



# IBM Proventia Desktop Endpoint Security

---

## Highlights

---

- ***Reduces risk from both known and unknown types of attacks***
- ***Provides multilayered security in a single agent***
- ***Helps to ensure compliance and simplify management***
- ***Helps prevent the type of attacks that lead to data theft***

### **Addressing the threat**

Your desktop environment is a prime target for malicious attacks which can result in widespread system outages and data loss. When a breach occurs, not only is your business productivity impacted, but you also face the grim possibility that sensitive business information may be compromised. Like many companies and organizations, your challenge is that your existing security solutions are not able to keep pace with rapidly evolving, profit-driven threats. What you need is an integrated and affordable desktop security solution that will provide preemptive, ahead of the threat protection.

IBM Proventia® Desktop Endpoint Security is designed to stop intrusions and attacks before they happen.

We can help you prevent downtime and costly data loss, mitigate known and new threats, ensure security compliance, and lower your total cost of ownership. With multilayered protection, we help you fight threats regardless of attack mode. Our solution combines personal firewall, antivirus and anti-spyware with innovative preemptive technologies like vulnerability-centric intrusion prevention and the IBM Internet Security Systems™ (ISS) patented virus prevention system<sup>1</sup>—all in a single agent that also supports the Microsoft® Windows Vista™ 32-bit operating system.

### **Reducing risk from known and unknown attacks**

Backed by cutting-edge, continuous security research, IBM Proventia Desktop Endpoint Security is designed

to preemptively stop both known and evolving threats. We combine innovative, behavior-based protection technologies with conventional, signature-based technologies to help identify and block new attacks before they happen. And our comprehensive support helps you fight both network-based and application-based threats.

### **Providing multilayered protection in a single agent**

Unlike other security solutions, IBM Proventia Desktop Endpoint Security delivers comprehensive protection in a single product, from a single vendor. Designed for easy integration with your existing infrastructure, we combine a personal firewall, intrusion prevention, buffer overflow exploit prevention, application protection and virus prevention in a single agent. This multilayered protection includes a combination of technologies:

- *Virus Prevention System (VPS)*
- *Buffer-overflow exploit prevention*
- *Vulnerability-centric intrusion prevention*

- *Anti-virus and anti-spyware signatures*
- *Personal firewall*
- *Application control*

### **Virus Prevention System**

IBM Proventia Desktop Endpoint Security's patented Virus Prevention System (VPS) detects and blocks a variety of malware, including more than 90 percent of new and unknown viruses and worms—without an update. Rather than relying on signatures for detection, VPS uses a behavioral system that analyzes the activities of an executable file and detects families of malicious code. The VPS runs programs in a virtual environment where it safely examines the program's behavior and evaluates it for malicious content. This process creates a view of what a program does or would do under certain conditions—providing a preemptive look at the intentions of an application. This deep analysis is the key to stopping real threats to your network without affecting legitimate programs or requiring custom application profiling.

### **Buffer-overflow exploit prevention**

Buffer-overflow exploit prevention is a "last line of defense" against zero-hour exploits designed to take advantage of new or unknown vulnerabilities. But, intrusion prevention technology can only block attacks against known exploits. What do you do with the unknown threats? IBM Proventia Desktop Endpoint Security is designed to protect hosts from attackers that attempt to use known or previously unknown buffer-overflow attacks to exploit the system or propagate. Like a circuit breaker, IBM Proventia Desktop Endpoint Security buffer-overflow exploit prevention is tripped to help protect the system as soon as malicious code tries to execute.

### **Intrusion prevention system**

In the last few years, the world of network vulnerabilities has merged with viruses. Malware writers have now taken full advantage of vulnerabilities to increase the penetration of their malicious programs. IBM Proventia Network Intrusion Prevention System is highly effective at preventing the spread of network worms. Coupled with

IBM Internet Security Systems (ISS) you have a solution that helps you remain ahead of the threat by blocking network-based attacks and helping prevent the spread of many attacks focused at specific vulnerabilities.

#### **Anti-virus/anti-spyware signature engine**

IBM Proventia Desktop Endpoint Security provides an industry-leading anti-virus and anti-spyware signature engine that helps stop known attacks from compromising an endpoint. The solution also scans and removes known endpoint infections from your network.

#### **Personal firewall**

As part of a layered approach to security, a personal firewall can reduce, but not eliminate, risk exposure introduced by network access. By blocking access

to ports, Internet Protocol (IP) addresses and services, personal firewall technology can help prevent attacks targeting protocols and services not needed for legitimate business.

#### **Application control**

Application control helps prevent application-based attacks on the desktop. It can protect desktops from threats before or during the launch phase of an attack. Acting as another last line of defense, application control is a useful protection technology that is designed to mitigate remaining threats after other protection methods have been employed and exhausted.

Application control is also useful for enforcing corporate policy for appropriate application usage.

#### **Helping to ensure compliance and simplify management**

IBM Proventia Desktop Endpoint Security meets regulatory requirements for host protection to safeguard access to your corporate network. We even help you enforce security policies on application use.

Our SiteProtector™ is a centralized security management system designed to let you control, monitor and analyze events with reduced staff and operational costs. An automated command and control center provides your staff with advanced event correlation and analysis and the capability to implement automatic updates. This scalable and flexible system can easily be integrated with your existing systems to deliver a single view of your enterprise.

## Requirements

<b>Processor</b>	500 MHz or higher Intel® Pentium® platform-compatible CPU, Proventia Desktop 10.0 for Vista 1 GHz 32-bit processor
<b>Memory</b>	256 MB of RAM or better, Proventia Desktop 10.0 for Vista 1 GB of system memory
<b>Disk space</b>	75 MB free disk space
<b>Network connection</b>	<ul style="list-style-type: none"><li>• 10/100 Mbps or 1 Gigabit<sup>2</sup> TCP/IP network connection over 10/100 Ethernet LAN/WAN, cable modem, DSL router, ISDN router or dial-up modem</li><li>• System must be using COMCTL32.DLL version 4.72 or newer. COMCTL32.DLL is available at Microsoft's Web site</li></ul>
<b>Operating system</b>	<ul style="list-style-type: none"><li>• Microsoft Windows® 2000 Professional</li><li>• Windows XP Professional</li><li>• Windows Vista</li></ul>
<b>Required additional software</b>	Microsoft Internet Explorer 6.0 or higher to view online help.
<b>Management software</b>	Use IBM Proventia Management SiteProtector centralized management system 2.0, Service Pack 6 or higher

IBM is an industry leader in security and privacy products, solutions and services. IBM Proventia Desktop Endpoint Security offers you true preemptive protection against vicious attacks. We offer you comprehensive protection at the desktop to combat modern threats, and make security more manageable.

### For more information

To learn more about IBM Proventia Desktop Endpoint Security, please contact your IBM representative or IBM Business Partner, or visit the following Web site:

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



© Copyright IBM Corporation 2007

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

Produced in the United States of America  
November 2007  
All Rights Reserved

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

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

Intel and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries 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.

<sup>1</sup> U.S. Patent No. 7,093,239

<sup>2</sup> Gigabit Ethernet hardware supported, but not 1 Gbps throughput