



# Securing Your Desktop Computers

## Today — and Tomorrow

Client software and other approaches help keep systems and data safe

Gateway-level security protects your company's network — from intrusions, e-mail viruses, spyware downloads, spam, phishing, hostile applets, and other attacks and inappropriate content trying to enter through the gateway that connects your LAN to the outside world.

**B**ut you can't rely on gateway level security to stop all the attacks. "Even though firewalls see every packet, they don't scan every data stream for viruses," points out Joel Snyder of Tucson, Ariz.-based technology consultancy Opus One. "Data streams such as instant messaging [IM] or BitTorrent peer-to-peer file transfers aren't checked for viruses."

Gateway security appliances don't always properly scan some applications, such as Web-based e-mail — and firewalls can't penetrate encryption, which is used by many e-mail and other programs to check for security threats, adds Snyder.

What's more, your network gateway isn't the only avenue these threats have into your network and computers. They're sneaking in via USB flash drives, CDs/DVDs, handhelds, smartphones and notebooks infected while outside of your office.

"The network perimeter doesn't really exist anymore," notes Bob Hansmann, senior product marketing manager, Trend

Micro Inc. "People can set up unsecured wireless LANs for their workgroup with inexpensive routers. We see more of that than any physical violation."

According to a survey of 250 North American security professionals conducted by the IT research firm Enterprise Strategy Group (ESG), "Employee notebooks were the most common source — 39 percent — of worm attacks that get into the company LAN," says Jon Olsik, senior analyst at ESG.

The second most common source, Olsik reports, was "through the firewall," followed by non-employee notebooks and VPNs (virtual private networks) connected to home systems. "Three of the top four sources of this threat went around the firewall," Olsik points out. "This is why multilayered 'defense-in-depth' threat management is necessary."

All of which points to the fact that client devices — the desktop and notebook computers used inside your company's offices — need local antivirus and other protection more than ever.

### Security Software Secures the Desktop

Today's desktop security starts with the basics. Every desktop computer should be running a software firewall, along with ▶

the tools to keep it free from viruses, worms, spyware, adware and other types of malware,” says Kevin Haley, group product manager, Client Security products, Symantec.

Current versions of Windows, Linux and Mac OS include firewall features. In addition, third-party firewalls, and security suites that include firewalls, are available from McAfee, Symantec, Trend Micro, Zone Labs (a Check Point company) and others.

Along with firewall and antivirus software, no desktop today should be considered safe without one or more antispymware solutions loaded, to detect and block these programs from loading and help remove any that have already managed to sneak onto a system.

More recent additions to recommended desktop security software include antiphishing, intrusion detection/prevention, content filtering and instant messaging protection tools. (Some companies may consider that gateway or server-level protection is sufficient for spam or content filtering. However, if the user expects to use the computer outside the company network, additional precautions can make sense.)

Popular business-oriented, centrally manageable desktop security suites include Symantec Client Security, which combines a firewall, antivirus and intrusion detection, and Trend Micro OfficeScan, which includes a firewall along with antivirus and antispymware components.

“There will be increased integration of antivirus and antispymware in desktop security this year,” says Trend Micro’s Hansmann. “You’ll also see more security addressing IM, smart phones and collaborative technologies.”

One trend, reports Tom Henderson, managing director of technology testing consultancy ExtremeLabs Inc., is “more client machines being delivered to the customer with up-to-date antivirus and other security software already installed and configured — because it’s too easy for a machine to be attacked while the user is connecting and configuring it.”

Henderson also stresses, “Lock down system configurations to prevent users from installing noncompliant applications.”

### Limit Access Appropriately

Security updates and patches may be issued daily, but — especially with notebooks that get disconnected from the network — these fixes may not always be received and applied in a timely fashion.

Also, systems that don’t belong to your company, such as visitors’ notebooks, may not be running the security tools your business uses. You want to make sure that each layer and level is secured.

Products like Symantec Network Access Control offer endpoint security to check the status of systems each time they reconnect to the network. The central system will check whether the operating system and required security applications are installed, running and up to date in terms of patches and databases. If not, they can provide limited access — for instance, read e-mail but not upload attachments or files — or push the needed updates down to the machine.

### Central Updates, Configuration and Patch Management

Regular updates of security definition files and patches to operating systems and applications are an essential aspect of today’s desktop security management. The software on each client machine can be set to retrieve and apply these updates

automatically. However, this is an inefficient way to do it for networked machines.

Increasingly, software aimed at small and large businesses offers central console management to get and apply these updates and patches — along with tools to let you determine each desktop machine’s current state and define which machines, applications and updates have the highest priorities.

Depending on the operating systems, security utilities and other applications involved, you may be able to use Microsoft’s Update Manager and Systems Management Server (SMS). CA, McAfee, Symantec, Trend Micro and other security vendors offer central console management; also, third-party configuration, patch and update managers are available from manufacturers including Altiris, Desktop Authority, LANDesk, Novell ZENworks and Sitekeeper.

### Alternative Hardware Approaches

Today’s desktop and notebook PCs have a very obvious security vulnerability — the computers are accessible to whoever walks past. Somebody might be able to download data through a USB port, remove a hard drive or take the entire computer.

A variety of hardware and software solutions can help reduce these vulnerabilities. USB ports can be “locked down,” using hardware and/or software tools, so that only authorized users can download or upload data. Locking cables from vendors like APC, Kensington, PC Guardian and Targus can reduce the risk of theft of parts or entire systems.

And there are more extreme — but also more comprehensive — approaches to reduce the vulnerability of hardware on the desktop.

Thin client hardware products from HP, Neoware and Wyse replace desktop computers with small, dataless devices connecting to a central server. Users keep the same keyboard, display and mouse. However, there’s no drive or data on their desk to be stolen. Alternatively, existing desktop computers can be converted to thin-client systems using software-based solutions like Microsoft Terminal Services or Citrix

For situations where the user needs the full power and flexibility of a dedicated PC — or companies that don’t want to change their desktop system paradigm — there are other ways to take the computer off the desktop, and back into the computer room or data center.

One is using console extenders which simply connect the user’s display, keyboard, mouse and other desktop peripherals via a cable or a network connection to the computer, which can be behind a locked door, in a closet or in a computer room. Console extender manufacturers include APC, ATEN, Logitech and Tripp Lite. Of course, this means you’re now trying to fit several dozen to hundreds of desktop PC systems into an area where space is already precious.

“PC blades,” often used in combination with a NAS (networked attached storage), offer a way to bring your desktop computing power inside your computer room, with each blade containing the CPU, RAM, video graphics and other components of a client computer.

ClearCube, for example, offers PC blades with either Intel Pentium 4 or Xeon processors. A ClearCube Cage holds up to 14 blades, and a standard six-foot rack can hold up to 14 cages — up to 112 PC blades.

## Next-Generation Security

Today's Windows-based desktop computers can be all too vulnerable to a range of threats — or they can be so secured that it's harder for users to get their work done. That's going to change in the next several years.

AMD and Intel are incorporating security features into their next generations of CPUs and motherboards. For example, AMD's Presidio program is a set of technologies that will be rolled out in the next two generations of AMD desktop technology, according to Steven McDowell, division manager for strategic marketing, AMD.

Multi-vendor initiatives like the Trusted Computing Group's Trusted Platform Module (TPM) specification include a microcomponent that can be added to motherboards or other devices. The objective is to store digital keys, signatures or other security information more securely than software-based approaches (e.g. in a file on a hard drive).

According to Brian Berger, executive vice president of marketing and sales, Wave Systems, and marketing chair for the Trusted Computing Group, business-class desktop, notebook and Tablet PCs with TPM modules are currently available from vendors including Fujitsu, HP, Intel, Lenovo, NEC, Panasonic, and Toshiba. Over 20 million TPM-equipped devices have already been shipped, he says, and "IDC predicts full-scale implementation across all PC platforms by 2009/2010."

Next-generation client computers will also support hardware-aided system virtualization, according to AMD's McDowell. This will allow, for example, Web browsing to be done in an


unsecured virtual machine. Any data or files the user wants to save to the secure business VM will have to pass through a firewall that inspects them carefully.

On the software side, Vista — the next version of Microsoft's flagship Windows operating system — will include numerous security features. "Vista will be immune to certain kinds of threats," says Trend Micro's Hansmann.

According to Windows network security consultant Tony Northrup, changes will include User Account Control (UAC), which lets common settings be changed from user level without requiring administrative privileges; Internet Explorer Protected Mode, which protects user data and configuration settings; Windows Defender (formerly known as Windows AntiSpyware) which will detect potentially suspicious software; and Windows Service Hardening.

## Advice for IT

One trend is clear: The need for desktop security won't be going away. If anything, it will only increase, as new applications create potential new vulnerabilities, and the increased use of mobile devices outside the company network increase the opportunities for network threats to bypass guardian gateway security.

Protecting your organization means guarding against attackers. However, don't forget about internal issues. Tools are essential, but so is user education. Clearly posted, easy-to-follow policies, combined with security awareness training, will help keep user errors to a minimum. 

# The Importance of Passwords

Desktop security can often begin with the common things — like passwords. For added security, have the staff at your business follow these guidelines.

- **Utilize complex passwords**

All workstations should have a complex or strong password for log-in. Complex passwords are those incorporating uppercase letters, lowercase letters, numbers and symbols. In addition, all workstations should have a password-protected screensaver or similar feature that allows the workstation to be secured from unauthorized use.

- **Eliminate automatic log-ins**

Workstations must never be set to automatically log in to the operating system or network services. And browsers on workstations should not be set to remember log-in/authentication information for Web access to services.

- **Change passwords regularly**

One of the most effective means users have of protecting computing systems is to change their passwords regularly — quarterly for access to normal systems, and monthly for access to more sensitive systems.

- **Secure passwords**

When passwords are changed frequently, it's easy for users to forget them. Passwords may be written down and stored in a secure location, such as a locking file cabinet or desk drawer. Remind personnel to never write a password on a sticky note attached to a monitor or stored under the keyboard, or record it in an application file, such as a Word document or Excel spreadsheet.



CDW offers a portfolio of value-added services to help expand your IT capabilities.