

Proventia Server for Windows Data Sheet

Overview

ISS' Proventia® Server for Windows software identifies and blocks known and unknown threats and helps enforce corporate security policy for servers. It combines a local firewall, intrusion detection and prevention system, and application integrity enforcement to ensure that servers are protected and adhere to corporate standards.

Proventia Server integrates seamlessly into your IT infrastructure and can be managed locally or centrally by ISS' award-winning SiteProtector management system.

Benefits

- **Protects servers against known and unknown attacks without requiring patches.** Forget emergency patch rollouts that disrupt servers and break server applications. Proventia Server's vulnerability-centric intrusion prevention blocks network worms and other exploits to known vulnerabilities, while buffer overflow exploit prevention blocks attacks against unknown buffer overflow exploits.
- **Audits server applications.** Quickly audit applications that are running and accessing the network before establishing an application or network lock down policy.
- **Enforces service and application policy.** Ensures that only authorized services and applications are running on servers. Prevents unauthorized programs from being installed.
- **Enforces network access policy.** Ensures that only authorized applications are accessing the network and sets port and IP restrictions for inbound and outbound server traffic.
- **Stops unauthorized administrators from making security changes.** Prevents anything or anyone from stopping or disabling Proventia Server regardless of local or remote administrative privileges.
- **Provides local user interface.** Local interface provides instant access to security policy configuration. Policy priority can be central control, local control, or shared control (with central priority).

- **Integrates with Active Directory.** Use Active Directory grouping structure to manage policies, monitor events, and create reports.
- **Enforces anti-virus compliance.** Ensures that servers are getting the latest antivirus updates and reports non-compliant servers.
- **Consumes little resources.** Small memory and CPU footprint. Small (600k) security updates keep servers current when necessary.

Pre-emptive Protection

Some host protection companies provide intrusion prevention signatures in addition to a local firewall. These signatures work very much like anti-virus signatures. They work great against threats that are known. They are useless for threats that are unknown.

The industry as a whole has to move to preventative protection in all aspects of security. ISS is leading that direction with its commitment to protect customers ahead of the threat.

Preemptive Network Threat Prevention

ISS is providing this protection today from the network level with our vulnerability protection built in to all of our network, server, and desktop products. This vulnerability-centric intrusion prevention has protected ISS customers from network-borne threats like worms, viruses and hacker attacks over the years. See the table on the next page for some examples of the network-based worm infections we have prevented.

Buffer Overflow Exploit Prevention

Buffer Overflow Exploit Prevention is a signature-less technology that actively looks for malicious code exploits in memory buffer overflows. This technology is vulnerability-independent, meaning it is one step ahead of knowing that particular vulnerabilities exist. It stops worms from propagating and prevents attackers from using buffer overflows to run arbitrary code on your systems.

This technology hooks system calls (not simply the API level) and prevents these exploits without noisy pop-ups.

Platforms Supported

Windows 2000 Server SP4
Windows 2000 Advanced Server SP4
Windows Server 2003 SP1 Standard Edition
Windows Server 2003 SP1 Web Edition
Windows Server 2003 SP1 Enterprise Edition