



# IBM Proventia Server Intrusion Prevention System for Windows

## Overview

IBM Proventia® Server Intrusion Prevention System (IPS) for Windows software helps organizations achieve and maintain compliance with regulations that require security against malicious threats which may compromise servers and sensitive data. With Proventia Server IPS, enterprises can protect against data breaches and benefit from capabilities that simplify and support compliance requirements.

Proventia Server IPS benefits extend beyond protection and compliance support by serving as a critical component in an organization's Data Loss Prevention (DLP) strategy. With trends in measuring the cost of server breaches based on cost per compromised record vs. server downtime, a comprehensive DLP strategy with Proventia Server IPS will:

- *Enable real-time reporting on data security and application protection*
- *Contribute to data loss prevention strategies and preemptive protection while enforcing corporate security policies for servers*
- *Inspect traffic entering the server to block malicious code that attempts to infiltrate and extract sensitive data*

Proventia Server IPS for Windows is designed to integrate seamlessly into your IT infrastructure and is managed centrally by the IBM SiteProtector™ system.

## Benefits

Proventia Server IPS delivers a wide array of capabilities that support the demands of compliance regulations and the security technology necessary to support a comprehensive DLP strategy.

Proventia Server IPS protects your servers from malicious attacks while supporting your compliance needs. The system provides real time file integrity monitoring to alert security teams to changes in specified files and folders. Benefits enable enterprises to maintain control of data access points and monitor changes to confidential data. Additionally, application controls can lock down user access to programs that can be used to take control of a server.

Proventia Server IPS is a critical component of any data loss prevention strategy. Proventia Server IPS stops internal/external server attacks before the threat can breach a system and result in data loss or theft. Proventia Server IPS stops internal and external server attacks and threats before it is compromised and critical data is breached. Providing an additional layer of defense after the firewall and IPS blocked attacks, Proventia Server IPS includes buffer overflow exploit prevention (BOEP) capabilities.

- **Maintains compliance with tracking and reporting tools.** Receive alerts for activity regarding privilege escalations, confidential file access/modifications and unauthorized configuration changes.
- **Protects servers against known and unknown attacks without requiring patches.** Forget emergency patch rollouts that disrupt servers and break server applications. Proventia Server IPS

*offers vulnerability-centric intrusion prevention designed to block 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.
- **Detects and responds to application-level attacks and/or unauthorized activity.** Employs log monitoring of operating system and application activity to maintain system integrity and compliance.
- **Enforces service and application policy.** Verifies that only authorized services and applications are running on servers. Prevents unauthorized programs from being installed.
- **Enforces network access policy.** Verifies that only authorized applications are accessing the network and sets port and IP restrictions for inbound and outbound server traffic.
- **Verifies the integrity of key files.** Combines real-time file integrity monitoring, with file system baselining to verify the integrity of sensitive files as well as critical system binaries and configuration files to track alterations by unauthorized users.
- **Stops unauthorized users from making security changes.** Prevents anything or anyone from stopping or disabling Proventia Server IPS 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.** Verifies that servers are receiving the latest anti-virus updates and reports non-compliant servers.

### **Preemptive Protection**

Some host protection solutions provide intrusion prevention signatures in addition to a local firewall. Much like anti-virus signatures, signature-based intrusion prevention works well against only known threats – but is useless against unknown exploits. Preemptive protection based on a combination of vulnerability-centric intrusion prevention coupled with other protection technologies is designed to keep valuable servers ahead of the threat.

### **Preemptive Threat Prevention**

IBM Internet Security Systems™ (ISS) provides preemptive protection with its network, server and desktop security offerings, including Proventia Server IPS for Windows. Vulnerability-centric intrusion prevention from IBM ISS has protected clients from network-borne threats like worms, viruses and hacker attacks for many years.

Proventia Server IPS	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
	Windows Server 2003 x64 Support	Integrated Firewall	Network Level IPS	Buffer Overflow Exploit Prevention	Integrated Anti-Malware	Application Control	Registry File Control	System Activity Monitoring	File Integrity Monitoring	Audit Policy Enforcement	Single-Console Solution (HIPS, NIPS, VA)

**Platforms Supported**

- *Windows Server 2003 x64 SP2, Standard Edition*
  - *x64 SP2, Enterprise Edition*
  - *x64 R2, Standard Edition*
  - *x64 R2, Enterprise Edition*
  - *x64 SP1, Standard Edition*
  - *x64 SP1, Enterprise Edition*
- *SP2, Standard Edition*
- *SP2, Web Edition*
- *SP2, Enterprise Edition*
- *R2, Standard Edition*
- *R2, Enterprise Edition*
- *SP1, Standard Edition*
- *SP1, Web Edition*
- *SP1, Enterprise Edition*
- *Windows 2000 Server SP4 and Advanced Server SP4*
- *VMware ESX 2.5 & 3.0 (guest OS)*

**For More Information**

For more information about Proventia Server IPS for Windows, please contact your authorized IBM ISS sales representative, or visit

**www.ibm.com/services/us/iss.**

**About IBM Internet Security Systems, Inc.**

IBM Internet Security Systems (ISS) is the trusted expert to global enterprises and world governments, providing products and services that protect against Internet threats. An established world leader in security since 1994, IBM ISS delivers proven cost efficiencies and reduces regulatory and business risk across the enterprise. IBM ISS products and services are based on the proactive security intelligence conducted by the IBM Internet Security Systems X-Force® research and development team – a world authority in vulnerability and threat research. For more information, visit **www.ibm.com/services/us/iss** or call 1 800 776-2362.



© Copyright IBM Corporation 2007

IBM United States  
IBM Global Services

Route 100  
Somers, NY 10589  
U.S.A.

Produced in the United States of America.  
11-07  
All Rights Reserved.

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Proventia and SiteProtector 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.


Windows is a registered trademark 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.

\* BOEP is currently available in 32-bit supported platforms only.

1 The IBM home page on the Internet can be found at **ibm.com**

 Printed in the (country of origin) on recycled paper containing 10% recovered post-consumer fiber.