



## **IBM Proventia Desktop Endpoint Security: providing powerful, multilayered protection for desktops.**

### **IBM Internet Security Systems (ISS) helps enhance enterprise security enterprise posture with powerful endpoint protection**

Preemptive security is now available at the endpoint with IBM Proventia® Desktop Endpoint Security (Proventia Desktop) from IBM Internet Security Systems (ISS). This advanced software promptly protects desktops and mobile devices against known and unknown threats and other improper activity. Proventia Desktop delivers effective, cost-efficient and standardized security for your enterprise's most important and commonly used IT assets.

Threats to endpoints—the lifeline of your organization—are rapidly evolving. Profit-driven attackers launch stealthy exploits that eschew detection by legacy security products. Particularly nefarious attacks, such as disposable

single-use Trojans, cannot be stopped with anti-virus technologies alone. With malware attacks on the rise, the profiteers continue to unleash new zero-hour threats that legacy, stand-alone security products like anti-virus and firewall protection simply cannot combat. And even if they could, these products cause management headaches for security and IT resources that often outweigh their benefits.

Proventia Desktop's multilayered technology forms a robust and effective security solution for endpoint devices. It combines personal firewall, anti-virus, application control and anti-spyware tools with preemptive technologies such as buffer-overflow exploit prevention, vulnerability-centric intrusion prevention, and the IBM ISS patented Virus Prevention System (VPS).\*

Proventia Desktop helps eliminate outages, downtime and excessive calls to the help desk. It integrates seamlessly into your IT infrastructure and can be managed locally or centrally. Proventia Desktop is part of the IBM protection platform, which offers preemptive security for the entire IT environment, with products and services that continuously assess vulnerabilities and prevent threats.

### **Why is advanced protection needed at the desktop?**

*With modern threats, firewalls and anti-virus protection alone are not enough*

Today's hybrid threats and sophisticated hackers regularly bypass and thwart conventional defenses. Many companies have suffered costly Internet attacks, even though they had firewalls and legacy anti-virus protection. For instance, buffer-overflow attacks are detected by some systems, but cannot be stopped before they are launched. Conventional anti-virus solutions using signature-based techniques can block known viruses, but offer no protection against new, unknown viruses.

*The stream of new users and devices creates a compliance nightmare*

New desktops and mobile computers at corporate offices, branch offices, employees' homes and on the road present a security compliance headache and a source of new Internet threats. The enterprise perimeter is only as strong as its weakest endpoint.

*The patching merry-go-round*

Emergency patches to your desktop operating systems and applications can help alleviate some threats, but chances are good that your IT and help desk resources are simply stretched too thin to keep pace. The problem is compounded by the fact that patches often cause problems more severe than those they are designed to fix.

*No "reactive" protection is fast enough to prevent losses*

Even the most current "reactive" security measures, such as anti-virus solutions, respond only after an attack has occurred—too late to prevent downtime, lost transactions, the compromise of confidential information and other potential liabilities.

### **Why Proventia Desktop? What are the benefits?**

*Single agent protection*

Proventia Desktop affords ahead of the threat protection on a single agent to help decrease your enterprise's overall risk equation. As an integrated endpoint agent, it eliminates the performance hits and subscription costs conferred by multiple agents. With Proventia Desktop, necessary security technology is integrated into one product.

*Lower total cost of ownership*

Proventia Desktop costs little to run, while preventing costly patching and remediation outlays. Multilayered protection from a single agent reduces your licensing and subscription costs, and helps to lower help desk calls and client remediation activity.

Proventia Desktop enables scalable policy control and management. Using the IBM Proventia Management SiteProtector™ system, administrators can control enterprisewide deployments from a single console.

### **How does multilayered protection work?**

*It stops threats at the application and network level.*

*Protection from application-based threats*

File-based attacks, such as viruses and Trojans, threaten desktops through the application vector. Proventia Desktop combats application-based threats with its VPS, application control, anti-virus and anti-spyware layers.

**Virus Prevention System**—Signature AV is a “scan and remove” technology that cleans endpoints, but it is only one piece of the puzzle, not the centerpiece of endpoint protection. Proventia Desktop complements traditional anti-virus protection with its patented VPS, which detects and blocks spyware and more than 95 percent of new and unknown viruses and worms—without updates or false positives. Rather than relying on signatures for detection, VPS analyzes the activities of an executable file and detects families of malicious code. VPS runs code in a virtual environment, safely monitors the execution and then evaluates for malicious content. This helps to ensure that real threats are stopped, while valid traffic is undisturbed.

**Application control**— Proventia Desktop provides the ability to allow or disallow certain applications from installing on the endpoint.

**Anti-virus and anti-spyware**— Proventia Desktop now includes the Bit Defender engine to scan for and remove known malware from hosts.

#### *Preempting network-based attacks*

**Personal firewall**— Proventia Desktop’s firewall blocks unauthorized access to ports, IP addresses and services, stopping attacks such as IP spoofing and terminal hijacking protocols and services.

**Vulnerability-based Proventia Intrusion Prevention System**— Proventia Desktop includes Proventia Intrusion Prevention technology, which shields the vulnerabilities that attackers target rather than providing a reactive signature for known exploits. It uses both signature-based and protocol-based analysis to stop known exploits and their variants.

**Buffer-overflow exploit prevention**— Proventia Desktop addresses buffer overflows. Buffer-overflow attacks are insidious, because you cannot protect yourself by simply not opening attached e-mail files. With its buffer-overflow exploit prevention feature, Proventia Desktop effectively blocks such attacks with a “plug-and-play” configuration.

#### **Guide to selecting a desktop security solution**

To assure that your evaluation of desktop security solutions yields an effective result, evaluation criteria should include the following attributes:

- True preemptive capabilities
- Multiple analysis techniques used to block both application-vector and network-vector threats
- Vulnerability-based security content provided by a security research leader
- Effective default protection policy
- Hands-free, out-of-the-box protection
- Scalable, central management capability
- Microsecond latency

#### **Experience the IBM ISS advantage today**

Discover how IBM Proventia Desktop 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 Internet Security Systems office nearest you. For office locations and to get more product information, 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 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.

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.