



IBM Proventia Network Enterprise Scanner

Identifying risk and prioritizing protection

IBM Proventia® Network Enterprise Scanner* (Enterprise Scanner) is designed to ensure the availability of your revenue-producing services and to protect your corporate data by identifying where risk exists, prioritizing and assigning protection activities and reporting on results.

Benefits

- Reduce risk to your network's uptime, bandwidth and critical systems with Enterprise Scanner's vulnerability management and protection capabilities.
- Free up resources by automating the scanning process.
- Leverage your existing infrastructure components: Enterprise Scanner provides seamless integration with Microsoft® Active Directory, asset management databases and workflow systems.
- Virtually eliminate duplicated effort: Information can be stored once and shared among systems.
- Reduce emergency patching and follow normal change-control processes: IBM Virtual Patch® technology helps protect at-risk systems and segments before the vendor-supplied patch is available.
- Support regulatory compliance with Enterprise Scanner's superset of audit tools taken from the auditors' preferred tool, IBM Internet Scanner® software.

Features and capabilities

Specifications

- Identifies 2,691 asset types out-of-the-box, including desktops, servers, routers, switches, applications and operating systems
- Identifies newly connected devices and previously undiscovered assets on the network
- Assigns or allows responsibility to be assigned to specific assets to meet corporate governance and traceability standards
- Is capable of passive/active asset identification with the inclusion of the IBM Proventia Network Anomaly Detection System (ADS)

Multisource discovery

- Active discovery scan
- Active Directory import
- Intrusion prevention system (IPS)-based discovery
- Proventia Network ADS discovery
- Asset database import
- Manual input
- Custom service discovery
 - User-defined

Asset identification techniques

- Ping sweep
- User Datagram Protocol (UDP) probe
- Asset fingerprinting
- Rapid discovery
- NetBIOS-based discovery
- Transfer Control Protocol (TCP) discovery
- UDP port discovery
- Operating system (OS) fingerprinting
- Application fingerprinting
- Integrated Networked Messaging Application Protocol (NMAP) 4.0 database

Network services identified

- 2,691

Asset classification

- Hierarchical group structure that mirrors your organizational structure, providing context for both scanning and reporting
- Active Directory import and mirroring
- Asset database import
- Geographical, organizational, topological or system-level classification

Vulnerability assessment

- Discovery-based assessment
 - Efficient, high-performance vulnerability assessment
- Scripted assessment
 - Allows for new content without updating product binaries
 - Provides smaller content updates (IBM X-Press Update™ product enhancements)
 - Supports faster time to market with security content
- Attack emulation
 - Performs specific tests in a nonimpacting manner (posing no danger to your network) to analyze the effects of a real attack
- Renowned vulnerability database by the IBM Internet Security Systems™ (ISS) X-Force® research and development team recognizes vulnerabilities and programmatic errors that could compromise an asset
- Host criticality-prioritized scanning

Security content updates featuring Virtual Patch technology

- Preemptive, ahead-of-the-threat coverage, powered by X-Force vulnerability-based research

Spyware scanning

- Detects existence of spyware

Trust X-Force option

- Automatically detects new vulnerabilities based on X-Force expert recommendations

Scan windows

- Automated scanning during open scan windows
- Auto-pause/auto-resume—automatic scan suspension upon closure of scan windows; resumes when the scan window reopens
- Scan-window configuration that's designed for ease of use
- Configurable refresh period refreshes data automatically during open scan window, helping to ensure up-to-date vulnerability information
- Group-oriented scan windows

Workflow

- Vulnerability prioritization
- Internal ticketing system
- Remedy integration
- Open application programming interface (API), supporting other ticketing systems
- Ownership assignment and tracking
- Activity logging and tracking
- Traditional patch-and-protect remediation
- Virtual Patch technology, in combination with the IBM Proventia Network Intrusion Prevention System (IPS) portfolio
- Automatic resolution validation
- Multiple vulnerabilities per ticket
- Status monitoring and tracking (eight levels)

Scan and block protection

- Vulnerability protection without deployment of a vendor-supplied patch when combined with IBM Proventia Network IPS
- Turnkey integration with Proventia Network IPS through the IBM Proventia Management SiteProtector™ system
- Detects vulnerabilities and identifies corresponding blocking algorithms within the Proventia Network IPS portfolio
- Unified management that provides easy configuration of IPS devices for discovered vulnerabilities

Reporting

- Reports that illustrate information in the context of your organization:
 - Group and report on risk in applicable business context using a mirror of your organization
 - Group and report by geography, network layout, business system or any other useful grouping of assets
 - Report risk to the right people at the right time—quickly compare risk of different business units, systems or geographies
- Flexible view-based analysis with more than 1,800 reports
- Enterprise-level multiscan, multiscanner reports
- Preconfigured report templates
- Exportable reports to PDF, CSV, HTML
- Schedule-driven reports
- Web-accessible reports
- FastAnalysis reports
- Extensive filtering

Automation

- Virtually eliminates manual steps, saving time and money
- Automatic and continuous scanning
- Scan prioritization
- Scan teams (multiple scanners working as one)
- X-Press Update enhancements of vulnerability information
- Asset classification and grouping

Easy-to-install appliance based on Linux® management

- Centrally managed by SiteProtector system—award-winning management system and the security industry's only platform designed to unify the protection of network, server and desktop assets
- Emergency scans—providing quick, ad hoc scans of your network on request
- Automated security intelligence updates on the newest electronic threats
 - X-Press Update product enhancements delivered by the globally respected X-Force research and development team

User interface options

- SiteProtector system centralized management interface
- Web-based Proventia manager local management interface

SiteProtector system

- Centralized command, reporting and analysis for Enterprise Scanner and all IBM ISS products
- User auditing
- Flexible event analysis

Proventia manager

- Web-based local management interface (LMI)
- Device configuration, establishment of SiteProtector communications link

Device health monitoring

- SiteProtector system centralized management interface
- Web-based local management interface

Asset-based management

- Asset-centric assessment policies associated with assets rather than with scanner
- Scan policy—asset-based scan policy allows policy association with assets or groups of assets rather than with scanners, allowing context-sensitive scanning
- Assessment refresh cycles
- Scan windows
- Assessment credentials for Microsoft Windows® and Secure Shell (SSH) technology
- Assessment policy
- Discovery policy/scan exclusions

Correlation

- Supports IBM SecurityFusion™ module
- SiteProtector FastAnalysis and centralized correlation

Independent discovery and assessment

- Separate policies
- Separate scan windows
- Separate refresh periods

World-class support

- 24x7 support, including platform updates

Hardware specifications

| Model | Enterprise Scanner 1500 | Enterprise Scanner 750 |
|---------------------------------|--|--|
| Physical characteristics | | |
| Form factor | 1-RU | Desktop |
| D x W x H | 429mm D x 382mm W x 44mm H 16.9" D x 15.0" W x 1.73" H | 177mm D x 250mm W x 39mm H 6.9" D x 9.8" W x 1.5" H |
| Weight | Gross 11.1kg (24.47lb) Net: 6.5kg (14.33lb) | 1.2kg (2.6lb) |
| Emissions | FCC Class A | FCC Class A |
| Certifications | CE/FCC/UL/cUL | CE/FCC/UL/cUL |
| Power | | |
| Power supply unit | Full-range 250-watt PSU auto-switching | 65-watt PSU, 100–240 volts AC, 47–63Hz |
| Operating environment | | |
| Temperature | Temp: 5°C–35°C (41°F–95°F) for P4 3.0–3.4GHz processors | Temp: 0°C–40°C (32°F–104°F) |
| Humidity | 20%–90% relative | 20%–90% relative |
| Storage environment | | |
| Temperature | -20°C–70°C (-4°F–158°F) | -20°C–70°C (-4°F–158°F) |
| Ports | | |
| Scan ports | Five 32-bit gigabit PCI-Express Ethernet ports (one active, four reserved for future use) | One 10/100/1,000 PCI Ethernet port |
| Management | One 32-bit gigabit Ethernet port | One 32-bit gigabit Ethernet port |
| Console | Serial port one – front-accessible RJ-45 connector | Serial port one – front-accessible RJ-45 connector |
| USB | Two USB 2.0/front accessible | Two USB 2.0/rear accessible |
| Front panel | | |
| LCD display | LCD panel 2 x 16 characters LCD module with four buttons (reserved for future use) | N/A |

Discovery performance specifications

| Enterprise Scanner 1500 | |
|-------------------------|----------------------------|
| Discovery | 2,600 - 3,000 IPs per hour |
| Assessment | 700 - 800 assets per hour |

| Enterprise Scanner 750 | |
|------------------------|----------------------------|
| Discovery | 2,400 - 2,800 IPs per hour |
| Assessment | 200 - 250 assets per hour |

Performance figures based on Firmware 1.3 with XPU 1.21 default policies on several different sized networks. Discovery speeds can be 2x to 3x faster on much smaller networks (50-500) hosts due to the low number of time-outs.

Scan-team performance gains

Performance features

- Dynamic check assignment to identify and run OS-specific checks
- Load balancing (teaming) among multiple scanners

Scan-time work distribution

- Ability to add a scanner at a location, to automatically and transparently load balance
- Perspective-based load balancing

Distributed scanning

- Performance optimization by adding multiple scanners in multiple network locations
- Multiple scanners colocated to load balance

For more information

Proventia Network Enterprise Scanner is also an integral part of IBM Managed Security Services, including IBM Vulnerability Management Service, and IBM Professional Security Services. IBM Managed Security Services provides 24x7x365 expert monitoring and protection for a fraction of the cost of training

| Scan team performance gains | | | |
|-----------------------------|-----------------------------|------------|---------------|
| Scan team | Percent reduction from base | | |
| | Discovery | Assessment | Time effect |
| One scanner | 0 percent | 0 percent | (base) 1 hour |
| Two scanners | 45 percent | 45 percent | 35 minutes |
| Three scanners | 60 percent | 60 percent | 24 minutes |
| Four scanners | 70 percent | 70 percent | 18 minutes |
| Five scanners | 75 percent | 75 percent | 15 minutes |
| Six scanners | 80 percent | 80 percent | 12 minutes |

and maintaining an in-house security staff. Discover how Enterprise Scanner can protect your business from Internet threats. Be sure to ask if your company qualifies for a 30-day evaluation. For an onsite demonstration, contact the IBM ISS office nearest you. For locations and more product information, visit: ibm.com/services/us/iss



© Copyright IBM Corporation 2008

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
02-08
All Rights Reserved

IBM, the IBM logo, Internet Scanner, Internet Security Systems, Proventia, SecurityFusion, SiteProtector, Virtual Patch, X-Force and X-Press Update are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

All performance data contained in this publication was obtained in the specific operating environment and under the conditions described above and is presented as an illustration. Performance obtained in other operating environments may vary and customers should conduct their own testing.

* U.S. Patent No. 7,093,239