



Refense VMS™ 4.0 Benefits and Features Overview

Refense VMS is a focused proactive vulnerability management solution for the backbone of every IT infrastructure, the network. Devices such as firewalls, routers, switches and wireless access points are required to be highly available and secure as they are the providers of LAN and WAN connectivity. A security compromise within these devices would be devastating. Refense VMS performs an automated in depth scan of firewalls, routers, network switches and wireless access points and identifies vulnerabilities internal to the device and non-compliance against security policies and standards. By eliminating the need for performing manual vulnerability assessments on these devices, Refense VMS significantly reduces the time, cost and effort required to secure your network.

Below is a list of some of the major benefits and features of Refense VMS.

Feature	Description	Benefit
Supports Market Leading Network Devices	Refense VMS supports: <ul style="list-style-type: none"> ▪ Firewalls ▪ Routers ▪ Switches ▪ Wireless Access Points 	Support for market leading devices helps provide a complete view of critical portions of a network infrastructure. Refense Technologies is continually adding support for other popular network devices.
Enterprise Scalability	Refense VMS scales to support the largest enterprise networks consisting of thousands of firewalls, routers, switches and wireless access points.	A manual security assessment on thousands of network devices is a tedious, intensive and inconsistent process. Refense VMS centralizes, standardizes and automates the assessment process.
Predefined Security Policies	An extensive array of predefined security policies are provided. These policies are based upon research and recommendations from organizations such as NSA, NIST, and SANS as well as the vendors such as Cisco and Avaya.	Preconfigured policies support industry best practices, standards and regulations. This provides the ability to quickly and easily receive detailed results.
Comprehensive Security Checks	Over 100 checks detect security vulnerabilities such as insecure and unneeded services, insecure routing protocols, insufficient and or non-existent encryption, DoS vulnerabilities, and insecure access mechanisms.	These security checks help secure some of the most critical vulnerabilities within network devices. Refense Technologies has the most sophisticated checking logic in the industry and is continually adding new checks.
Supports Wireless Access Points	Performs a detailed security scan of the wireless device to ensure a secure wireless configuration within the device operating system.	A single insecure wireless access point can provide open access to your network. Refense VMS can help ensure your wireless network devices are secure.

Scheduled Scans	Automated scheduled scans which can be configured to run hourly, daily, weekly, monthly, to almost any schedule to meet your needs.	Scheduled scans provide the ability to perform security assessments during off hours and or according to periodic schedules.
Comprehensive Policy Management Interface	The Policy Manager is an easy to use application that allows you to customize preconfigured policies or completely create a new policy based on your requirements.	Provides the ability to easily customize security policies and create new policies within a matter of minutes.
Supported by our Security Threat Research Center (STR)	Support provided by our dedicated research center which analyzes current security vulnerabilities relevant to network devices.	Based upon research and customer feedback, the Refense STR provides timely product updates and security checks.
Detects Unencrypted and Insecure Passwords	Provides the ability to identify passwords that are not encrypted within the configuration and do not meet industry best practices for length and password complexity.	A strong password is one of the first lines of defense towards ensuring a secure network device. Refense VMS can ensure your login passwords are secure and compliant to your policies and standards.
Detects Unused Enabled Switch Ports and Interfaces	Enables users to identify ports and interfaces within network devices which are not used, but are enabled.	Unused ports and interfaces could provide an attacker access to your network. Detecting unused enabled ports across the enterprise helps towards ensuring a strong security perimeter.
Completely Non-Intrusive	Refense VMS has little to no performance impact on a device as all processing is performed on the Refense VMS appliance.	The non-intrusive nature of Refense VMS ensures your network infrastructure will not be affected by the scanning.
Strong In Depth Reporting	Powerful reporting enables you to define the specific information to be viewed.	In depth reporting provides concise detailed security information.
Offline Scanning Capabilities	Provides the ability to perform security scans even if network access is not available.	This allows security audits to be performed without any network access to the device.
Logical Groupings of Devices	Logical device groupings enable you to group devices based upon any criteria you select.	This allows the ability to group devices via their purpose, location or model, etc.

About Refense Technologies

Refense Technologies is a leading provider of vulnerability management solutions for network devices. The company develops solutions that address security concerns within network devices, the foundation of an IT infrastructure. With Refense VMS, organizations can proactively identify and mitigate threats and vulnerabilities within wireless and wired network devices.

For more information, visit our website at www.refense.com or call 1-800-432-6187.