

112374

VIRUS: DETECTED

THE POWER TO *neutralize*
THREATS BEFORE THEY
impact THE DESKTOP.

proventia[®]

Desktop

POWERFUL,
MULTI-LAYERED
protection
FOR DESKTOPS

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

Today's piecemeal desktop security solutions fail to recognize that desktops are susceptible to major attacks from two different vectors. File-based attacks, such as viruses, e-mail worms, Trojans and spyware threaten desktops through the application vector. Packet-based attacks, such as denial of service and Internet worms threaten desktops through the network vector. Preempting both application- and network-based attacks requires multi-layered technology.

Proventia Desktop's multi-layered technology forms the most robust and effective solution ever developed for endpoint devices. It combines personal firewall and application control with cutting edge preemptive technologies like buffer overflow exploit prevention, vulnerability-centric intrusion prevention, and ISS' patent-pending virus prevention system. Only Proventia Desktop from ISS applies these layered technologies to preemptively stop both network- and application-based threats in a way that requires no baselining, profiling, or end-user intervention.

Proventia Desktop eliminates outages, employee downtime and excessive calls to the helpdesk. It integrates seamlessly into your IT infrastructure and can be managed locally or centrally by ISS' SiteProtector™ centralized management system.

Proventia Desktop is part of ISS' Proventia Enterprise Security Platform (ESP). Proventia ESP offers preemptive security for the entire IT infrastructure, with products and services that continuously assess vulnerabilities and prevent threats, and information management and reporting capabilities that show the value of security.

Why is advanced protection needed at the desktop?

Because desktops are your first and last line of defense

Outside your protected environment, your enterprise's remote sites and remote users are exposed to a multitude of threats; you must assure that remote users don't become unknowing conduits for threats to enter your network. Within your enterprise, you must make your desktops the last defense against threats that may have already penetrated your network. These imperatives present complex challenges:

WITH MODERN THREATS, FIREWALLS AND ANTIVIRUS ALONE AREN'T 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 antivirus protection. For instance, buffer overflow attacks are detected by some systems, but can't be stopped before they are launched. Conventional antivirus 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 never-ending security compliance headache, and a constant source of new Internet threats.

THE PATCHING MERRY-GO-ROUND

Emergency patches to your desktop operating systems and applications can help alleviate some threats, but such fixes can number in the hundreds. Chances are, your IT and helpdesk 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. That's why patches should not be rushed to wide deployment before careful testing.

NO "REACTIVE" PROTECTION IS FAST ENOUGH TO PREVENT LOSSES

Internet threats can now spread to thousands of desktop and mobile computers in seconds. Even the most current "reactive" security measures like antivirus respond only after an attack has occurred—often too late to prevent downtime, lost transactions, the compromise of confidential information and potential liabilities.

Why Proventia Desktop?

Because it delivers the preemptive protection you need

Proventia Desktop is a multi-layered solution for desktops that delivers true preemptive protection. It incorporates Proventia intrusion prevention, which leverages ISS' world-renowned X-Force® security research and intelligence capabilities, with several other revolutionary preemptive technologies from ISS. These technologies all work together to stop Internet threats before they can penetrate your desktops and impact your business—averting downtime and lost revenues.

What are the benefits?

EFFECTIVE PROTECTION FROM SPYWARE PLUS BOTH KNOWN AND UNKNOWN VIRUSES AND WORMS

Proventia Desktop's Virus Prevention System (VPS) detects and blocks spyware and more than 97 percent of new and unknown viruses and worms—without an update. Rather than relying on signatures for detection, VPS uses a patent-pending behavioral system that analyzes the activities of an executable file and detects whole families of malicious code. VPS runs code in a virtual environment, safely monitors the execution, and then evaluates for malicious content. This ensures that real threats are stopped, while valid traffic is undisturbed.

AN END TO DESTRUCTIVE BUFFER OVERFLOW ATTACKS

Proventia Desktop effectively addresses buffer overflows, which account for a significant portion of all high risk vulnerabilities. Buffer overflow attacks are insidious, because you can't protect yourself simply by not opening attached e-mail files. In fact, you don't even have to open a malicious e-mail message to enable the attack. With its Buffer Overflow Exploit Prevention, Proventia Desktop effectively blocks such attacks. Like a circuit breaker, it automatically trips to protect the system the instant malicious code tries to run.

VIRTUAL PATCHES ALLOW A RETURN TO SANITY

Proventia Desktop's intrusion prevention technology focuses on vulnerabilities to defend the likely targets of attacks within desktop systems—giving overworked personnel time to test and deploy vendor-issued patches on a rational, predetermined schedule.

STREAMLINED COMPLIANCE MANAGEMENT

Proventia Desktop ensures that users have compliant systems or are running protective software, like the desktop agent or antivirus, before allowing local access to the corporate network or remote access through a VPN. It can also prevent users from running or even installing banned programs.

LOCATION-BASED PROTECTION

Proventia Desktop automatically enables additional security when a laptop enters a foreign or un-trusted network, such as a wireless connection in a coffee shop.

EASY INTEGRATION

Proventia Desktop runs on the Windows 2000 Professional (SP 3-4) and Windows XP Professional (SP 1-1a) operating systems. It fits seamlessly within your existing corporate infrastructure and interoperates with Active Directory, most e-mail and Web clients, and popular antivirus and Virtual Private Network software.

SIMPLE, SCALABLE SECURITY

Proventia Desktop is easy to manage and scalable for small to very large deployments. Using ISS' SiteProtector centralized management system, administrators can control 100,000 Proventia Desktop agents from a single console.

LOWER TOTAL COST OF OWNERSHIP

Proventia Desktop reduces the total cost of ownership for security because it provides integrated, centrally managed desktop protection that is dramatically more effective and easier to oversee than patchwork solutions.

Multi-layered, multi-vector protection from Proventia Desktop defends an organization's desktop systems from all types of threats—known and unknown.





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 critical attributes:

	YES	NO
<input type="checkbox"/> True preemptive capabilities	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Multiple analysis techniques used to block both application-vector and network-vector threats	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Vulnerability-based security content	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Effective default protection policy	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Hands-free, out-of-the-box protection	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Scalable, central management capability	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Microsecond Latency	<input type="checkbox"/>	<input type="checkbox"/>

GLOBAL HEADQUARTERS

6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236-2600
e-mail: sales@iss.net

REGIONAL HEADQUARTERS

Australia and New Zealand
Internet Security Systems Pty Ltd.
Level 6, 15 Astor Terrace
Spring Hill Queensland 4000
Australia
Phone: +61 (0)7 3838-1555
Fax: +61 (0)7 3832-4756
e-mail: aus-info@iss.net

Asia Pacific
Internet Security Systems K. K.
JR Tokyu Meguro Bldg. 3-1-1
Kami-Osaki, Shinagawa-ku
Tokyo 141-0021
Japan
Phone: +81 (3) 5740-4050
Fax: +81 (3) 5487-0711
e-mail: jp-sales@iss.net

Europe, Middle East and Africa
Ringlaan 39 bus 5
1853 Strombeek-Bever
Belgium
Phone: +32 (2) 479 67 97
Fax: +32 (2) 479 75 18
e-mail: isseur@iss.net

Latin America
6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236-2709
Fax: (509) 756-5406
e-mail: isslatam@iss.net

Experience the advantage!

Discover how Proventia Desktop can protect your business from Internet threats. Be sure to ask if your company qualifies for a free 30-day trial.

Get more product information: www.iss.net

For an on-site demonstration, contact the ISS office nearest you.