StillSecure® VAM™

Eliminates risk through end-to-end vulnerability management.

VAM v5.1

Technical datasheet

February 17, 2004

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.

Table of contents

Introduction

StillSecure™ VAM™ identifies, tracks, and manages the repair of network security vulnerabilities that expose your organization to risk and financial loss.

VAM discovers vulnerabilities (that could allow unauthorized programs to compromise your network resources) and enables you to manage repairs through the following processes:

- **Inventory** – Inventories devices through *Autodiscovery*™
- **Scan** – Tests devices for vulnerabilities through *Intelliscan*™, port scans, and custom scans
- **Assign** – Automatically assigns repairs and sends notifications
- **Repair** – Tracks and facilitates the repair of identified vulnerabilities through the *Vulnerability Repair Workflow*™
- **Report/compliance** – Creates reports showing vulnerability, scanning, and repair activities

VAM is automatically updated as often as hourly with the latest Vulnerability Scan rules, ensuring up-to-the-minute protection against newly discovered threats. An annual subscription to VAM includes all vulnerability rule updates (scan rule updates), software upgrades, and engineer-delivered technical support. Beginning with VAM 5.0, local rule checks (rules that run locally via an SSH shell) have been added to the rules database, along with the ability to create and import your own custom rules.

This document is intended for technical audiences and provides details regarding VAM functionality as well as examples and scenarios of typical VAM installations.

Architecture and deployment

VAM is managed from a single Central server (CS). Scanning is accomplished through a single Onboard scanner, and/or from one or more Distributed scanners (DSs). Distributed scanning enables VAM to scan remote networks and/or scale to large network environments.

In a distributed scanning environment, all scanning and repair activities are securely controlled and coordinated through the VAM CS. Additional DSs can be deployed to load balance on larger networks and to scan remotely. Access to the CS is through the Web-based StillSecure Console, providing flexible ‘anytime, anywhere’ management.

In VAM, there are three categories of scanners:

- **Onboard scanner** – Each VAM installation has a single onboard scanner, which installs with the VAM Central server. This scanner is used to scan the local area network (LAN) in which the central server is installed.
- **Distributed scanner(s)** – A VAM installation can have multiple optional Distributed scanners (DSs) that reside on servers distributed throughout your network.
- **Virtual scanner(s)** – A VAM installation can have multiple optional virtual scanners. Virtual scanners are created when importing data via the API. They serve as device containers, and are not capable of scanning.

There are two primary reasons to deploy distributed scanners:

- **Scaling** – To increase the number of devices scanned and the number of scans that can be performed
- **Scanning remote networks** – To scan portions of your network not accessible by your onboard scanner, potentially due to firewalls or access control lists, or to conserve low bandwidth network links.

VAM Central server

Regardless of where scanning is performed (via the onboard or distributed scanners), all data is stored, secured, and managed in the Central server, which is generally located on the internal portion of an organization’s network.

VAM is provided with a hardened operating system (OS), which is described below.

- **CommonOs™** – This OS (*CommonOs*™) is based on a version of Linux (primarily Redhat Enterprise Linux 3.0 (RHEL)), created and maintained by StillSecure. StillSecure tracks RHEL; however, we build and digitally sign each RPM to work on CommonOs. StillSecure deploys only the safest, proven, and stable version of the Linux kernel and RPMs.
- **Hardened OS** – The OS is hardened by employing the following controls:
  - **Packages** – The number and contents of packages present on the system are thoroughly inspected and tightly controlled.
  - **Firewall** – An on-board firewall (IPTables) restricts outside connections to only secure services (encrypted traffic) on specific ports (22 and 443). When using a Distributed Scanner, a mutually-verified SSL, 1:1 connection is established on port 1005.
  - **Network parameters** – Certain types of dangerous or unnecessary network services are disabled (for example, Ping). Other undesirable traffic is reduced or eliminated (for example, address spoofing, ping floods, etc.).

All vulnerability data is stored in a database with access control capabilities. Login passwords for various services (for example, FTP, SMB, and POP) are encrypted. These measures ensure that confidential data stays in-house and is protected from unauthorized access.

VAM Distributed scanners

Distributed scanners (DSs) distribute the workload, enabling coverage of larger, more complex networks. Distributed scanners are delivered as stand-alone hardware appliances, complete with a hardened OS. Both single- and dual-CPU models are available. DSs do not store any device vulnerability data; instead data is sent securely (encrypted using Secure Sockets Layer (SSL)) to the Central server.

DS configuration is flexible; each DS can have different *Autodiscovery*™ and Scan parameters, and each DS can scan using any policy.

DSs enable VAM to scan through or behind firewalls (and other access control measures) using SSL over transfer control protocol (TCP) on port 1005. No communication is initiated by the DSs.

A firewall is hardware, software, or a combination of the two, designed to control and prevent access to a network. In order for VAM to navigate through your firewalls, you must allow traffic from TCP port 1005 on the central server to the DSs.

Management interface

The Management interface is the StillSecure Console. The console is accessible through HTTPS (SSL) via a web browser. See “System requirements” on page 23 for a list of supported browsers.

Optimization

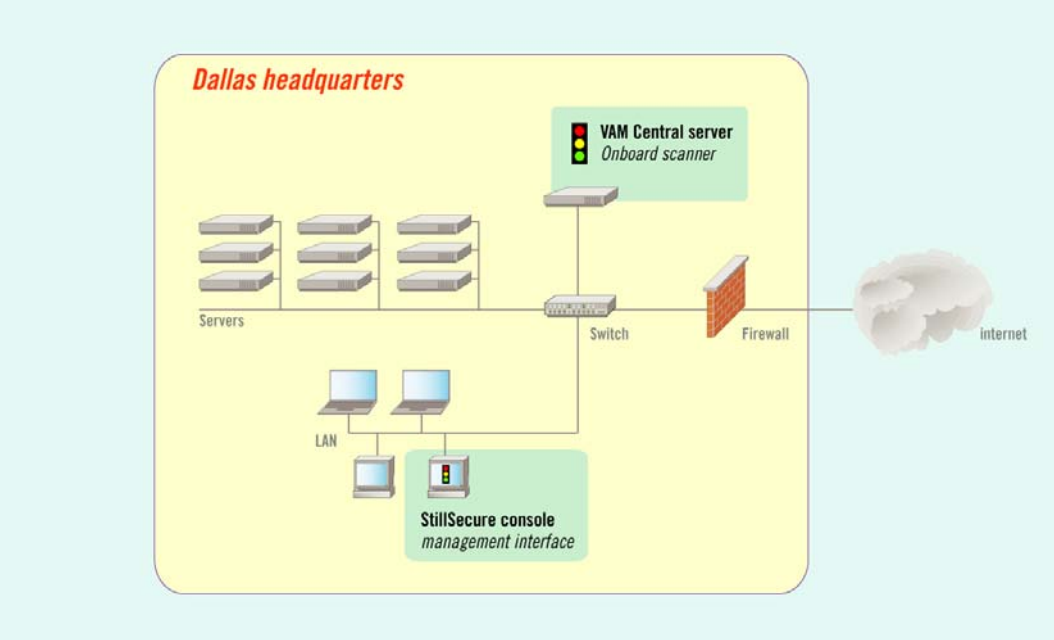
VAM’s configuration is very flexible, allowing you to fine-tune the installation to your unique network requirements. For more information on tuning, see “Performance tuning” on page 21.

Scanner scenarios

The following figures show three possible VAM deployment scenarios:

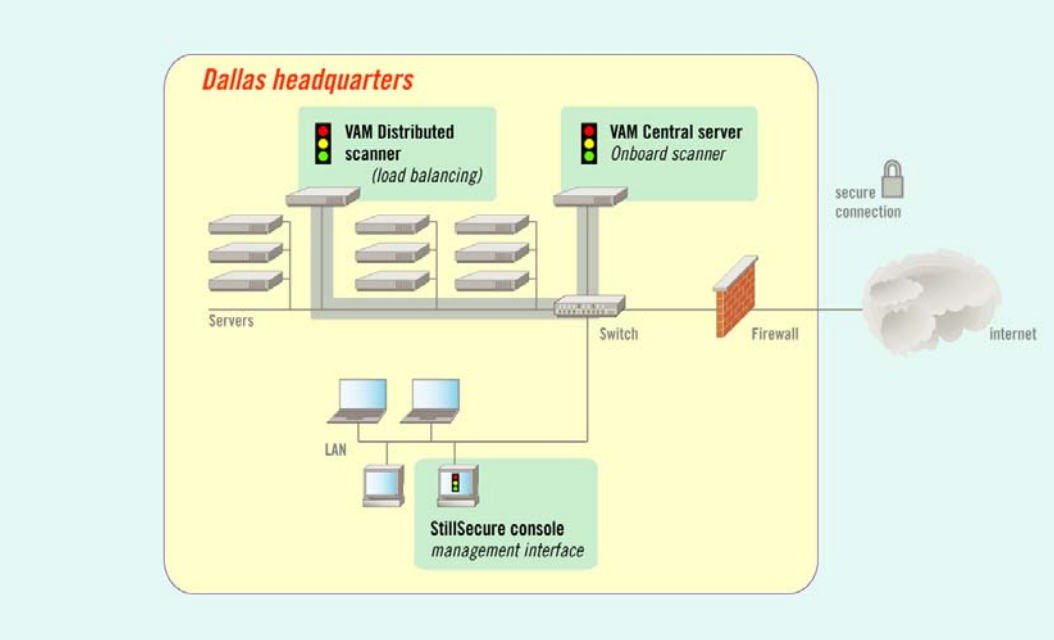
"Figure 1: Single scanner scenario" on page 6 shows how VAM can be utilized in a single scanner environment—scanning the network behind your firewall, for example.

Figure 1: Single scanner scenario



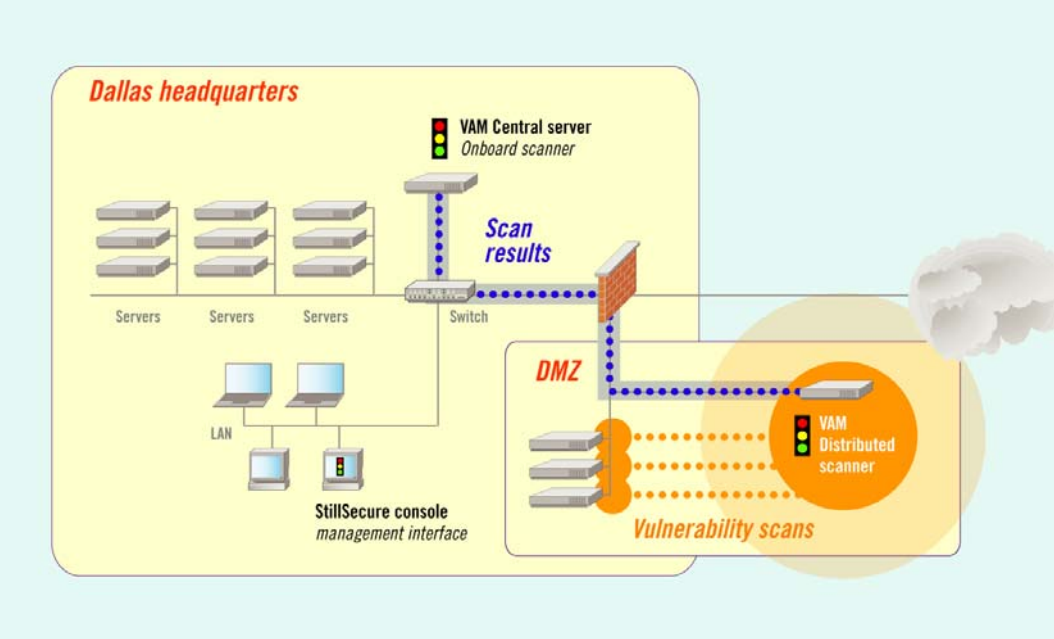
"Figure 2: Load-balancing scenario" on page 7 shows how VAM can be utilized in a load-balanced environment—scanning the network behind your firewall and distributing the load with distributed scanners.

Figure 2: Load-balancing scenario



"Figure 3: Remote scanning scenario" on page 8 shows how VAM can be utilized in a complex environment—scanning the network behind your firewall, distributing the load with distributed scanners, and utilizing remote scanning for your entire network, regardless of the device's physical location.

Figure 3: Remote scanning scenario



VAM process

The VAM process comprises five phases: Inventory (*Autodiscovery*™), Scan (*Intelliscan*™, port scan, and/or custom scans), Assign, Repair (*Vulnerability Repair Workflow*™), and Report/compliance:

Inventory

VAM can discover and inventory an unlimited number of devices during the inventory process. The inventory process, called *Autodiscovery*, utilizes the open-source Network Mapper (NMAP) utility.

NMAP scans networks using internet protocol (IP) packets to determine characteristics of the network such as the operating system (OS), available hosts, available services (ports), and firewalls in use.

Autodiscovery utilizes a phased approach to discover devices on the network. The process has been optimized to provide high-speed detection of large numbers of devices as well as accurate identification of OS and ports. These seven phases are fully customizable for each scanner.

Each of the seven phases performs more and more comprehensive scans, continually discovering devices. Once a device has been discovered, two threads are started for that device; one for OS-type discovery, and one for looking up the DNS/NetBIOS name. These two threads are separate scans that run in parallel with the six phases. By default, up to five (one per host) OS-type scans will run at the same time. These scans are configurable for each DS.

"Phases and TCP ports" on page 9 lists example TCP ports and the phase in which they are scanned:

Table 1: Phases and TCP ports

Phase number	Port number	Port type
1	20	FTP
1	22	SSH
1	23	Telnet
1	25	SMTP
1	80	HTTP
1	137	NetBIOS Name Service
1	138	NetBIOS Datagram Service
1	139	NetBIOS Session Service
1	443	HTTPS
1	445	Microsoft-DS
3	22	SSH
3	23	Telnet
3	445	Microsoft-DS
4	21	FTP
4	25	SMTP
4	80	HTTP
4	110	POP3
4	143	IMAP
4	389	LDAP
4	443	HTTPS

After *Autodiscovery* completes, you can find open ports by executing a scan policy with port scans enabled.

The OS is determined via NMAP, which sends TCP/IP packets (tests) and waits for a response. Any results received are compared to a database of known operating system signatures. If there is a match, more test packets are sent to both open and closed ports. Based on the response received, the OS can usually be determined.

Currently, VAM can detect nearly 900 OSs (see the *Users' guide* for the current list and specific versions). The following are some of the more popular OSs VAM detects:

- Checkpoint
- Cisco IOS router/switches
- Cisco Pix
- Free BSD
- IBM OS/400
- Linux
- Mac OS 9
- Mac OS X

- MS Win 2000
- MS Win 95
- MS Win NT
- MS XP
- Open BSD
- UNIX – HP
- UNIX – Other (see the *Users' guide* for details)
- UNIX – Solaris

The device profiles created as a result of *Autodiscovery* are stored in tables as are vulnerabilities, scan policies, and so on.

Discovered devices

Devices discovered during *Autodiscovery* are automatically assigned to a group. If you have a small number of devices, this may be the default group that is automatically created when VAM installs. For larger installations (more devices), you can use groups you create to organize and manage VAM. For more information on groups, see "Groups" on page 19.

VAM creates and maintains a unique device profile for each unique IP address it has discovered on your network. A device profile is also created for any devices imported via the API.

Autodiscovery performance and optimization

The size and complexity of your network will determine the amount of time required to complete the *Autodiscovery* process.

Autodiscovery is flexible; it can be run manually or automatically (the default), it can be configured per scanner installed, and it can be disabled. You can also *Autodiscover* devices on-demand, via the On-demand scan capability.

For example, specifying multiple, specific network ranges as opposed to one large network range can make scanning for new devices a more efficient process. For more information on fine-tuning your VAM installation, see "Performance tuning" on page 21.

Scan

VAM performs the following four types of scans:

- Scheduled scans:
  - Device discovery only (no port scans included)
  - Vulnerability scanning (includes device discovery)
- On-demand scans
  - Device discovery only (no port scans included)
  - Vulnerability scanning (includes device discovery)

On-demand scans

An *On-demand scan* enables you to do immediate scans with minimal configuration.

The following examples illustrate how an on-demand scan meets your scanning needs:

- **Provides immediate information** – Scan devices by entering a single IP address or range of IP addresses to get information about a device, or range of devices (great for auditors or admins responding to executive inquiry).
- **Checks for new exploits** – Scan across specific devices when a new exploit comes out—select a scan rule (Intelliscan™ or selected rules), input an IP range and start scanning!
- **Scans unknown devices** – Scan an unknown device that has appeared on your network.
- **Verifies repairs** – Scan to verify a vulnerability on a specific device has been repaired.

Scheduled scans

Once devices have been discovered via *Autodiscovery*, you can assign them to scan policies, which automatically conduct vulnerability scans on a schedule of your choosing. The number of IPs purchased with your subscription determines the number of devices you can scan at any one time. Scanning is conducted by either the *onboard scanner*, through distributed scanner(s), or both.

Scan policies are a collection of *Scan rules* and port scans that test devices for vulnerabilities. VAM utilizes scheduled scan policies that are pre-defined (installed with VAM) or user-defined.

Scans can be intrusive or non-intrusive. Intrusive scans scan more thoroughly by actually exercising various exploits, but can cause a server to crash or malfunction. Intrusive scans should be performed on occasion, as that is what a hacker will try to do to your system, but should be scheduled for non-critical hours or days.

At the scan-policy level, you can specify that only certain ports are allowed to be open.

Pre-defined scan policies

VAM installs with five pre-defined scan policies:

- Hourly+
- Daily+
- Weekly+
- Monthly+
- SANS Top 20 Internet Security Vulnerabilities

Each pre-defined scan policy (except SANS Top 20 Internet Security Vulnerabilities) includes an *Intelliscan* and additional port scans (if enabled). *Intelliscan* runs at the frequency indicated by the policy name, for example, Hourly. The SANS Top 20 Internet Security Vulnerabilities policy runs on a variable, customizable schedule.

VAM automates the process of applying scan rules to devices with its *Intelliscan* capability. Based on the device type (for example, a Web server or an application server), *Intelliscan* automatically determines which *Scan rules* are appropriate. (**Note**: The SANS Top 20 Internet Security Vulnerabilities scan policy does not include *Intelliscan*.) You need only assign the device to a pre-defined scan policy; VAM takes over from there, applying the appropriate vulnerability scans to that device.

Scheduled scan policy attributes include the number and types of scan rules included and the frequency the rules are run.

The SANS Top 20 Internet Security Vulnerabilities scan policy is a pre-defined scan policy that scans devices for the vulnerabilities on the SANS Top 20 Internet Security Vulnerabilities list. As the SANS organization updates their list of the most commonly exploited vulnerabilities, this scan policy is automatically updated during rule updates to reflect the changes.

User-defined scan policies

User-defined (custom) scan policies have the same attributes as pre-defined scan policies with the added benefit of rule specification—you can specify which rules to run.

You might create a custom scan policy if you have a number of similar devices you want to scan in a specific way. For example, you could create a custom scan policy to verify that all of your Lotus Notes servers have no Lotus Notes-related vulnerabilities.

Port scans

Within a scan policy, you can select from the following port scans:

- TCP ports
- UDP common ports
- UDP ports 1 – 1024
- UDP ports 1 – 65535

UDP common ports are those ports that are most commonly used. These are stored in a database and can be modified by the user via the command line.

Scan rules

Scan policies consist of any number of scan rules. Each scan rule tests a device for a specific security vulnerability. Applying a scan rule to a device yields one of the following results:

- **Successful pass** – The device does not have the specific scan rule vulnerability.
- **Scan rule violation** – The device does have some vulnerability specified in the scan rule. VAM then initiates the *Vulnerability Repair Workflow* process for that vulnerability.
- **Scan execution failure** – The most common reason for execution failure is when VAM cannot connect to a device because the device is powered off. An execution failure will also occur if there is a network problem—if your network is down, every device will fail.

VAM uses the Nessus remote security scanner to execute its security tests as scan rules.

Scan rule parameters

Each scan rule has several parameters as shown in the following table:

Table 2: Rule parameters

Item	Description
Severity	Indicates the importance of the vulnerability. These classifications are set and defined by the Nessus open source community and are imported as part of the Nessus test definitions. The classifications are based on a number of factors including if the vulnerability is being exploited, if the Internet infrastructure is at risk, the number of systems on the Internet at risk, how easy it is to exploit the vulnerability, the preconditions required to exploit the vulnerability, and if the information about the vulnerability is widely known. Possible values are: • Critical • Major • Minor

Table 2: Rule parameters (cont.)

Item	Description
Rule family	A grouping of similar rules. The categories of rule families are: • Backdoors • CGI Abuses • Cisco • Default UNIX Accounts • Denial of Service • Finger Abuses • Firewalls • FTP • Gain a shell remotely • Gain root remotely • General • Misc (local rules are here for the VAM v5.0 release) • Netware • NIS • Peer-to-peer File Sharing • Remote file access • RPC • Settings • SMTP problems • SNMP • Useless services • Windows • Windows: User management
Scan rule type	Rule type. Possible values are: • Intrusive • Non-intrusive
External references	Most vulnerabilities are categorized by one or more external security organizations for the purpose of information dissemination and vulnerability classification. The major organizations are SecurityFocus' Buqtraq (http://www.securityfocus.com/), and Mitre's Common Vulnerabilities and Exposures (http://cve.mitre.org/). If the vulnerability being described is catalogued by these other organizations, VAM displays a link that allows you to view additional information about the vulnerability. **Note**: *SecurityFocus and Mitre links are provided for your convenience. StillSecure does not warrant that these links are accurate or updated.*
Description	The description of the scan, what it scans for, what results in a vulnerability, and how to resolve it.
Scan details	Displays the scan history if the vulnerability has been discovered on a device.

Scan rule example

The **Finger abuses** family currently contains 10 rules. The **Solaris finger disclosure** timing attack rule has the following description:

Table 3: Solaris finger disclosure RULE example

Item	Description
Severity	Major
Rule family	Finger abuses
Scan rule type	Non intrusive
External references	StillSecure: Ref #10788 Bugtraq: Ref #3457 CVE:
Description	There is a bug in the remote finger service which, when triggered, allows a user to force the remote finger daemon to display the list of the accounts that have never been used, by issuing the request: finger 'a b c d e f g h'@target This list will help an attacker to guess the operating system type. It will also tell him which accounts have never been used, which will often make him focus his attacks on these accounts. Solution: disable the finger service in /etc/inetd.conf and restart the inetd process, or apply the relevant patches from Sun Microsystems.

Rule updates

VAM can be configured to automatically check for and integrate the latest vulnerability scan rules as often as hourly, ensuring up-to-the-minute protection against newly discovered threats.

VAM polls the StillSecure update site to check for new scan rules. If there are new scan rules, VAM updates the scan rule database. Stillsecure *never* contacts the VAM server to push rules. New scan rules are automatically assigned to a scan policy as they are integrated. The next time a scan policy runs, VAM automatically assigns new rules to the appropriate devices through *Intelliscan*.

VAM does not delete old rules. Deprecated rules (rules that are obsolete or rules that have been replaced with improved rules) are not used for vulnerability scanning but remain in the database to support previously discovered vulnerabilities associated with these rules.

Scheduling frequent rule updates offers the highest level of protection for your network.

Scan policy performance and optimization

Each Scan policy has four possible frequencies for rule scanning: Hourly, Daily, Weekly, and Monthly. Scheduled scan policies are already optimized to run as fast and accurately as possible for any given rule.

Custom (pre-defined) scan policy rules should be organized so that you attain maximum scanning coverage while not overburdening your network, servers, or VAM installation. Keep the following points in mind while organizing your rules:

- Devices deemed mission-critical can be scanned hourly or daily, while less critical devices can be scanned weekly or monthly.
- VAM performs two types of port scans:
  - **TCP** – TCP port scans generally run quickly when scanning a device.

– **UDP** – UDP port scans, on the other hand, can take a long time to complete because of how some devices respond when multiple UDP ports are scanned. To ensure efficient scanning, VAM provides three UDP port scans: (1) common UDP ports, (2) UDP ports 1-1024, and (3) UDP ports 1-65535. The common UDP ports scan is the quickest since it has the fewest ports to scan, whereas the UDP ports 1-65535 port scan can take more than 24 hours to perform on some devices. *Scheduled scan policies* use combinations of these different types of port scans.

False-positive scan results are results that may indicate a vulnerability when none actually exists. For example, a Linux box is not vulnerable to a Windows attack, but may be indicated as vulnerable after a scan. *Intelliscan* takes advantage of this knowledge to dramatically reduce the incidence of false-positive scan results. You can also organize your scan policies in a similar fashion. See "Performance tuning" on page 21 for more information on fine-tuning your VAM installation.

Assign

Vulnerabilities are automatically assigned to individual(s) responsible for repair, ensuring accountability. The *Vulnerability Repair Workflow* automatically does the following:

- Notifies and assigns appropriate staff when new vulnerabilities are found.
- Assigns vulnerabilities, showing who is responsible.

Repair

VAM's Vulnerability Repair Workflow™ tracks and facilitates the repair of all identified vulnerabilities through repair verification, providing clear accountability throughout the remediation process. The workflow automatically prioritizes repair schedules based on the affected device's importance. The *Vulnerability Repair Workflow* automatically does the following:

- Tracks vulnerabilities, showing who is responsible, the scheduled repair date, and the progress of repairs in Gantt chart format.
- Performs verification scans on reported repairs.
- Compiles a complete device history for meeting compliance and auditing requirements.

VAM v4.0 and later incorporates patch management via Microsoft's Systems Management Server (SMS); assign repairs to SMS and let VAM manage the repair process, removing the vulnerability from the workflow when the patch has installed successfully.

Vulnerability states

The core of VAM's *Vulnerability Repair Workflow* is its state engine. Each vulnerability can exist in one of seven possible states:

- **Found (F)** – A vulnerability has been found on a device
- **Confirmed (C)** (optional) – A vulnerability has been confirmed and some action has been assigned. For example, it has been assigned to a repairer, discarded, or ignored.
- **Under repair (U)** – A vulnerability is being evaluated/repaired by a repairer.
- **Pending repair verification (P)** – A vulnerability has been repaired and is awaiting a follow-up scan to verify the repair. This can be manually initiated if desired. If the verification scan indicates the vulnerability is not repaired, it is moved back to the under repair state.
- **SMS repairs in progress** – A vulnerability has been assigned to SMS for repairs, but the repairs have not yet been reported as fixed.
- **Repaired (R)** – When a verification scan verifies that a vulnerability has been repaired, VAM automatically assigns it to the Repaired state.
- **Ignored (I)** – A vulnerability has been assigned the Ignored state and will be ignored by VAM.

Moving a vulnerability from one state to another is done by the user based on the roles and responsibilities assigned and by VAM for SMS-assigned repairs.

Roles and responsibilities

VAM's Vulnerability Repair Workflow™ allows the administrator to assign the following roles:

- **Confirmer** – The person who verifies the validity of a newly found vulnerability. Confirmers verify that vulnerabilities found by VAM are legitimate. Confirmers assign discovered vulnerabilities to repairers.
- **Primary repairer** – The first person assigned to repair a vulnerability. Repairers fix vulnerabilities that have been found on devices in your network. You can assign both a primary and a secondary repairer.
- **Secondary repairer** – Backup person assigned to repair a vulnerability.
- **Owner** – The owner of the device; this person may or may not participate in the Vulnerability Repair Workflow.

Repair schedule

As part of its workflow management features, VAM automatically assigns each vulnerability a repair schedule. The length of the repair schedule is driven by the importance level you assign to each device. The default value for the repair timeframes are shown in "Repair timeframe default values" on page 16:

Table 4: Repair timeframe default values

Days	Item
3	High importance devices
7	Medium importance devices
14	Low importance devices

These values can be changed globally, or on a per-vulnerability basis.

Device importance levels

Device importance levels are used to prioritize repairs and define repair schedules. Assign devices to importance levels based on your specific business needs. For example, the following assignment criteria are suggested:

- **High** – Mission critical, sensitive data, downtime impact (for example, a public web server, business-to-business (B2B) server, or a mail server)
- **Medium** – Downtime impact (for example, an Intranet web server or a file server)
- **Low** – None of the above (for example, an individual's computer)

Notifications

When new vulnerabilities are discovered, or as vulnerabilities progress through the repair workflow, VAM notifies (via email) users when they have new tasks requiring their attention. These notifications are assigned at a global level based on the users' default workflow roles.

VAM also automatically notifies users and (optionally) non-VAM users when events occur that require their attention. These notifications are separate from the emails that are sent to users with defined workflow roles (discussed in the previous paragraph).

The events for which notifications can be sent are:

- **When a new device is discovered** – VAM sends notifications when *Autodiscovery* discovers devices not previously known to VAM.
- **When a workflow state is changed** – VAM can send notifications when the workflow state of a vulnerability changes.
- **When a vulnerability is ignored** – When a vulnerability on a device is selected to be ignored, an email notification can be sent to other email accounts such as a security administrator.

VAM sends these email notifications to the email address associated with the user's VAM account. Additional email notifications can be sent to non-user email addresses, distribution lists, and pager email accounts.

Notifications are assigned by group. Each group you maintain in VAM can have a unique notification setup.

Device history

Device history is a collection of all vulnerabilities and repairs for a particular device since it was discovered in the network.

Report / compliance

VAM consolidates data produced by vulnerability scanning and remediation activities and outputs concise, actionable reports tailored to the needs of managers, auditors, and IT staff.

Report types

Generated on a corporate, division, or workgroup level, VAM reports provide concise security status information and detail responsibilities for updates and repairs. Report types include the following:

- **Executive status report** – Highlights how the most important vulnerabilities are being addressed; designed for upper management, auditors, and regulators. Select from the following report options:
  - Scorecard (graph)
  - Repaired vulnerabilities
  - Found vulnerabilities
- **Vulnerability details** – Breaks down all existing vulnerabilities by device, specifying repair schedules and responsibilities. Select from the following report options:
  - Vulnerabilities by importance
  - Vulnerability scorecard
  - Vulnerabilities by severity
- **Vulnerability frequency - current** – Provides details on each type of currently existing vulnerability. Select from the following report options:
  - Summary only
  - Scan details for all devices
  - Expand details
- **SANS Top 20 Internet Security Vulnerabilities** – Breaks down existing SANS Top 20 Internet Security Vulnerabilities by device, device group, time period, and severity.
- **SANS Top 20 Internet Security Vulnerabilities (CSV)** – A comma-separated-value version of the SANS Top 20 Internet Security Vulnerabilities report that is appropriate for importing into a spreadsheet application.
- **SMS Patch summary** – Keeps you up-to-date on what vulnerabilities have been assigned to SMS, when they were assigned, and what the repair status is. Select from the following report options:
  - Summary only
  - Include successful patches
  - Include failed patches
  - Expand details
- **Ignored vulnerabilities** – Provides a listing of vulnerabilities that have been both ignored globally and ignored for specific devices. Select from the following report options:
  - Summary only
  - Scan details for all devices
  - Expand details

Customizing reports

Customize your reports by selecting:

- The report options listed above
- The report period
- Collections
- Scan policies
- Devices
- Vulnerabilities by severity

Report formats

Reports are saved in hypertext markup language (HTML) format and are open database connectivity (ODBC)-compliant so the data can be imported into third-party reporting applications such as Crystal Reports or Excel.

Administration and management

VAM administration consists of managing *User accounts*, creating *Groups*, *Collections*, and performance tuning.

User accounts

All users accessing VAM must have a VAM user account. Each user account is assigned permissions that govern what the user can see and accomplish in VAM.

You can create user accounts from within VAM, or you can import LDAP accounts. When you import LDAP directory information, those imported accounts continue to be managed by LDAP. VAM updates imported account information every six hours.

VAM users can be assigned to multiple VAM groups. When working in the main VAM window, users are only permitted to view information pertaining to the groups to which they belong.

VAM user accounts can be assigned one of four possible permission levels:

- Admin
- Write
- Read
- Disabled

The permissions assigned to an account drive what a user can access and accomplish in the VAM interface. Care must be used, therefore, when assigning permissions. Permissions should be assigned on a need-to-know, need-to-accomplish basis.

Figure 1: User permissions

Permission	Description
Admin	Assign admin permission to users responsible for managing your VAM installation. Admin users have unrestricted access to all VAM functions and belong to all groups. While there should be one primary administrator of VAM, assign admin accounts to people responsible for maintenance of devices on the network.
Write	Assign write permission to users who participate in the *Vulnerability Repair Workflow*. All write-permission users can act as confirmers or repairers, and they can generate reports for the devices they are assigned.

Figure 1: User permissions (cont.)

Permission	Description
Read	Assign read permission to users, such as executives and managers, who need to view the information stored and maintained in VAM. Read users are permitted to view all information in the main VAM screen and generate most reports.
Disabled	User accounts assigned a disabled status have no access permissions whatsoever; their accounts are maintained in VAM, but the user is prohibited from logging onto the system. Disabled accounts can be re-activated at any time simply by assigning one of the other three permissions.

Groups

Groups bring together subsets of devices and the IT staff members responsible for their maintenance. Groups ease administration and facilitate targeted reporting. They allow you to segregate VAM information and control the VAM access provided to various portions of your organization.

Groups are optional; networks containing a modest number of devices may not need multiple groups—the single default group automatically created during installation may be sufficient. You can organize groups by criteria that make sense for your organization, such as physical location or organizational unit. The following figures show local groups and geographical groups:

Figure 2: Figure 5: Local Groups

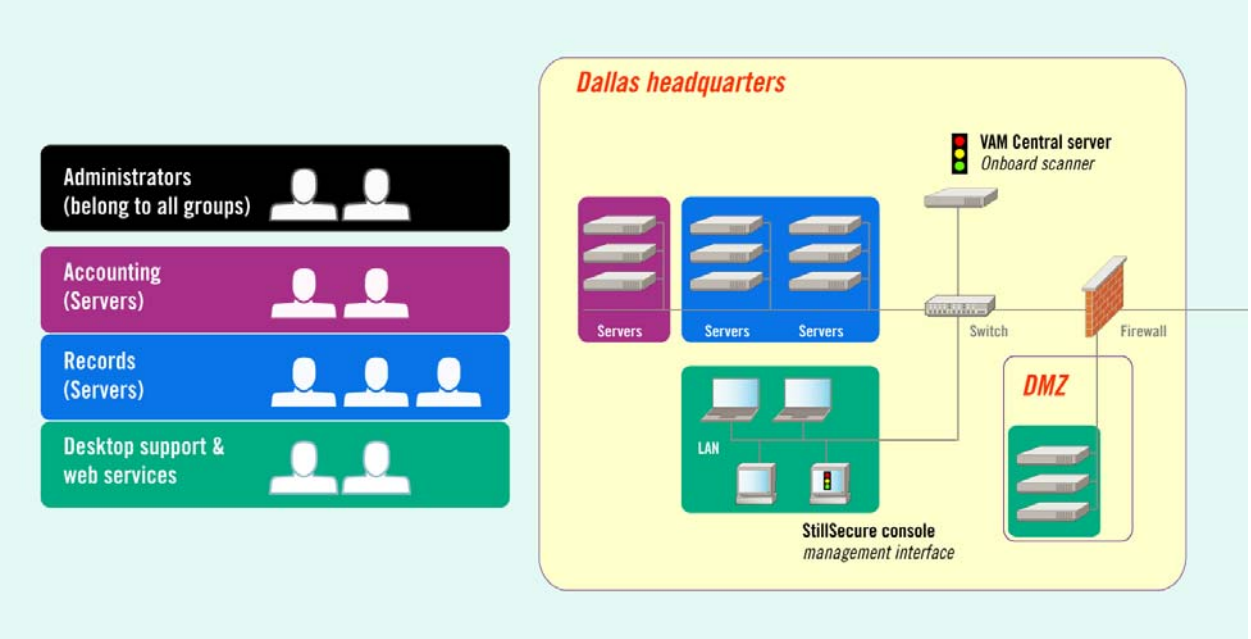
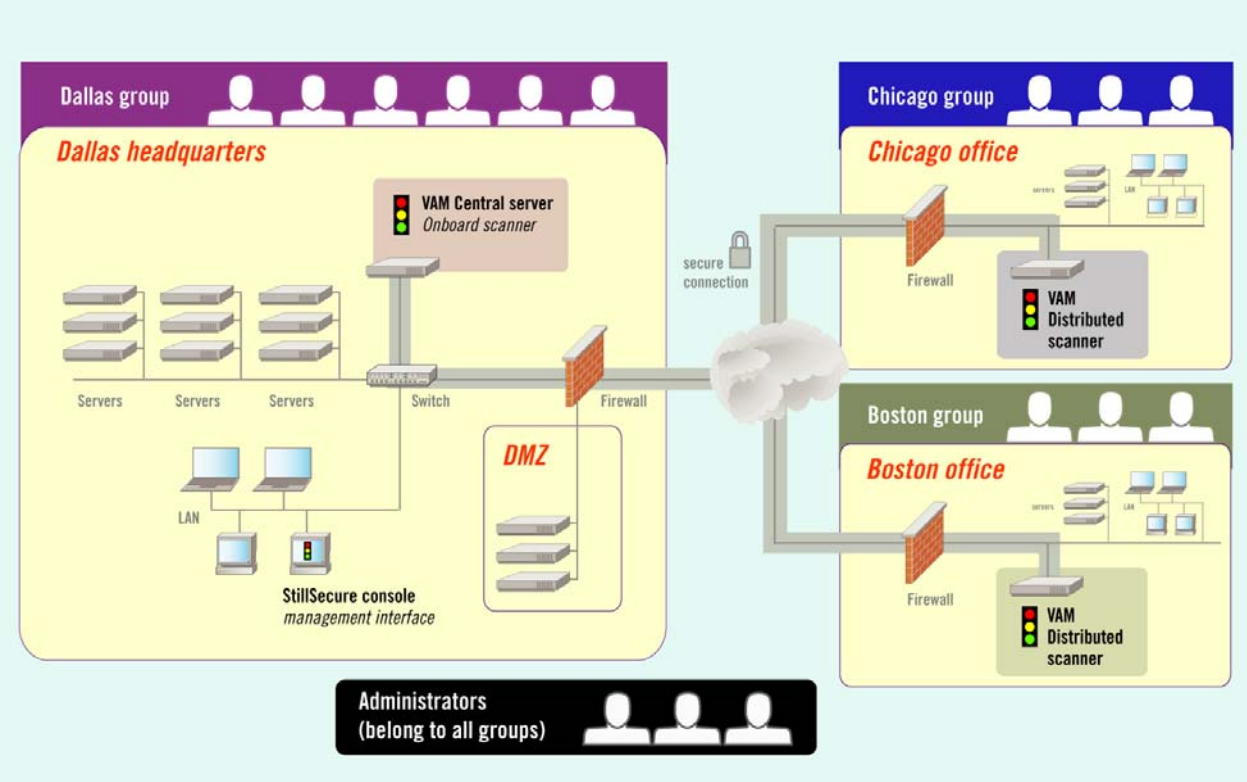


Figure 3: Figure 6: Geographical Groups



If you intend to employ multiple groups, we recommend you create your group structure before autodiscovering devices on your network. By doing so, discovered devices will automatically be assigned to the appropriate group.

Once a group has been created, you can assign VAM users to the group and move devices between groups. A device can belong to only one group at a time.

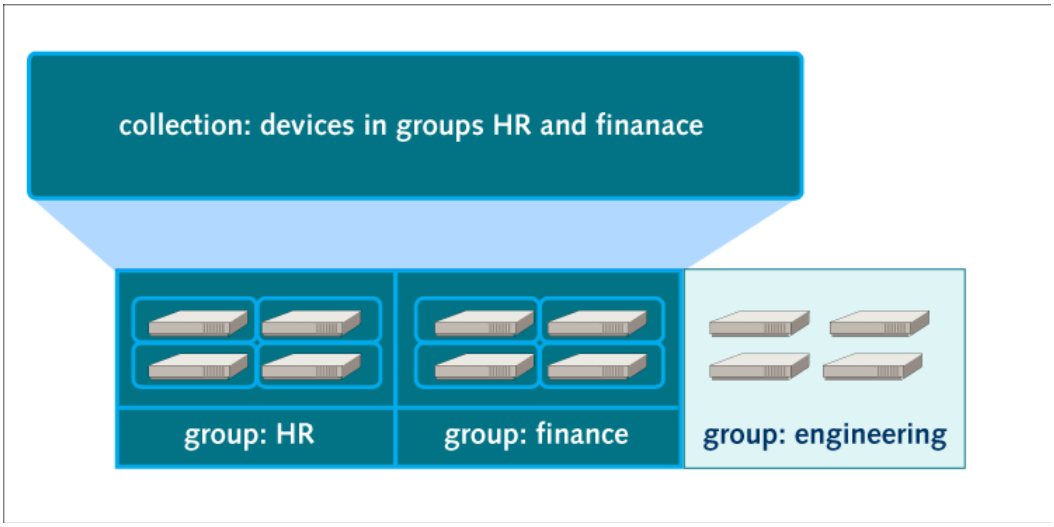
There are a number of points that apply to groups in VAM:

- Users with admin permissions belong to all groups. They can see everything in VAM configuration and in all groups.
- Devices can belong to only one group; users can belong to multiple groups. This is important because you want only one person to be accountable for keeping a device secure. If a device were in several groups, repair activities could slip through the cracks if one person thinks the other will repair.
- You cannot delete an existing group without moving devices and workflow participants to other groups. This ensures that you will never lose a device once it has been placed in VAM. Devices with vulnerabilities will not get lost because the vulnerability repairs are tied to users. A device may only be deleted from VAM by deleting the device profile.

Collections

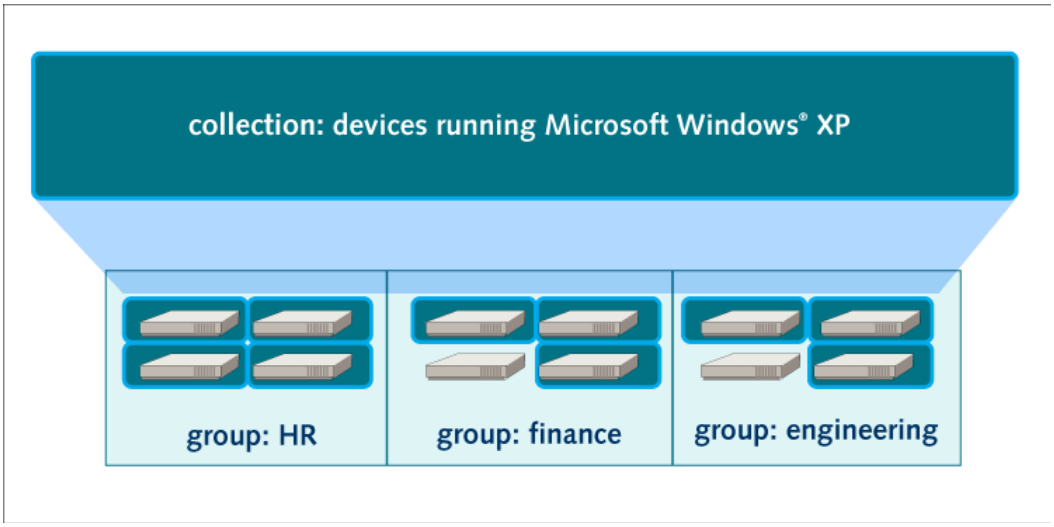
Collections let you define and work with sets of devices based on flexible user-defined attributes. These attributes include IP, device name, descriptive name, operating system, NetBIOS name, DHCP device, group, scanner name, discovery date, device importance, notes, and more. For example, create a collection containing the HR and Finance groups as shown below:

Figure 4: Collection of all devices in HR and Finance groups



You can also create a collection based on other attributes, such as devices running the Microsoft Windows XP operating system as shown below:

Figure 5: Collections of all Windows XP devices



You do not have to do anything to associate devices with collections; collections automatically include devices based on attributes that you define. A device can belong to any number of collections. Once you create the expressions that define your collection, VAM automatically associates devices that match the expressions with the collection, and shows the expression at the bottom of the window in a query format that you can copy and use in third-party applications, such as Crystal Reports. The collections capability allows you to filter by collection in the workflow, groups, scanners, scan policies, and reports.

Performance tuning

Performance tuning is the balancing of performance and accuracy by fine-tuning the scan parameters. It is possible to scan networks at a rapid pace; however, you sacrifice accuracy. Alternatively, you can ensure accuracy by reducing speed of scans. This balance is critical for organizations to understand and is easy to manage with VAM.

There are many factors to be considered in fine-tuning VAM to run optimally. VAM's default settings will suit most users; however, you do have the ability to make adjustments. The configurable scan parameters and their effect on performance follow:

- **IP addresses to be scanned** – Specifying multiple, specific network ranges as opposed to one large network range can make scanning for new devices a more efficient process.
- **Concurrent port and vulnerability scans** – Specifying the number of concurrent scans run allows you to optimize the performance of your scanner hardware. If you have more powerful hardware (in terms of resources available), you can run more scans at the same time. Providing the option to specify port and vulnerability scans separately allows you to choose where to dedicate your hardware resources.
- **Scan timeout** – This parameter can be adjusted to optimize scan time with regard to latency in your network. A lower value for a low latency network (such as LAN), and a higher value for high latency networks (such as WAN). Setting this value too low may cause false timeouts, setting it too high adds unnecessary time to the scanning process.
- **Autodiscovery phase details** – The earlier Autodiscovery phases (Phases 1 and 2) run quickly and find easy-to-find hosts. The later phases perform a more in-depth scan to find hidden hosts, and, therefore, take longer to run. However, one of the benefits of Autodiscovery is to discover new, perhaps rogue devices on your network. For this reason, you may want to enable all phases of Autodiscovery.
- **Simultaneous rule execution** – When you are fine-tuning your system, keep in mind that there is a relationship between the number of rules you execute simultaneously and the potential accuracy you see in the results; as the number of rules increase, the potential accuracy decreases.
- **OS scanning parameters** – Operating system detection can be enabled and disabled as another option when you are fine-tuning your system for optimum performance.
- **Optimize tests** – This parameter can be enabled or disabled to balance vulnerability scan time with accuracy (decrease in the number of false-positive results).
- **Logins** – Device logins allow the VAM scanner to access services and perform more detailed vulnerability scans and include: FTP, HTTP, POP2, POP3, IMAP, and SMB.
- **Use knowledgebase** – The knowledgebase saves previous host scan information to be used in future scans. Enabling the knowledgebase may reduce bandwidth and reduce the time to obtain results, but there is an increased risk of missing a vulnerability or an open port due to the re-use of old information.

Archiving data

Beginning with VAM v4.0, the system automatically archives the entire database once daily on the VAM Central server. This archive is provided as a means to roll back a database within 24 hours in case of user error or data corruption in the primary database. This archive is not meant to replace a regular database backup.

Using VAM with TT and CM systems

VAM exports details of each vulnerability and workflow state change into a log file that you can use as input to a trouble ticketing (TT) or configuration management (CM) system.

Application programming interface

The StillSecure API extends VAM capabilities, allowing you to import and export data into and out of VAM via the *VAM Integrated Framework*™. This provides an interface framework for integrating VAM with your existing systems. For example, allow a ticketing system to modify the workflow when a vulnerability-related ticket is closed, so the repair of the vulnerability can be verified by VAM.

System requirements

"System requirements" on page 23 lists the VAM system requirements:

Table 5: System requirements

Component		Minimum	Recommended
Central server – A dedicated server with the following system requirements			
	Processor	Pentium III 800 MHz	Pentium III 1.2 GHz
	RAM	512 MB RAM	1.0 GB RAM
	Disk space	9 GB	9 GB
	Network interface card	One network interface card 10/100 (3Com or Intel)	One network interface card 10/100 (3Com or Intel)
	Internet	An Internet connection that allows outbound SSL communications	
Workstation – Workstation running one of the following browsers with 128-bit encryption: *Windows*: • Mozilla Firefox 0.93 (or higher) • Mozilla 1.7 (or higher) • Internet Explorer 6.0 (or higher) *Linux*: • Mozilla Firefox 0.93 (or higher) • Mozilla 1.7 (or higher)			
Distributed scanner – VAM Distributed scanners are shipped as preconfigured hardware appliances. DSs are available as either single-CPU or dual-CPU appliances.			
License – A subscription license key			
Product updates – The latest VAM product updates			

Glossary

ACK	Acknowledge – A reply that confirms that the request was received.
Admin permission	Admin users have unrestricted access to all VAM functions and belong to all groups.
API	Application program interface – a way that two programs can communicate. APIs provide functions, rules, and instructions for passing information and instructions between programs.
Autodiscovery scan	The scan (using NMAP) that detects and profiles devices on your network. VAM runs this scan on a regular schedule to ensure all devices are accounted for and to alert you of any new devices that may require vulnerability scanning.
backdoor	A disguised or hidden entry point in a software program or system. An open backdoor can be intentional (for maintenance use), or unintentional. If a backdoor is discovered, malicious users or software can gain entry and cause damage.
Central server	The central server consolidates, centralizes, and secures data from the onboard scanner and any distributed scanners (optional) you have installed on the network. Regardless of where scanning is being performed (onboard or distributed scanners), all data is stored, secured, and managed in the central server, which is generally located on the internal portion of an organization's network. (CS)
CGI	Common gateway interface – A script (program) that extends web server capability and functionality. CGI scripts can be written in many different languages; their primary purpose is to accept and return data that conforms to the CGI specification, allowing programs to interact with the World Wide Web.
collection	Collections let you define and work with sets of devices based on flexible user-defined attributes. These attributes include IP, device name, descriptive name, operating system, NetBIOS name, DHCP device, group, scanner name, discovery date, device importance, and notes.
comma separated value	A file whose elements are separated by a comma. (CSV)
Confirmed (C)	A state in VAM where a vulnerability has been confirmed to exist on a device by the confirmer and assigned to a repairer (confirmation is only required when there is a confirmer assigned to a device).
Confirmer	The person in the VAM workflow who verifies the validity of a newly found vulnerability.
CSV	See comma-separated value
Custom scan policy	A user-defined scan policy, whereby the user manually selects the scan rules to apply to a device and sets the schedule of when the scan policy is run. For example, you might create a *Custom scan* policy if you have a number of similar devices you want to scan in a specific way.
CVE	Common vulnerabilities and exposures – A list of standardized names for vulnerabilities and other information security exposures. CVE aims to standardize the names for all publicly known vulnerabilities and security exposures. (http://cve.mitre.org/)
Default workflow	The global-level assignment of roles in the VAM *Vulnerability Repair Workflow*™.
demilitarized zone	An area of a computer network that provides a layer of security between the network and the Internet.

denial of service	An attack designed to prevent normal operation of a system. Denial of service is usually caused by overloading the servers in some way.
device	A machine found connected to your network. Example devices include servers, desktop computers and routers.
Device history	In VAM, a list and description of the vulnerabilities found and repairs performed over time.
Device importance	In VAM, a device is assigned one of three importance levels: high, medium, or low, depending on the impact to the business should the device be unavailable. The device's importance level is used to determine the repair schedule for vulnerabilities found on that device.
Distributed scanner	A scanner in VAM that resides on a server in your network and communicates with the central server. Distributed scanners are delivered as stand-alone hardware devices with a hardened OS. (DS)
Distributed scanning	Enables VAM to scan remote networks and to scale to very large network environments by using distributed scanners.
DNS	See domain name server
domain name server	A computer that translates domain names (such as latis.com) into IP addresses (such as 216.239.41.99).
DoS	See denial of service
DS	See Distributed scanner
Executive status report	A VAM report that highlights how the most important vulnerabilities are being addressed. It is designed for upper management, auditors, and regulators.
External references	A link to an external source of information in VAM that provides more information on vulnerabilities.
false-positive	False-positive scan results are results that may indicate a vulnerability when none actually exists. For example, a Linux box is not vulnerable to a Windows attack, but may be indicated as vulnerable after a scan.
finger	A UNIX utility that reports back information about UNIX user accounts.
firewall	Hardware or software or both designed to control and prevent access to a network.
Found (F)	In VAM, when vulnerability has been discovered on a device.
FTP	File transfer protocol – An Internet protocol that enables you to transfer files between computers on the Internet.
Gantt chart	A horizontal bar chart used in project management.
Groups	In VAM, groups allow you to organize your network devices and the IT personnel responsible for their maintenance and management.
hacker	A programmer who tries to break into computer systems.
hardened OS	An operating system with no vulnerabilities.
HTTP	Hyper text transfer protocol – An application protocol for transferring files.

HTTPS	Hyper text transfer protocol over secure socket layer or HTTP over SSL – An application protocol for transferring files that utilizes the SSL for increased security of the transmitted information.
ICMP	Internet Control Message Protocol – A standard error and control message protocol used for Internet systems. The commonly-used Ping command uses the echo request / echo reply sequence.
Ignored (I)	In VAM, when a vulnerability is designated as not applicable to this device and should be ignored this time or forever. You can choose to ignore a vulnerability at any point in the workflow.
IMAP	Internet Message Access Protocol – A standard protocol for accessing email from your server where the email is stored on the server.
***Intelliscan*™**	An intelligent scan in VAM that automatically selects and applies the scan rules appropriate for each device. *Intelliscan* eliminates the need for you to determine which scan rules to apply to each individual device.
intrusive rule	A scan rule that when applied to a device may change the device's state, possibly causing it to malfunction or crash. Intrusive rules may attempt to gain some privileges on the remote host and/or cause network services on the remote host not to function as expected. Caution should be exercised when using intrusive rules.
IP	Internet Protocol – A protocol by which data is sent from one computer to another on the Internet.
knowledgebase	A centralized repository for information. In VAM, a knowledgebase can be selected to store information about recent rule processing.
LDAP	Lightweight Directory Access Protocol – A software protocol that allows lookup functionality over the network.
Linux	A free or low-cost UNIX-like OS.
Management interface	In VAM, the StillSecure Console.
Map	In VAM, the process of discovering devices.
NASL	Nessus Attack Scripting Language – A scripting language designed for the Nessus security scanner.
Nessus	A free, (open source), powerful, remote security scanner.
NetBIOS	Network Basic Input/Output System – A program that allows applications on different computers to communicate within a LAN.
Netware	Made by Novell, a commonly-used network server OS.
network information system	A network naming and administration system for small networks.
NIS	See network information system
NMAP	Network Map – An open source component that accomplishes the task of OS and application fingerprinting.
Onboard scanner	The scanner that installs with the VAM central server.
open source	Software that is intended to be freely shared, improved, and redistributed.

operating system	The program manages all the other programs in a computer.
OS	See operating system
Owner	In VAM, the owner of the device; this person may or may not participate in the *Vulnerability Repair Workflow*™.
Peer-to-peer	A communications model in which each workstation has the same capabilities and responsibilities. Either workstation can initiate a communication session; that is, all workstations can function as client and server.
Pending repair verification (P)	In VAM, when the repairer has indicated the vulnerability has been repaired and is ready to be verified by a scan. The user may initiate the scan or allow the system to run as scheduled. If there's more work to be done before a verification scan should be run, a repairer can move the vulnerability back to *Under repair*.
POP3	Post Office Protocol 3 – A standard protocol for receiving email where email is downloaded from the server to your computer.
port	A physical or logical connection place.
Port scan	VAM performs two types of port scans: TCP and UDP. TCP port scans generally run quickly when scanning a device. UDP port scans, on the other hand, can take a long time to complete because of how some devices respond when multiple UDP ports are scanned.
Primary repairer	In VAM, the first person assigned to repair a vulnerability.
On-demand scan	In VAM, a method to scan that allows you to do on-demand scans with minimal (quick) setup.
Read permission	In VAM, a permission level where the user has read but not write access.
remote procedure call	A protocol where one program can request a service from another program on a different computer in a network without knowing the network details.
Repair schedule	In VAM, the date a vulnerability is scheduled for repair.
Repair verified (R)	In VAM, when a scan has been run that verifies the vulnerability no longer exists.
Roles	In VAM, a function assigned to a user (for example, confirmer).
root	The base of something. The lowest-level directory, or the administrator (owner) of a system.
router	A computer or internetworking device that directs traffic and moves packets between networks.
RPC	See remote procedure call
Rule family	In VAM, a categorization of rules into similar types.
SANS	SysAdmin, Audit, Network, Security – SANS Institute is a trusted leader in information security research, certification and education. (http://www.sans.org)
SANS Top 20 Internet Security Vulnerabilities list	The SANS Top 20 Internet Security Vulnerabilities List is a prioritized list of the 20 most critical internet security vulnerabilities that require immediate remediation. It is compiled by the SANS Institute and the National Infrastructure Protection Center (NIPC).

SANS Top 20 Internet Security Vulnerabilities report	In VAM, a reporting of the SANS Top 20 Internet Security Vulnerabilities vulnerabilities found on your system.
Scan policy	In VAM, a collection of scan rules that test devices for vulnerabilities. VAM installs with five pre-defined scan policies: Hourly+, Daily+, Weekly+, Monthly+, and SANS Top 20 Internet Security Vulnerabilities.
Scan rule	In VAM, a scan rule tests a device for a specific security vulnerability. Applying a scan rule to a device yields one of two results: (1) a successful pass of that scan or (2) a scan rule violation, which results in VAM initiating the *Vulnerability Repair Workflow* ™process for that vulnerability.
Scheduled scan policy	In VAM, a pre-defined scan policy (supplied with the installation) or a user-defined (custom) scan policy.
Secondary repairer	In VAM, the backup person assigned to repair a vulnerability.
severity	A classification of a vulnerability that indicates the importance level. This classification is based on a number of factors including if the vulnerability is being exploited, if the Internet infrastructure is at risk, the number of systems on the Internet at risk, how easy it is to exploit the vulnerability, the preconditions required to exploit the vulnerability, and if the information about the vulnerability is widely known.
shell	A UNIX term for the user interface of an OS. A shell is the programming layer that understands and executes commands (command interpreter) entered by a user.
SMTP	Simple Mail Transfer Protocol – A TCP/IP protocol used in sending and receiving email. Used in conjunction with POP3 or IMAP.
SNMP	Simple Network Management Protocol – A protocol governing network management and the monitoring of network devices.
SSH	Secure Shell or Secure Socket Shell – A UNIX-based command interface and protocol used to securely gain access to a remote computer.
SSL	A commonly-used protocol that manages the security of message transmissions over the Internet.
switch	A device that routes incoming data from any of multiple input ports to a specific output port in the direction of the data's intended destination.
TCP	Transmission Control Protocol – A protocol (set of rules) used (with IP) to send data over the Internet.
telnet	A protocol used for accessing remote computers
UDP	User Datagram Protocol – A limited-service protocol used to exchange messages between computers over the Internet.
Under repair (R)	In VAM, when a vulnerability has been assigned to and accepted by a repairer.
UNIX	A multi-user multi-tasking operating system.
User account	All users accessing VAM must have a VAM user account. Each user account is assigned permissions that govern what the user can see and accomplish in VAM.
VAM	Vulnerability Assessment and Management
VAM Console	The management interface into VAM.

Verification scan	In VAM, a scan run to verify that a vulnerability has been repaired.
vulnerability	A security threat that has been discovered on a device. A device has a vulnerability when a scan rule violation occurs.
Vulnerability details report	In VAM, a report that breaks down all existing vulnerabilities by device, specifying repair schedules and responsibilities.
Vulnerability frequency report	In VAM, a report that provides details on each type of currently existing vulnerability.
Vulnerability Repair Workflow™	The highly automated process of managing the repair of a vulnerability from the time it is found through its repair. There are five workflow states that a vulnerability can be assigned as it progresses through the workflow. VAM automatically assigns vulnerabilities to the individuals responsible for repairs and schedules repair due dates as designated by the device importance level
Vulnerability scanning	In VAM, the process of scanning a network for vulnerabilities.
Windows	An OS that runs on top of DOS and provides a GUI environment.
Write permission	In VAM, a permission level where a user has the ability to write and configure.