ENTRUST

Enhance threat monitoring and cut administrative burden while protecting endpoints against known and unknown threats.

In today’s world, the network is the business, plain and simple. The information stored on and accessed through the network — everything from training webinars and market research to customer transactions and investment strategies — is critical to nearly every aspect of a company’s day-to-day operations.

ING ENDPOINTS

Yet, a significant portion of the network remains in the hands of nontechnical staff with little understanding of the complexities of security. These are often devices operated beyond the confines of the network’s firewall and outside the physical reach of the team charged with maintaining the network’s integrity.

That is the proverbial endpoint, the intersection between a firm’s employees and the network resources that make their work possible. And while today’s layered security model stresses a holistic defense-in-depth approach to protecting network assets, the endpoint presents unique challenges to network security and so demands special consideration.

Fortunately, there are security solutions available to protect enterprise network endpoints. The benefits of a layered and multidimensional plan of attack can help prevent risks from theft, interference and abuse.

In the Wild

An endpoint comes to life whenever an employee or other person interacts with a company’s network. “Ultimately, the endpoint is simply a human that is touching technology,” says Scott Emo, head of endpoint product marketing at Check Point Software Technologies. “Typically in today’s business world that technology is touching a network and that’s what makes it dangerous.”

Some obvious examples in the corporate environment include desktop and notebook computers and smartphones. But any piece of equipment that provides access to company resources via a network connection can and should be considered an endpoint.

Increasingly, mobile devices like iPhones, BlackBerry devices and other personal digital assistants (PDAs) are endpoints on the network. Endpoints can also include USB drives, burned CDs and DVDs, Voice over IP (VoIP) devices, kiosk stations, even physical infrastructure such as networked door locks and surveillance cameras.

“Defining the endpoint is a lot harder today than it was five years ago, says analyst Mark Kadrich, CEO of The Security Consortium. “A lot of things that you don’t realize have network connections have network connections.”

And in this age of increasing mobility, the number of potential endpoints is multiplying rapidly. E-readers, netbooks, even portable media players often have access to some network services and can create ever-larger windows into your corporate network.

Securing the endpoint tends to be difficult not only because there are so many — and so many kinds of — endpoints, but because there are so many ways that any particular device can be compromised. Therefore, businesses must consider physical security beyond the network infrastructure and the corporate data center.

Although determined thieves could conceivably steal a server, it’s not likely to be left in a cab or swiped by a pickpocket. Nor is it likely to be used in an insecure environment such as a coffee shop with a Wi-Fi hotspot or in a home with unprotected wireless network access.

Types of Threats

Endpoints face three broad categories of threat: physical such as theft or loss, infection by malware, and intrusion or eavesdropping by third parties. Each of these potential vulnerabilities requires a different response to protect both the data stored on devices and the network as a whole.

1. Physical Data Loss — Because endpoints offer access to a wide range of private information, losing physical control over a device can be devastating. Mobile devices such as notebooks and smartphones are particularly prone to being lost, whether through their owners’ error or by theft.

DEFENSE IN DEPTH:

A Way of Network Life

Securing a business network is complex. The layered approach to security aims to manage that complexity by envisioning the network as a set of nested layers, like an onion or a set of Russian nesting dolls, each with its own appropriate forms of security.

Each layer sits inside the protection of the last and provides protection to the next, slowing down (and, with hope, deterring) attackers. And should a layer be breached, the theory is that each ensuing layer also provides network monitoring tools adequate time to detect the breach and so prevent it from allowing the hacker or malware systemwide access.

From the outside in, these layers boil down to:

- **The endpoint:** Any device through which a user interacts with the network, such as smartphones, notebooks, desktops and other attached devices
- **The perimeter:** The outside boundary of the network defined by its firewall
- **The network infrastructure:** All inter-connected resources available inside the corporate firewall, including computers, storage repositories, access points, routers and switches
- **Servers:** Both the physical devices on which applications and services run and the software that provides applications, files, e-mail and other services to users on the network
- **Applications:** The particular programs with which users interact to perform tasks, including e-commerce applications, customer relations management software, productivity suites, bookkeeping and accounting programs, e-mail clients, web browsers and multimedia editors
- **The data:** Any information generated and/or used in the operation of the business, including letters and memos, transaction records, marketing reports, sales presentations, spreadsheets, personnel files, product designs and training materials

But the risk of physical data loss includes more than just mobile devices — even wired workstations can potentially be at risk. “There are some attacks that no firewall can prevent,” says Dmitriy Ayrapetov, SonicWALL product line manager for network security.

“For example, I can walk in with a thumb drive, through the front door of an organization and plug it into a laptop.” Without effective safeguards in place, anyone with physical access to a machine on the network can attempt to access corporate information.

“The best way to defend against physical data loss is with encryption,” Check Point’s Emo says. Full-disk encryption is a necessity on mobile devices to prevent unauthorized access to not only the data but also any applications and clients that connect to the corporate network.

Controlling a device’s ports so that data can’t be taken by unauthorized users through a thumb drive or external hard drive is also critical. Check Point’s Endpoint Security suite automatically encrypts data stored on external media, protecting against intentional theft as well as user error such as the loss of an unencrypted flash drive or DVD.

2. Malware — The most rapidly changing threat area in the digital realm is malware. Hackers with criminal intent tap an ever-evolving arsenal of viruses, Trojan horse attacks, worms, spyware and other software installed surreptitiously to gain access to network resources for financial gain and other more deviant motives.

“These programs are intended to do damage,” says Emo. “And the damage they do is entirely up to the imagination of their creators.”

Malware can come from just about anywhere: a corrupted file, an e-mail attachment, even legitimate websites whose pages have been modified by malicious hackers to create payload-laden malware downloads. And once hackers gain access to a system, they will take advantage of whatever resources and tools are available to copy data, steal passwords, send spam or other attacks, and control any network resources available to the device, including those behind the corporate firewall.

Traditional antimalware protection relied on the use of virus signatures to detect code known to harbor malicious software. As the creators of malware grew more sophisticated, however, signature-based malware detection became only one aspect of protection against malware.

For example, Symantec Endpoint Protection incorporates heuristic analysis, intrusion detection and application control. It’s designed to determine when a program is behaving outside the norm and whether to terminate it.

3. Intrusion — Although intrusion overlaps somewhat with malware — keyloggers and IRC bots used by third parties to spy on users, for example — it is worthwhile to distinguish between broadly targeted automated malware such as viruses and Trojans and intentional snooping. “Increasingly, threats are becoming extremely targeted, with extensive research about the particular person used to craft specific attacks,” says Bernard LaRoche, Symantec’s senior director of product marketing for enterprise security.

The tools for detecting and blocking malware that’s used to spy on a particular user’s activities are generally effective. This is because suspicious activity by a program is suspicious regardless of whether the malware was the result of a random infection or a targeted attack.

But to protect against eavesdropping over a shared Internet connection such as a Wi-Fi hotspot or hotel network, a strong personal firewall can prove essential. A number of vendors like Check Point, McAfee, SonicWALL, Symantec and WatchGuard offer such products.

In addition, creating a secure tunnel back to the corporate network through a virtual private network (VPN) is a priority. It can help ensure that all traffic between the endpoint and the server is encrypted, which protects the data even if someone sniffs the data stream.

The Network-Endpoint Connection

Effective endpoint security extends beyond a device itself. "The endpoint is not an island," says Mike Rothman, president of the security analysis firm Securosis. "Endpoint security needs to be considered within a much bigger security architecture."

No single solution can ever be 100 percent secure. Attacks are evolving at a tremendous rate and nobody can know what new threat will emerge tomorrow. Today's security planners take a layered approach to network security, building each successive layer to compensate for the potential failure of the layer above it.

"Let's say the best catch rate is 99 percent," says SonicWall's Ayrapetov. "If you have 1,000 attacks and a 99 percent catch rate, then 10 attacks will still get through. If you only have one security layer, then you only have that one chance to catch them."

In a layered model, attacks that get through the first line of defense, in this case the endpoint, are subjected to another filter at the next. "If your next layer also has a 99 percent catch rate, then 99 percent of those 10 attacks will be caught, leaving none or, maybe, one," Ayrapetov adds.

For example, firewalls from Check Point, SonicWall and Symantec offer compliance checking, a method for assuring that the software on a connecting device is up-to-date and fully operational before giving the user access to the corporate network. This can play a vital role in keeping out the predators because successful attacks generally modify the endpoint to make the attack and its consequences invisible.

"Antivirus and other protections only work on a known, uninfected body," says Kadrich. Once a system is infected, you can no longer depend on that system's defenses to protect the network and have to rely on another, external system — another layer — to detect, quarantine and remove an infection.

Symantec's Protection Suite Enterprise Edition integrates endpoint tools such as antimalware with centralized administrative and management functions that run from the server. "If I'm the network administrator, how can I have transparency and visibility so I can see when and how the endpoint is being attacked?" asks Symantec's LaRoche. Creating a second view of the system from another layer addresses that issue.

Principles and Practices

Security in reality is not a product or even a system, it is a process, says Kadrich. "People think about security as a point-and-shoot situation when they really need to think of it as a behavioral problem, a procedural problem." The technology used to secure the endpoint provides the tools to implement and automate policies that protect the entirety of the network.

Fortunately, there are fairly well understood principles that can be applied to any security situation. This goes for protecting a house from burglars or an enterprise data center from corporate spies.

"Security starts with a few basic questions," Rothman says. "What are your risks? How are you exposed? And then you back into, what's the best way to protect specific devices" from those risks and exposures?"

"Learn the principles," advises Ayrapetov. "Once you've learned the principles, you can apply them to any case." ◊

ANATOMY of an Attack

An attack can be broken down into four basic stages, says Bernard LaRoche, senior director of product marketing for enterprise security at Symantec.

1. **Incursion:** The attacker gains access to a system, whether through a virus or other infection or through physical access to the network.

2. **Discovery:** The attacker explores how the system is protected and where information resides.

3. **Capture:** The attacker evaluates the risks involved in retrieving specific information against the potential payoff.

4. **Exfiltration:** The attacker copies data off the system or tampers with system components in some way.

Working with your account manager, a CDW technology specialist can customize a security solution for your business.