



# Securing the Client

---

Multidimensional endpoint security plan prevents risks from theft, interference and abuse.

Running a business is full of risks and challenges. And in today's increasingly complex IT environment, it's difficult to make it through a day without fretting over viruses, intrusions, spam and new and insidious forms of theft.

These days, it's impossible to manage operations without protecting against an onslaught of security threats. Spyware, rootkits, phishing and pharming techniques, malicious code and outright theft are all growing dangers.

Yet, as the sophistication level of hackers and crooks grows, it's no longer possible to rely on only basic protections. Today, you need more than antivirus software, intrusion detection systems and Virtual Private Networks (VPNs) to effectively block security breaches.

### Layered Approach

Without a multifaceted and layered approach to endpoint security — using the right tools and techniques — disaster can ensue. As the business environment has become more dangerous, "It's up to organizations to respond appropriately," says Joseph Feiman, a research vice president at tech research firm Gartner, in Stamford, Conn. Adds Kevin Haley, manager of the endpoint security product line for Symantec: "Complacency can lead to huge problems."

No enterprise can afford to lose valuable data or see its systems damaged. But the outright cost of an incident isn't the only consideration.

Businesses that find themselves the target of hackers or thieves may face legal liabilities, diminished employee productivity, damage to their reputation and reduced system and network performance levels. The toll can ripple throughout the organization and beyond, affecting customers and business partners.

All this is leading a growing number of companies to adopt an endpoint security mentality. Although many organizations have effectively secured the perimeter of their network, the weak point is at the desktop and on the notebook. This approach translates into using a holistic approach to combat threats.

### Endpoint Security Challenges

The endpoint security challenge is fourfold:

- Protect the endpoints against malware
- Prevent infected endpoints from introducing malware and unauthorized software to your network
- Prevent data leakage and data theft via endpoint devices
- Protect against the endpoint users themselves

Of course, you can take an extreme approach and simply lock down your network, so that remote clients cannot access it. That's effective, but it's not practical in today's mobile-computing environment.

You can also try to get your organization to commit to a thin-client approach, where all the applications and information remain inside your network perimeter. However, that can be a costly and long-term project.

A more reasonable approach is to develop an endpoint security strategy that balances both security risks and end-user convenience and productivity.

### Confronting Danger

Hackers and thieves are constantly on the lookout for weak points within companies. Although IT security risks have been around since the first mainframes appeared decades ago, the advent of the Internet and open architectures has spawned bigger and more insidious attacks.

"As new technologies take hold and there are more ways to connect, a greater number of vulnerabilities occur," says Sam Curry, vice president of product management at software provider CA.

In many cases, the result is a cat-and-mouse game that has each side making countermeasures to respond to increasingly complex tactics. For example, some malware writers have now achieved "zero day" status, meaning they exploit a security vulnerability the day it becomes known.

Meanwhile, polymorphic viruses, which have the ability to modify their own codes each time they replicate, have become part of the digital landscape. They are sometimes able to slip past antivirus software, thus ratcheting up the challenges for organizations looking to defend data and assets.

In the early days of computing, the payload usually arrived via disk or e-mail, but now virus attacks have become more sophisticated and varied. One of the most vulnerable areas is instant messaging (IM), which has exploded in popularity over the last few years.

Today, many employees expect IM as a basic service offering but are unaware of how effective it is at carrying and spreading malicious code, including viruses, worms, Trojan horses and social engineering tools.

The biggest problem with instant messaging is that there's no way to verify or authenticate the person on the other end. This makes it easier to spread malware.

E-mail viruses continue to evolve as well. Some messages spoof known users, while others use the HyperText Markup Language (HTML) scripting ability in a mail client, such as Outlook or Eudora, to download malicious code.



## Tips for Better Endpoint Security

- Create a security policy that takes into account all client devices, including desktop and notebook computers, PDAs, portable storage products and smartphones.
- Establish clear usage standards for all business-owned devices, including who should use them, how they should be used and what data can be accessed.
- Train employees to use systems and applications securely.
- Evaluate a broad range of security technologies, including client firewalls, encryption, antivirus software, antispam programs and intrusion detection/prevention systems, to determine which are most appropriate.
- Conduct a thorough and ongoing analysis of systems and applications to ensure that security standards are being met by managers and staff.
- Keep antivirus, antispam and antispam programs up to date.

Still others use stealth techniques that intercept an antivirus software's requests to scan a file. A few also combine malware with social engineering to trick users into visiting a Web page, where they download a virus or fill out information that looks real but is in reality a scam.

### The Human Element

Social engineering isn't only a way to spread viruses. It's an increasingly popular method used by thieves to steal identity data.

Over the last few years, phishing (fraudulently acquiring sensitive information, such as passwords and credit card numbers, by masquerading as a trustworthy person or business) and pharming (the exploitation of a vulnerability in DNS [Domain Name System] server software that allows a hacker to acquire the domain name for a Web site, and to redirect the site's traffic to another site) have emerged as major problems for businesses.

While most phishing techniques target individuals through spam and many appear to come from banks and other financial services firms (using spoofed e-mail addresses), a few have attempted to glean account numbers or financial data that reside in customer or vendor databases.

Increasingly, businesses find themselves the target of phishers as well as the victims — as thieves replicate legitimate company Web sites and use them to trick unwitting consumers. American Express, Citibank, Wells Fargo, Bank of America, Visa and Microsoft are among the companies that have had to deal with business identity theft.

Spyware and adware also have become major problems — and protection against these threats has become essential. As the Internet has evolved into a mainstream tool, it has redefined the notion of privacy and security.

Some hackers and data thieves send e-mail attachments that contain hidden applications that install themselves on a PC and use stealth methods to control systems, glean data or log keystrokes. Less malevolent adware infests a PC with code that generates pop-up ads. These can waste staff time and drain overall productivity.

A few applications also install rootkits. These programs, which install surreptitiously on Windows, Linux, Solaris and other platforms, conceal running processes, files or system data, thus making it easier for an intruder to gain and maintain access to a system without detection.

### Security Products

The rising level of sophistication, and the growing importance of protecting data that's critical to business operations, calls for a multidirectional approach to endpoint security that provides multiple levels of protection.

Among the technologies that can be part of the layered approach to endpoint security include:

- Network Access Controls
- Data Encryption
- Personal or Network Firewalls
- Antivirus Software
- Antispam Software
- Antispyware
- URL Content
- Web Filtering
- Intrusion Prevention and Intrusion Detection Systems
- Authentication Technologies (such as biometrics systems)

Not all organizations need to deploy all of these security elements, but using a combination of technologies can help prevent data loss or theft in the event that one layer of defense is breached.

Here's a sampling of security products on the market that can help organizations create a multifaceted client security approach:

**Symantec Multi-Tier Protection** provides protection against malware for notebooks, desktops and servers, mail servers and gateways. It includes Symantec Endpoint Protection, Symantec AntiVirus for Linux and Macintosh, and mail protection that shields against e-mail-borne virus threats and security risks. Endpoint Protection integrates technologies such as antivirus, antispyware, firewall, intrusion prevention and device control.

Vircom's modusGate is a secure e-mail gateway that provides content-filtering technology to protect inbound and outbound e-mail communications. The product provides a first defense against denial of service, spam and other attacks.

If a message cannot be validated, modusGate won't accept it. Vircom's Sequential Content Analyzer engine monitors millions of daily transmissions to maintain a knowledge base of the latest threats in circulation. The product applies separate filtering strategies, administration and end-user quarantining to counteract phishing.

Webroot's AntiVirus with AntiSpyware & Firewall software provides comprehensive protection against a range of security threats such as viruses, spyware, adware, worms, trojans and key loggers. It also monitors all traffic to and from a computer to block unauthorized access attempts. If a PC is already infected with malware, the software uses advanced discovery methods to find and destroy malicious programs.

Websense Enterprise is a Web filtering software tool that enables organizations to safeguard Internet access by employees, allowing companies to establish flexible Internet use policies and filter sites based on time of day. Organizations can set policies for file types and more than 80 application protocols, including e-mail, file transfer, remote access, streaming media, instant messaging and peer-to-peer protocols.

PGP Encryption Platform enables organizations to deploy gateway- and desktop-based encryption based on specific requirements for data security within the organization. PGP products can secure internal and external communications, data stored on servers, desktops and notebooks, as well as automated backups and data transfers.

Check Point Integrity SecureClient combines a VPN and endpoint security in a single client installation. The product features centralized management, advanced remote access security, a network firewall, host intrusion prevention and integrated antispyware.

## Risky Business

Maintaining a high level of endpoint security is no simple proposition. Over the last few years, attacks have grown in sophistication and malware has become far more dangerous, unpredictable and widespread.

Not only have hackers stepped up their assaults on businesses, they've become smarter and more creative, using buffer overruns, spoofing, stolen IDs, SQL (Structured Query Language) injection techniques and an array of other approaches.

Because so many pieces to the security puzzle exist, many organizations find themselves allocating growing money and resources to a variety of security flash points, including infrastructure, VPN, intrusion detection, monitoring tools and actual code.

While some of these security solutions can be costly, organizations increasingly view them as a basic cost. In fact, many understand that they're no longer an option but a necessity. ◊

## USB Drive Security

Universal Serial Bus flash drives are infiltrating the workplace — for good reason. They're easy to use and not too hard on the budget.

Yet, data loss via USB drives and other removable media is now the top concern for endpoint security, ahead of trojans, spyware and other threats.

A recent survey on endpoint security sponsored by Vontu Inc. and conducted by Forrester Consulting, released in January 2007, showed that most companies have lost confidential data through removable media such as USB drives in the past two years.

Among the key findings of the report, based on an online survey of 151 decision-makers at North American companies with annual revenues of more than \$200 million, are that more than half of respondents (52 percent) have lost confidential data through removable media.

USB drives are convenient. They allow employees to carry copies of e-mail and other documents on them, cutting down on the need for remote access to the office network. Salespeople can also load presentations and brochures on them and then hand out the devices to prospects.

The devices come in capacities ranging from mere megabytes to hundreds of gigabytes. While these little devices are a cost-effective way to carry data around, information technology managers need to guard against security breaches.

### Security precautions when using portable storage include:

1. Setting company policies and driving employee awareness of the security issues posed by thumb drives
2. Making certain the host computers are running up-to-date antivirus, antispam and antispyware software
3. Using only those drives that offer built-in encryption and/or password protection
4. Considering endpoint security software that allows administrators to manage user access and log thumb-drive activity