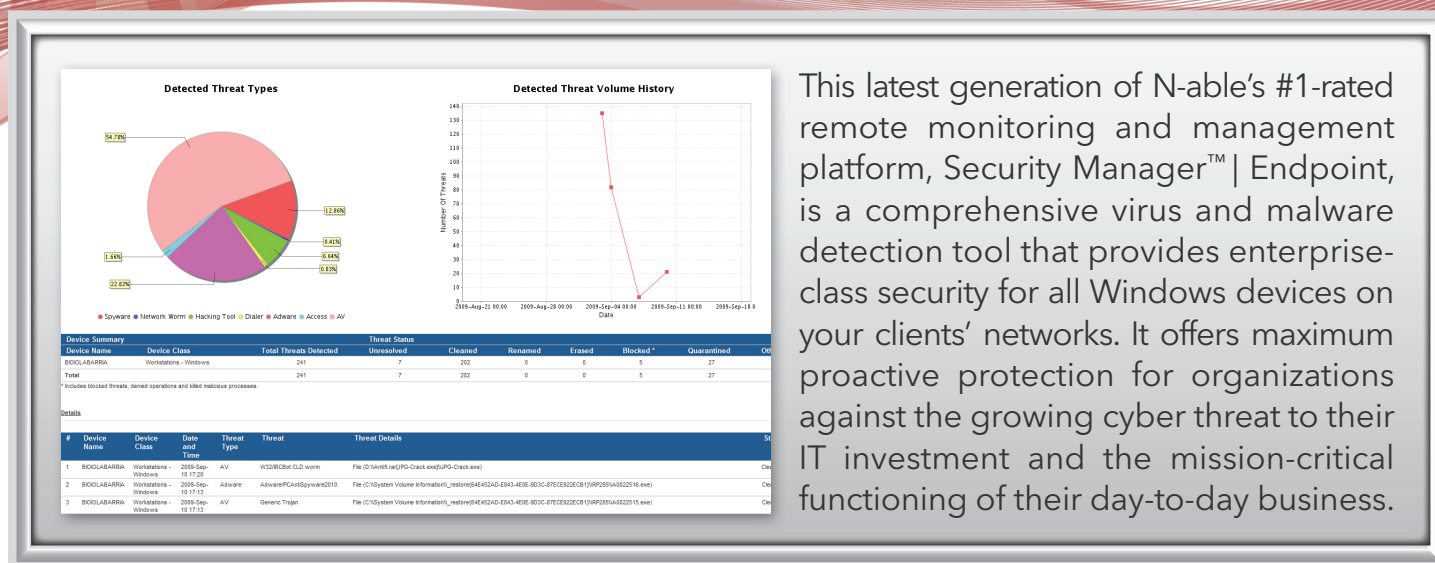




ENDPOINT SECURITY MANAGER



This latest generation of N-able's #1-rated remote monitoring and management platform, Security Manager™ | Endpoint, is a comprehensive virus and malware detection tool that provides enterprise-class security for all Windows devices on your clients' networks. It offers maximum proactive protection for organizations against the growing cyber threat to their IT investment and the mission-critical functioning of their day-to-day business.

Security Manager | Endpoint delivers integrated anti-virus, anti-spam, anti-malware, personal firewall and host intrusion prevention for your customers' Windows desktops, laptops and servers. Powered by an industry-leading security engine, it is fully integrated into N-central to offer added value by providing deployment, configuration, updating, monitoring and reporting services across all customers - all from a single console.

BENEFITS

Protect critical and sensitive information: Allows you to effectively guard your customers' most valued assets by providing a security solution that will protect information on all network endpoints.

Increase productivity: Reduce interruptions or downtime in your customers' networks by blocking spam and controlling the use of unproductive or banned applications.

Reduce operational complexity and lower costs: Delivers complete endpoint security in a single solution, eliminating the need for multiple security tools using multiple consoles.

KEY FEATURES

Exchange Email Protection: Provides integrated email scanning to remove viruses and spam from your clients email.

Comprehensive protection: Provides an all-in-one security solution to protect against all forms of threats to your customers' Windows environment.

Central console: Manage all customers and endpoints from the N-central user interface.

Around-the-clock updates: Can automatically download the latest detection updates even if a device is temporarily outside its internal network.

Configuration management: Uses profiles that allow you to configure all of the settings that will be applied to multiple devices upon installation of the endpoint security software, significantly decreasing setup time.

Real-time incident and alerts monitoring: Centralized monitoring unifies the information of all protections across all customers.

See reverse for details.

KEY FEATURES

Comprehensive protection

Delivers an all-in-one security solution, including anti-virus, anti-spam, anti-malware, personal firewall and host intrusion prevention. Advanced proactive technologies such as the genetic heuristic engine, behavioral blocking and behavioral scanning ensure your customers' networks are fully protected.

Configuration management

Configure all of the settings that will be applied to multiple devices upon installation of the endpoint security software, significantly decreasing setup time. You have the flexibility to enable security modules and define their settings separately for Windows servers, Windows workstations and Exchange Servers.

Around-the-clock updates

Automatically download the latest detection updates even if a device is temporarily outside its internal network. This allows you to provide customers maximum protection anywhere, any time.

Multi-stakeholder reports

Communicate vital information to executive, management, operational and technical stakeholders, as well as external parties such as auditors.

Real-time incident and alerts monitoring

Use the centralized monitoring in N-central to unify the information of all protections across all customers, allowing your technical staff to stay alert and take actions in real time. Define the type of security events that will dispatch an e-mail notification.

Easy deployment

Provides simple remote deployment by device or device group, ensuring bandwidth-friendly mass rollout and signature file updates. Existing protection found on a device will be removed automatically in most cases.

Detailed reports

Generates security status and security threat reports - important deliverables for customers with regulatory compliance requirements.

The Security Manager Status Report presents the status of your security configuration, giving you the power to demonstrate that your endpoint protection programs are implemented and working. The Security Manager Threats Report enables you to review the threat detections, actions taken to neutralize each threat and track the history and volume of threats over time.

Centrally managed quarantine

Allows you to review any suspicious files that have been isolated and determine the course of action for each of them remotely.

Features Checklist

Anti-virus and anti-spyware	✓
Firewall	✓
Intrusion prevention	✓
Proactive detection	✓
Rule-based system behavior blocking	✓
On-demand behavioral analysis	✓
Endpoint anti-spam	✓
Malware audit & disinfection service	✓
Application control	✓
2007 WildList proactive detection	✓
Behavioral analysis detection	✓
Rootkit detection	✓
Exchange Email Protection	✓

System Requirements

- » **Supported operating systems:** Microsoft Windows Server 2000/2003, Microsoft Windows Small Business Server 2008, Windows XP, Windows Vista (x86 and x64)), Exchange 2003, Exchange 2007 (for Exchange Email Protection)
- » **Minimum hardware configuration:** Pentium III, 512 MB RAM, 500 MB HDD space

