

# Internet Scanner® Vulnerability Assessment Application

## INTELLIGENT SCANNING AGENT

With Dynamic Check Assignment, Internet scanner will identify more assets and unearth more vulnerabilities with a higher degree of accuracy and speed than any other product.

## POLICY MANAGEMENT

Allows users to customize the policy used for scanning; comes pre-loaded with 20 standard scanning policies. Features include:

- 20 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 CVE, wildcard, vulnerability name)

## ADMINISTRATION, ACCESS AND CONTROL

Uses authorized administrative access to end points for in-depth scanning; identifies privileged admin accounts to gather more information about network devices. Features include:

- Domain account registration and support
- Administrative access to end points supported
- Obfuscated known account administration
- Database administration
- Enhanced command line interface
- Program file location specification
- Scanner 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 (OS and network devices):

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

## REAL-TIME DISPLAY OPTIONS

Presents information onscreen 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 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
- 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 link references to obtain more information. Provides expert security information, including:

- Help locally
- 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+ pre-defined reports includes:

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

## INTERNET SCANNER IDENTIFIES THE FOLLOWING VULNERABILITY TYPES/CATEGORIES:

Brute Force Password- Guessing  
Backdoors  
Browser  
CGI-Bin  
Daemons  
DCOM  
Denial of Service  
DNS  
E-mail

Firewalls  
FTP  
Information Gathering  
Instant Messaging  
LDAP  
NetBIOS  
Network  
Network Sniffers  
NFS System Requirements

NIS  
Protocol Spoofing  
Router Switch  
RPC  
Shares  
SNMP  
Web Scan  
Windows Critical Issues  
Windows Groups

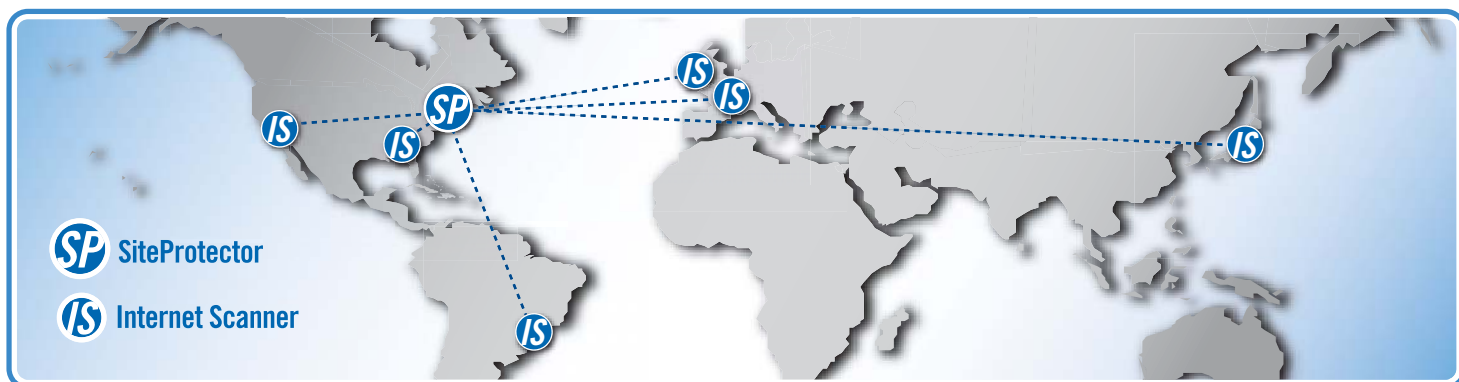
Windows Networking  
Windows Password Checks  
Windows Password Policy  
Windows Patches  
Windows Policy Issues  
Windows Registry  
Windows Services  
Windows Users  
X-Windows

## INTERNET SCANNER IDENTIFIES VULNERABILITIES FOR OVER 1300 VARIOUS ASSET TYPES INCLUDING THE FOLLOWING OPERATING SYSTEMS:

AIX	FreeBSD	NetBSD	SuSE Linux
BeOS	HP Apollo Domain/OS	NeXTSTEP	Trustix Secure Linux
BSD generic	HP-UX	Novell NetWare	Turbolinux
Caldera OpenLinux	IBM AS/400	OpenBSD	Ultrix
Caldera UnixWare	Immunix	OpenVMS	UNICOS
Cisco IOS	IRIX	OS/2	UnitedLinux
Compaq True64	Linux based OS'	OS-9	VxWork
Conectiva Linux	Mac OS	QNX	
Convex OS	Mandrake Linux	RedHat Linux	
Debian Linux	Microsoft Windows (all versions)	SCO Open Server	
DG/UX	NEC EWS-UX/V	Slackware Linux	
EnGarde Secure Linux	NEC UP-UX/V	Solaris	
Fedora Core	NEC UX/4800	SunOS	

## Vulnerability Management

ISS' SiteProtector™ central management system controls multiple Internet scanner agents provides a comprehensive enterprise vulnerability management system.



## Additional Capabilities available with SiteProtector

### ENTERPRISE CLASS SCALABILITY

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

- Multi-scanner control
- Multi-tiered architecture
- Distributed vulnerability collection
- Enterprise database support
- Multiple site support
- Enterprise dashboard with vulnerability drill-down capabilities
- Multi-window view
- Centralized servers

### ENTERPRISE REPORTING

Enables multi-scanner / multi-scan enterprise correlation, aggregation and reporting.

Includes all stand-alone scanner-reporting capabilities plus:

- Enterprise multi-scan reports
- Pre-canned 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 & 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 X-Press update

## 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

Easily and accurately identifies, groups and manages your information assets through:

- Active directory integration
- Automatic asset grouping
- Manual asset grouping
- Integrated protection view
- Group name customization
- Group-based reporting
- Multi-level 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 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 service packs
- Automatic content 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
- 17 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 AND VULNERABILITY ANALYSIS VIEWS (CONT)

- Data export to printer
- Data export with vulnerability info
- 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
- 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
- Defrag