *"Tune-to-scale" approach based on network size, complexity*
- Identifies 900+ distinct OSs and OS variations
- Multiple methods to determine live IPs
- Unique profile maintained/updated for each discovered device

Vulnerability scanning

- Systematic scanning (i.e., *Intelliscan™*): applies only scans appropriate for device (based on device fingerprint)
- Scheduled scanning – completely customizable
- On-demand scanning
- Employs open source Nessus* scanning engine – agent-less architecture
- Scan data from other scanners can be imported through the *Enterprise Integration Framework™*
- Manages unlimited number of scan policies (i.e., collections of individual scan rules and port scans)
- Pre-defined scan policies ship with product:
 - *SANS Top 20 Internet Security Vulnerabilities*
 - *Hourly, Daily, Weekly, and Monthly scan policies*
- Custom scan policies:
 - *User-selected scan rule sets*
 - *Meets organization-specific scanning/compliance requirements*
- Port scanning options include:
 - *TCP common ports*
 - *UDP common ports*
 - *User-defined port ranges for both TCP and UDP*
- *Industry-leading support for the following local checks:*
 - *Linux, Solaris, HP-UX (Q4), AIX (Q3/Q4), Windows, Redhat*
- Non-intrusive device scanning by default
- Intrusive scanning optional for deep inspection
- Data exportable in Nessus format for integration with existing security/management systems

Scan rules

- Over 9,000+ rule set (continually expanding)
- Rule set consolidated from multiple sources
 - *StillSecure® Security Alert Team (SAT)*
 - *Open Security Scanner Association (OS2A)*
 - *Open source, GPL*
- Automatic rule updates
 - *Initiated by SSL request to SAT server*
 - *Occur up to hourly (frequency is user configurable)*
 - *Manual rule updates on demand*
- New rules automatically incorporated into existing scan policies
- Import existing .nessusrc files
- Custom rule creation/rule editing
- Rule-specific repair/research available through product interface from:
 - *StillSecure SAT*
 - *SecurityFocus Bugtraq*
 - *Mitre CVE*
 - *Others*

Repair management

- Device- and vulnerability-centric workflow engine
- Tracks vulnerability through seven workflow states until repair confirmed
- Automated repair verification scanning
- Threat prioritization/repair scheduling based on:
 - *Device importance (user configurable)*
 - *Vulnerability severity*
- Assignable user roles:
 - *Vulnerability confirmer*
 - *Repairer*
 - *Secondary repairer*
 - *Device owner*
- Automatic notification/assignment of vulnerabilities to designated repairer, others
- Tracks/displays repair date, assigned repairer, and repair progress
- Automated repair:
 - *Native integration with Microsoft SMS*
 - *Supported integration with other patch managers*
- Individual device histories include all vulnerabilities and repair activities

Reporting/compliance

- Security POV™: Highly configurable reporting module (optional)
- Enables both targeted reporting and high-level trending and workflow analysis
- Reporting filterable on any combination of parameters maintained in database, including:
 - *Device(s)*
 - *Vulnerabilities*
 - *Operating system*
 - *Rules*
 - *Scan policies*
 - *Users*
 - *Repair schedules*
 - *Discovery/repair date*
 - *Group*
 - *Collection*
- Savable filter options for repeatability; fast, easy customization
- Scheduled and on-demand reporting
- Administrator created and controlled:
 - *Public reports available to all users*
 - *Personalized 'My reports' to meet local user or group-specific needs*
- Regroup/resort on demand
- Reporting enhancements distributed through rule update process; no upgrades necessary to enable new reporting functionality
- Report designer included for formatting, co-branding, customization, etc.

Deployment/scalability

- Hierarchical group-based management
- Enterprise-scale distributed architecture:
 - *Central Server includes complete application and onboard scanner*
 - *Distributed Scanner(s) (zero-maintenance appliance) for load-balancing and remote scanning (single and multiple CPU models available)*
- Central Server controls unlimited number of distributed scanners; all scanning/repair activity centralized and controlled through single Web-based interface
- Automated distributed scanner upgrades
- Capable of managing tens of thousands of devices and millions of vulnerabilities when deployed on off-the-shelf hardware
- Centralized data warehouse; no data stored on Distributed Scanners (encrypted SSL transmissions initiated by Central Server)

System management

- Multi-user, role-based permissions/access:
 - Administrators
 - Write access (e.g., repairers)
 - Read-only access (e.g., auditors, management, etc.)
- LDAP integration for authentication against existing user infrastructure
- Functionality exposed to user on need-to-know basis driven by assigned permissions (i.e., fine-grained permissions)
- Fine-grained, assignable permissions for write users
- Groups: associate subsets of devices with users; enables targeted reporting, separation of responsibilities
- Collections: dynamic subsets of devices based on user-defined attributes including:
 - IP address
 - Operating system
 - DHCP device
 - Group
 - Scanner name
 - Discovery date
 - Device importance
 - NetBIOS name
 - Others
- Newly discovered devices automatically added to existing collection(s)
- Authenticated proxy server support

Integration within IT environment

- Open API (available in Java or XML) for integration with third-party IT/security systems including:
 - Trouble ticketing
 - Patch managers
 - Asset inventory
 - Third-party vulnerability scanners
 - Intrusion prevention/detection systems
 - Network managers
 - Change managers
 - Security information managers
 - Others
- Includes software developer's kit
- Connectors available off the shelf for:
 - Management systems: Citadel Hercules, Skybox
 - Third-party vulnerability scanners: eEye Retina, ISS, Harris, Nessus
 - StillSecure suite: Safe Access (network access control) Strata Guard (IDS/IPS)
 - More under development
- Custom connectors developed on request

Extensibility

- Extensible Security Plug-In Architecture™ (ESPA) enables customization of repair workflow through user-created plug-in scripts
- Allows workflow to be fine-tuned to meet organizational needs
- Plug-ins:
 - Selected and run from within VAM interface
 - Developed using any programming or scripting language that can parse XML
 - Access to plug-ins permission-controlled
- Example plug-in functionality:
 - Export select data to specific business system
 - Customize workflow prioritization
 - Change device profile information
- XML interface manager allows plug-ins to be launched from anywhere on network

OS/platform/architecture

- CommonOS: Hardened Linux® OS, ships/installs with VAM
- Open architecture; customizable, extensible

- On-board ODBC-compliant MySQL database and JDBC
- Design incorporates multiple open-source components
- Data archiving options
 - Automatic daily archiving of entire database
 - Configuration settings backup
 - Third-party backup tool integration
 - Offload database to other media or device

Availability

- Software – user-installed on dedicated host
- Hardware appliance – custom configured per consultation with customer
- Purchasing models:
 - Annual subscription
 - Perpetual: purchase plus annual maintenance
- Subscription/purchase includes all rule updates and product upgrades

Support

- Engineer-delivered
 - Available at no charge to subscribers
 - 8:00 a.m. to 6:00 p.m. MST; 24-hour support available
 - Training and tuning assistance available

System requirements

Central Server:

1. A dedicated server for product installation with the following minimum system requirements:

- Pentium® 4 1.3 GHz (2.0 GHz recommended)
- 512 MB RAM (1 GB recommended)
- 36 GB disk space
- One server-quality network interface card 10/100 (3Com or Intel)
- CD ROM drive
- An Internet connection that allows outbound SSL communications

2. Management console: A workstation running one of the following browsers (128-bit encryption required):

- Mozilla Firefox 0.9.3 and higher (Linux, Windows®)
- Mozilla 1.7 and higher (Linux, Windows)
- Internet Explorer 6.0 and higher (Windows)

Distributed Scanner:

The VAM Distributed Scanner is shipped as software or preconfigured hardware appliance.

Hardware appliance

StillSecure custom-configures hardware appliance in consultation with customers.



VAM preconfigured hardware appliance.

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