



## IBM Internet Scanner software

### Intelligent scanning agent

With dynamic check assignment, IBM Internet Scanner® software will identify assets and unearth vulnerabilities with a high degree of accuracy and speed.

### Policy management

The policy management feature of Internet Scanner software allows users to customize the policy used for scanning; it comes preloaded with 20 standard scanning policies. Specific features include:

- Twenty default scanning policies
- Custom scanning policy
- Derive new template capabilities
- Edit/change policy
- FlexCheck custom checks with custom executables (user-defined)
- Searchable policy system (search by common vulnerabilities and exposures (CVEs), wildcards or vulnerability names)

### Administration, access and control

Internet Scanner software uses authorized administrative access to endpoints for in-depth scanning and identifies privileged administrative accounts to gather more information about network devices. Features include:

- Domain account registration and support
- Administrative access to supported endpoints
- Obfuscation of known account administration
- Database administration
- Enhanced command line interface
- Program file location specification
- Scanner data source name (DSN) modification
- Local logging

### **Asset identification**

Uses stack fingerprinting techniques and imports information from already-existing asset databases within your organization. Identifies more than 1,300 asset types (operating systems and network devices):

- Integrated Networked Messaging Application Protocol (NMAP) fingerprinting
- User-defined fingerprinting
- Scan-time ping asset identification
- Host-file import
- Host-list generator
- Host-file export
- Range enumeration
- Domain name system (DNS) name
- Internet Protocol (IP) address identification
- NetBIOS name
- NetBIOS domain
- Operating system type
- MAC address
- IP-stack fingerprinting
- Open-port banner identification

### **Real-time display options**

Presents information on screen for quick identification of vulnerabilities and vulnerable hosts. On-screen display functions include:

- Host view
- Vulnerability view
- Services view
- Accounts view
- Real-time activity monitoring with check progress
- Active session monitoring
- Scan status window
- Context-sensitive windows

### **Local scan control**

Gives the scan operator more precise control over the scanner with tools that automate manual tasks like merging scan sessions. Features that save the scan operator time include:

- Scan now
- Stop scan
- Pause/resume scan
- MultiScan session support
- Merge scan sessions
- Edit sensor properties
- Denial of service check segregation
- IBM X-Press Update™ product enhancements

### **Comprehensive vulnerability catalog**

Guides the user to the root cause of a vulnerability, detailed descriptions of the vulnerability, remediation steps to remove the vulnerability and reference links to obtain more information about the vulnerability. Provides expert security information, including:

- Local help
- Remediation information
- Reports based upon vulnerability information

### **Reporting**

Allows quick and easy information-sharing across all levels of the organization. A comprehensive set of 74+ predefined reports includes:

- Executive reports
- Line-management reports
- Technician reports
- Trend reports
- Operating-system reports
- Foreign-language support
- Import custom reports

### **Internet Scanner software identifies several vulnerability categories**

- Backdoors
- Browser
- Brute-force password guessing
- CGI-bin
- Daemons
- Denial-of-service
- Distributed Component Object Model (DCOM)
- DNS
- E-mail
- Firewalls
- File Transfer Protocol (FTP)
- Information-gathering
- Instant messaging
- Lightweight Directory Access Protocol (LDAP)
- Microsoft® Windows® critical issues
- NetBIOS
- Network
- Network file system requirements
- Network information system requirements
- Network sniffers
- Protocol spoofing
- Remote procedure call (RPC)
- Router switch
- Shares
- Simple Network Management Protocol (SNMP)
- Web scan
- Windows groups
- Windows networking
- Windows password checks
- Windows password policy
- Windows patches
- Windows policy issues
- Windows registry
- Windows services
- Windows users
- X-Windows

**Internet Scanner is designed to identify vulnerabilities for more than 1,300 asset types, including the following operating systems**

- BeOS
- BSD generic
- Caldera OpenLinux
- Caldera UnixWare
- Cisco IOS
- Compaq True64
- Conectiva Linux®
- Convex OS
- Debian Linux
- DG/UX
- EnGarde Secure Linux
- Fedora Core
- FreeBSD
- HP Apollo Domain/OS
- HP-UX
- IBM AIX®
- IBM AS/400®
- Immunix
- IRIX
- Linux-based OS
- Mac OS
- Mandrake Linux
- Microsoft Windows (all versions)
- NEC EWS-UX/V
- NEC UP-UX/V
- NEC UX/4800
- NetBSD
- NeXTSTEP
- Novell NetWare

- OpenBSD
- OpenVMS
- IBM OS/2®
- OS-9
- QNX
- RedHat Linux
- SCO Open Server
- Slackware Linux
- Solaris
- SunOS
- SuSE Linux
- Trustix Secure Linux
- Turbolinux
- Ultrix
- UNICOS
- UnitedLinux
- VxWork

#### **Vulnerability management**

IBM Proventia® Management SiteProtector™ central management system controls multiple Internet Scanner agents and provides a comprehensive enterprise vulnerability management system.

## **Additional capabilities available with the SiteProtector system**

### **Enterprise-class scalability**

The SiteProtector system controls and operates hundreds of remote scanning agents and reports on the results quickly and easily. Scalable for the largest enterprises, the SiteProtector system offers the following vulnerability-management features:

- Multiscanner control
- Multitiered architecture
- Distributed vulnerability collection
- Enterprise database support
- Multiple site support
- Enterprise dashboard with vulnerability drill-down capabilities
- Multiwindow view
- Centralized servers

### **Enterprise reporting**

Enables multiscanner/multiscan enterprise correlation, aggregation and reporting. Includes all stand-alone scanner-reporting capabilities, plus:

- Enterprise multiscan reports
- Precanned default reports
- Exports reports to PDF, CSV, HTML
- Group-based reporting
- Schedulable reports
- Web-accessible reports
- Fast analysis reports
- Extensive filtering

### **Remote scanning capabilities**

Controls and operates scanning agents located in remote geographies or behind firewalls. Remote operations include:

- Start scan (scan now)
- Edit policy
- Stop scan
- Pause/resume scan

### **Automated and schedulable commands**

Eliminates the need to run recurring scans manually. Task scheduler eliminates steps and saves you time with:

- Start scan
- Stop scan
- Report creation
- Apply IBM X-Press Update product enhancements

### **User administration**

Empowers multiple users with appropriate access to control their portion of the vulnerability management process. Features include:

- Administration using domain accounts (optional)
- Administration using local accounts
- Multiple user roles
- Group-based user access control

## **Asset management**

Designed for ease and accuracy, identifies groups and manages your information assets through:

- Active directory integration
- Prompt asset grouping
- Manual asset grouping
- Integrated protection view
- Group-name customization
- Group-based reporting
- Multilevel asset grouping
- Group-based user access control
- Ungrouped asset identification

## **Discovery and assessment**

Includes automatic (passive) discovery of information assets based upon traffic analysis from your IBM Internet Security Systems (ISS) security infrastructure; helps identify new assets as they are added to the network and groups them according to user-defined roles or holds in the “ungrouped asset” category.

## **Updates**

Receives regular security content updates to enhance scanning and vulnerability management. Updates include:

- X-Press Update product enhancements and service packs
- Prompt updates
- On demand updates
- Update scheduling
- Updates via Web
- Updates offline when not connected
- Centralized update server
- Update mirrors

## **Data and vulnerability analysis views**

Displays security information in real time; flexible display provides granular view of event details or summary information; once an analysis view is established it can be saved, recalled or shared with others users. Views include:

- Group-oriented analysis views
- Seventeen default analysis views
- Right-click data navigation (fast analysis)
- Custom views
- Vulnerability clearing
- Vulnerability-incident creation
- Vulnerability-exception creation
- Drill-down to event details
- View vulnerability information
- Target-analysis mode
- Sensor/scanner-analysis mode
- Data export to printer
- Data export with vulnerability information
- Schedulable data export
- Graphical analysis views
- Baseline and compare views
- Return to baseline
- Group filters
- Analysis view filters
- Custom analysis display
- Consolidated vulnerability views

#### Administrative functions

- Internet proxy support
- Secure sockets layer (SSL)-encrypted communication
- Trusted certificate support (SSL)
- Optional local documentation
- Web documentation
- Administrative trace (local logging)
- User auditing

#### Data maintenance

- Schema documentation available
- Purge data now
- Purge data on schedule
- Data backups
- Disk defragmentation

#### For more information

To evaluate Internet Scanner software today, call 1 800 776-2362, e-mail [sales@iss.net](mailto:sales@iss.net), or visit:

**[ibm.com/services/us/iss](http://ibm.com/services/us/iss)**



© Copyright IBM Corporation 2007

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

Produced in the United States of America  
04-07  
All Rights Reserved

IBM, the IBM logo, AIX, AS/400 and OS/2 are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Internet Scanner, Proventia and SiteProtector and X-Press Update are trademarks or registered trademarks of Internet Security Systems, Inc., in the United States, other countries, or both. Internet Security Systems, Inc., is a wholly-owned subsidiary of International Business Machines Corporation.

Portable Document Format (PDF) is a trademark of Adobe Systems Incorporated in the United States, other countries, or both.

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

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

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.