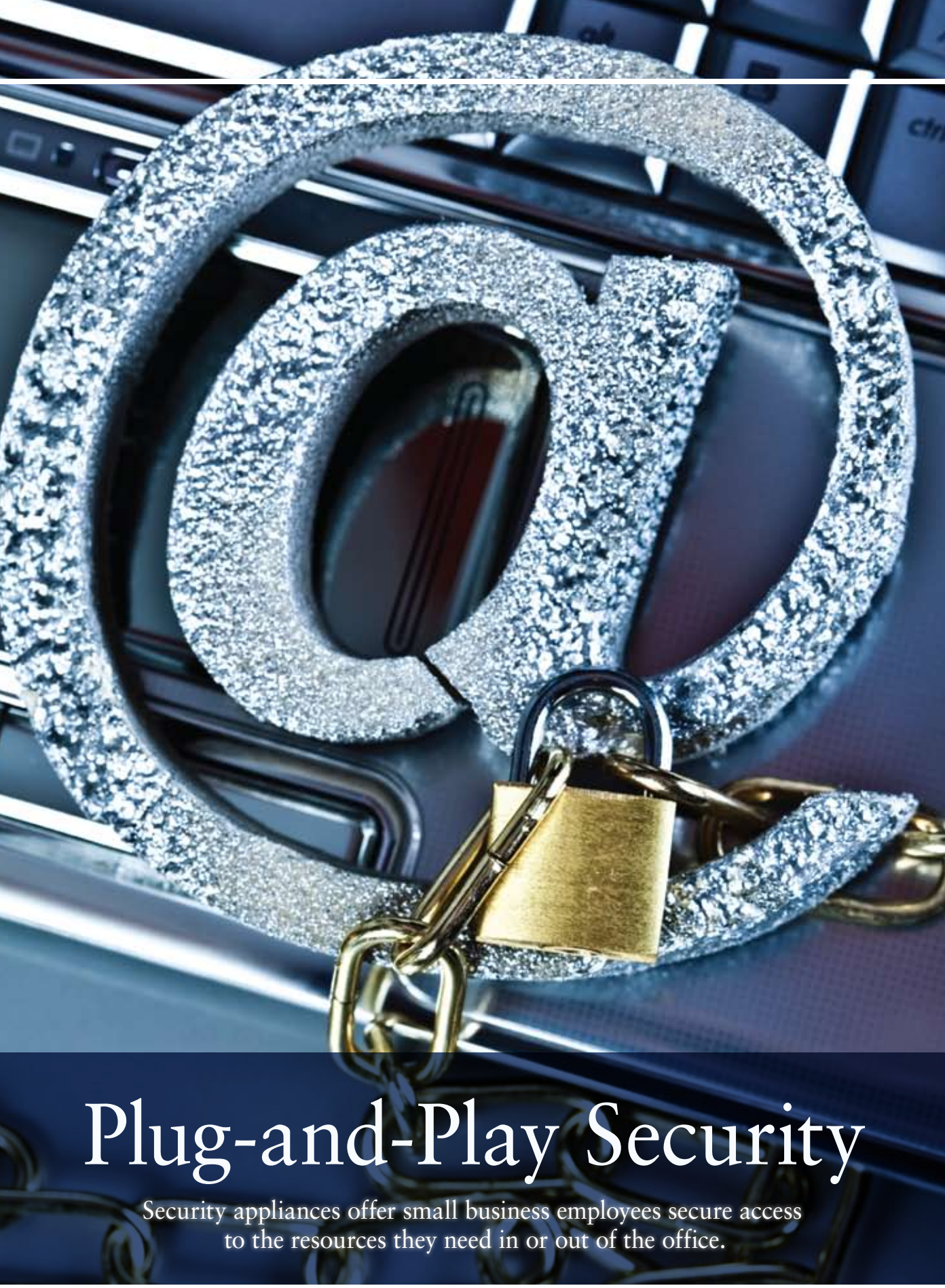

Plug-and-Play Security

Security appliances offer small business employees secure access to the resources they need in or out of the office.

The Internet is a dangerous place. Between hackers, script kiddies, corporate espionage, viruses, worms, malware and plain old user errors, it might seem almost not worth the hassle to connect a company at all.

Of course, not being online isn't an option in today's business world. Between providing access to applications for remote sales staff and teleworkers who do the day-to-day heavy lifting and serving up e-commerce tools for customers, there's hardly a business around anymore that isn't at least a little web-centric.

So how can a small business, with limited IT staff, an every-penny-counts budget and a thousand other things to worry about make sure that its data is safe and secure? Fortunately, a new breed of security appliances makes it easy for small businesses to protect their networks with minimum tech know-how, so they can focus on the business of running a business.

Security Challenge

Network security has traditionally been a rather complex affair. There are so many kinds of threats that can attack the network, with countless ways to get inside and start wreaking havoc — and the tools that protect against one kind of threat might be useless against another.

At a minimum, network security consists of a firewall to detect and prevent efforts to enter the network or to send data out. Other must-haves include antivirus and antimalware software that detects malicious programs, either as they are downloaded (via e-mail or from a web page) or as they attempt to install themselves or operate on an infected computer.

Intrusion detection is another key component of network security. It monitors network and/or system activities for malicious software or hardware that doesn't belong on the network.

These tools can and should be run both at the level of individual machines and at the gateway to the network. For example, recent Microsoft Windows computers ship with a firewall to prevent unrequested incoming traffic and hackers or free-floating Internet worms from accessing the computer remotely.

Likewise, most small businesses run a firewall on their entire network, even if they don't know it. This is because most routers function as a basic firewall as well as a modem, hub and a switch. This prevents unauthorized incoming traffic such as worms or hack attacks.

Although this may seem redundant, security is definitely an area where it pays to take a belt-and-suspenders approach. This is because new threats emerge all the time. What's more, no one tool can possibly cover every possible contingency.

UTM and Small Business

In the past, the way to implement all the different kinds of security tools a business needed to protect its network was to set up a server with separate point solutions for each task. This might include virus scanning, intrusion detection, malware protection, spam blocking and so on.

In a large enterprise setting where there were several specialized employees that could focus solely on security issues, this approach had logic on its side. But small businesses don't have security teams. They may not even have full-time IT support.

They cannot afford someone to maintain constant diligence over a single, highly specialized application. Mike Rothman, president of the security analysis firm Securosis, points out that >>>>

Elements of a Security Plan

Writing a formal security plan for a business is a good idea. Having even a rough overview of what needs protecting and how the pieces fit together can help the company make smarter choices and waste less time on imaginary problems. Here are some questions to ask:

1. **What are we trying to protect?** Customer data, intellectual property, income statements are obvious. But don't forget about things such as network resources.
2. **What are the main elements of your network?** A small wired network with a few desktop computers and a storage server requires a different approach than a mixed Ethernet and Wi-Fi network in a retail environment or one with numerous remote workers.
3. **What skills does your staff have?** An honest assessment of the abilities of your employees will help you put together a security system tailored to their strengths and weaknesses.
4. **What threats do you face?** Some threats, such as free-floating Internet worms, are simply endemic to the Internet and always present. Others, such as tech-savvy competitors or criminals with a specific interest in your data, will be unique to your particular situation.
5. **What data protection guidelines must you comply with?** If you accept credit card payments, store medical records, process legal data or hold government contracts, you may need to meet specific security compliance mandates.
6. **What will a security breach cost you?** Knowing what's at stake will help determine what is reasonable to spend on your network security. You need to quantify the cost of an incident with required security measures.
7. **How will you recover from a breach?** As advanced as today's security technologies are, no approach is 100 percent foolproof. Having a plan in place for recovery from various kinds and degrees of attacks will allow getting a business back on its feet as quickly as possible when something goes wrong.

small businesses face a "triad of pain" when it comes to security: "They don't have enough time, enough resources or enough expertise to manage enterprise-level security applications."

Security appliances are a much better fit for small businesses. "If you're a small business and you want quick coverage at a reasonable price from people who have been doing security for a long time, you go for a security appliance," says Jeff Wilson, principal analyst for network security at Infonetics Research. "There are tons of specialized applications, but small-to-midsized businesses shouldn't even look at them."

Security appliances are standalone, preconfigured devices that plug directly into the network and start working instantly. Although single-function appliances exist, as Wilson points out, most small businesses should be looking at unified threat management (UTM) devices.

These appliances combine a firewall with antivirus, antimalware, intrusion protection and other security tools, all accessible through a single combined interface. In addition, UTM solutions come in the form of physical UTM appliances as well as UTM software.

"You get protection without having to understand what's going on under the hood," says analyst Mark Kadrich, CEO of the Security Consortium. "Load it in the rack, plug in the line in, plug in the line out, and a basic set of rules begin to protect you."

The simplicity of the appliance model yields a wide range of benefits for small businesses. Because they require little time to set up and manage, security appliances allow already over-burdened IT staff to focus on other concerns, increasing productivity across the business and saving employers the cost of hiring new workers to deal with the added responsibilities of security.

Because the various tools that make up a UTM system are designed to work together well and all share a single interface, they are easier to manage. And that can help lead to fewer mistakes or oversights.

Better security in general means better productivity too. Spam prevention at the appliance means less clutter for workers to wade through in their inboxes.

Blocking malicious software at the network level means workers don't have to stand idly by while their computers are reimaged following a virus or Trojan horse infection. And everyone benefits from increased peace of mind when they know their hard work isn't going to be deleted by a poorly written worm or undermined by an outside attack.

Deployment Tactics

A UTM appliance represents an important first wall of defense in a company's overall security plan. "It's important to think of security in terms of layers," says Dmitriy Ayrapetov, product line manager for network security at SonicWALL.

"Think of a bank," he says. "It's not like the bank has a vault door opening out onto the front street. First you have to go through the front door, get past the security guard, go behind the desk, pass the security camera, and go through several doors before you ever get to the vault door."

The outer layer provided by a security appliance is the bank's front door. All traffic going into and out of your network has to pass through it before it can reach anything important on your network.

The security appliance scans each packet of information that passes through that "door." This is to make sure it doesn't contain anything suspicious, whether that's a virus or other malware spam, or increasingly, a malformed file that could be used to exploit a security hole in another application or at a later time.

"The number one source of attacks last year was through malformed PDF files," says Ayrapetov. "Attackers maliciously craft a PDF file that takes advantage of a vulnerability to install whatever they want on a system. The file looks totally legitimate — the only way to stop it is by inspecting each packet."

This is basically a new phenomenon. In the past, most attacks were carried out using applications — viruses, spyware, keystroke loggers and other malicious executables that installed themselves onto a system.

SonicWALL's NSA 2400 and WatchGuard Technologies' XTM 2 Series use deep-packet inspection to examine each file as it arrives on the network and to provide security at the content level. "If a business is not doing that, it's leaving the door open," Ayrapetov says.

This applies to remote access as well. When employees connect to your network from outside, they have no control over the state of their machines or their Internet connections. Even a careful employee could become infected by connecting through a public Wi-Fi hotspot or even a home network, while a less diligent computer user might connect with an infected device.

SonicWALL's NSA 2400MX Clean VPN system subjects all virtual private network (VPN) traffic to deep-packet inspection. It also offers antivirus, antispam and intrusion protection before letting an outside device onto the network.

Ease of Management

Automation is important in small business settings where it might be impractical to give every intrusion, detected virus or other threat individual, hands-on attention. Security appliances allow you to set up policies, often using familiar wizard-based interfaces, to automatically respond when certain conditions transpire.

For example, the Cisco Systems SA 500 Series Security Appliances monitor not just incoming traffic with the usual mix of firewall, antivirus, antimalware, spam detection and intrusion protection, but also individual computers on the network using the ProtectLink Endpoint service.

When a computer on the network fails to meet the conditions imposed by assigned security policies — for example, if a computer is infected by a virus, or fails to authenticate properly — ProtectLink disconnects the system from the network. This prevents any problem from propagating through the network and bringing the whole system down.

Scalability is also important, especially for small businesses because their needs often outstrip their resources as they grow. WatchGuard's line of security appliances runs from the XTM 2 Series, aimed at businesses with up to 50 users, to the XTM 1050, for enterprises with up to 10,000 users.

Although a small business may never reach 10,000 employees, it could well top 50. Therefore, it's important to know that upgrading your system won't mean radically disrupting the security plan or business as a whole.

"Each appliance runs the same operating system," says Tim Helming, WatchGuard's director of product management. "So as you move up, you don't have to learn a bunch of different interfaces."

Risky Business

There was a time when small businesses could be fairly confident that they presented too small a target to be of interest to most hackers. But times have changed; hackers have become cybermercenaries, with an interest more in getting paid than making a name. The result? Every computer on the Internet is a target.

"Hacking has gone commercial," says Wilson of Infonetics Research. "It has nothing to do with ego anymore. Today, we have nimble, organized hackers looking for anything that can be bought and sold digitally."

That means your business is at risk the minute it connects to the Internet — and almost no business today can afford not to connect to the Internet. Security appliances help minimize that risk, offering powerful threat management capabilities at a cost and scale well suited to small business budgets.

"The security appliance market is doing something we could never do before," says Kadrich of the Security Consortium. "They're providing a baseline of protection by making security accessible to everyone." ◊

According to a Symantec study:

75%
Businesses that experienced cyberattacks in 2009 (29% on a regular basis)

41%
Businesses that reported these attacks as "somewhat or highly effective"

29%
Businesses that said attacks had grown significantly in 2009

SOURCE: Symantec

Identify potential security vulnerabilities by taking the CDW security survey at CDW.com/securityassessment