

Your Entire IT Infrastructure Depends Upon Network Devices

If a server is compromised, it is a problem, if a firewall, router or switch is compromised, this is a major disaster as hundreds of systems rely on those devices for connectivity. Network security efforts past and present focus on many areas, application security, database security and more, but almost always network devices such as firewalls, routers and switches are an after thought. Due to the critical role of firewalls, routers and switches, they are an attractive, popular target for attackers who frequently seek to disrupt IT operations and or compromise sensitive data.

> Refense OnDemand™, our Software-as-a-Service, proactively discovers and helps mitigate vulnerabilities within firewalls, routers and switches which threaten the availability and integrity of those devices.

Discover Your Vulnerable Wireless Networks, Before Attackers Do

Recent research from RSA Security demonstrated that 63% of wireless networks surveyed were insecure and vulnerable to attackers. Enterprises across the globe have already or are starting to rapidly deploy wireless LAN's, to leverage the increase in productivity and cost savings. This additional connectivity does not come without risk, as a single insecure wireless access point could provide attackers an open door into a network, effectively bypassing other security measures. To further complicate the issue, discovering that insecure wireless access point among hundreds of wireless access points, is akin to the proverbial "needle in a haystack".

> Refense OnDemand™ provides an automated solution to identify security vulnerabilities within wireless access points across the entire enterprise. This enables organizations to ensure they are securely configured and more importantly that they stay that way.

The Proactive Security Solution for Network Devices

- > Refense OnDemand™ is a vulnerability management solution dedicated to identifying and mitigating threats and vulnerabilities within network devices
- > Proactively detects vulnerable wireless access points, pinpointing vulnerabilities such as lack of wireless encryption, access control and much more
- > Identifies current and potential vulnerabilities within firewall, routers and switches in areas such as SNMP, AAA, logging, etc.

Based on Industry Best Practices and Standards

Refense OnDemand™ enables organizations to perform real time vulnerability scans utilizing predefined security policies which can be completely customized for compliance to specific policies and standards. Our predefined policies are based on industry best practices and recommendations from NSA, NIST, SANS and others.



94% of the financial organizations tested showed basic router vulnerabilities that could put the availability of their online banking systems in jeopardy .

—NTA Monitor

Through 2009, 70% of successful wireless attacks will result from the mis-configuration of wireless devices.

—Gartner

We invite you to try a free evaluation. Contact sales@refense.com or visit us at www.refense.com/trial

Assists in Complying With:

- > DISA STIGs
- > DoD Directive 8100.2
- > ISO27000
- > PCI DSS
- > FISMA
- > HIPAA
- > GLBA
- > Sarbanes-Oxley

Refense OnDemand's intuitive security console gives a complete and concise view of the security posture of network devices across the entire enterprise. Refense OnDemand is provided as a SaaS solution that is available 24/7/365 via a secure web browser. Customers can experience the benefits in minutes by connecting to our OnDemand service.

Policy Manager

Offers over 200 security checks. Choose from a wide range of predefined industry standard security policies or tailor a user defined security policy. The policy manager provides the flexibility of creating baseline security policies to ensure policy compliance across the infrastructure. Policies can also be created to ensure all network devices are not vulnerable to the latest worm or vulnerability that threatens a network.

Dynamic Flexible Reporting

Standard reports designed for both executive and technical audiences, identifies areas of concern and provides actionable intelligence to remedy each vulnerability or misconfiguration.

Supports a wide range of leading network devices

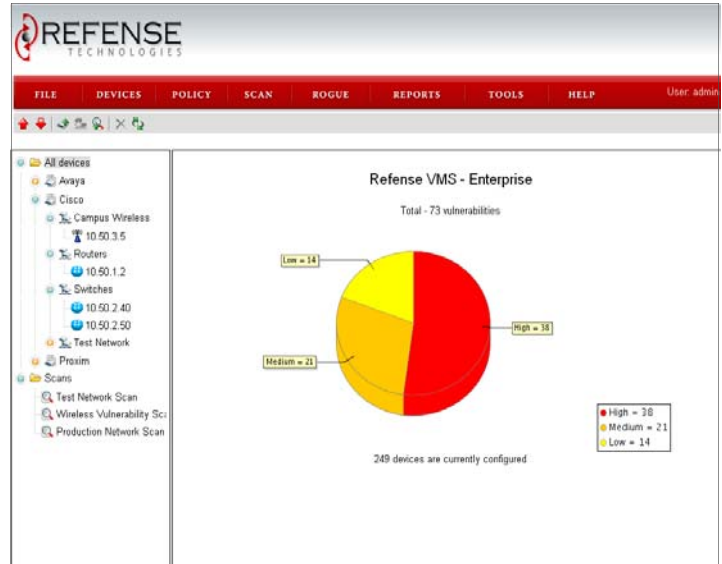
Detects insecure and misconfigured firewalls, routers, switches and wireless access points.

Over 200 security checks

Scans for vulnerabilities such as insecure unneeded services, insecure authentication, lack of encryption, insufficient logging and much more.

Start auditing your network in minutes

There is no hardware, software or agents to install. Simply log in to our secure web interface and start auditing your network for the latest vulnerabilities.



VMS—OnDemand Software as a Service

- > Full Managed Service
- > Efficient, simple solution

VMS—Mobile Software based

- > Designed for Auditors/Consultants
- > Lightning fast

VMS—Enterprise Enterprise Appliance

- > Scales to support 1000's of devices
- > Hardened, high performance system
- > Plug-N-Scan (less 30 min to start)

Models

- VMS-100
- VMS-500
- VMS-1000

About Refense

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 OnDemand, organizations can proactively identify and mitigate threats and vulnerabilities within wireless and wired network devices.



Refense Technologies, Inc
105 Brooks Ave
Raleigh, NC 27607
Phone 1.800.432.6187
sales@refense.com
www.refense.com