



Counterpane™
Internet Security

Managed Security Monitoring: Network Security for the 21st Century

Bruce Schneier, Founder & CTO



Introduction

The Internet is critical to business. Companies have no choice but to connect their internal networks to the rest of the world: customers, suppliers, partners, and their own employees. But with that connection comes new threats: malicious hackers, criminals, industrial spies. These network predators regularly steal corporate assets and intellectual property, cause service breaks and system failures, sully corporate brands, and frighten customers. Unless companies can successfully navigate around these, they will not be able to unlock the full business potential of the Internet.

Real security is about people. On the day you're attacked, it doesn't matter how your network is configured, or how many security devices you've installed. What matters is who is defending you. The only way to stay ahead of new vulnerabilities and attacks is through detection and response. In the real world, this translates to alarm systems and guards. On the Internet, this means active network monitoring.

Security network monitoring provides immediate feedback regarding the efficacy of a network's security—in real time, as it changes in the face of new attacks, new threats, software updates, and reconfigurations. Monitoring is the window into a network's security; without it, a security administrator is flying blind. Wherever a network is in the process of building security, monitoring is the first thing you need to do.

The Importance of Security

Computer security is a fundamental enabling technology of the Internet; it's what transforms the Internet from an academic curiosity into a serious business tool. The limits of security are the limits of the Internet. And no business or person is without these security needs.

The risks are real: theft of trade secrets, customer information, money. People also talk about the productivity losses due to computer security problems. I've seen figures as high as \$10 billion quoted for worldwide losses due to the ILOVEYOU virus; most of that is due to these productivity losses. More important are the indirect risks: loss of customers, damage to brand, loss of goodwill. And more indirect risks are coming. European countries have strict privacy laws; companies can be held liable if they do not take steps to protect the privacy of their customers. The U.S. has similar laws in particular industries—banking and healthcare—and there are bills in Congress to protect privacy more generally.

Real security is about people. On the day you're attacked, what matters is who is defending you. The only way to stay ahead of new vulnerabilities and attacks is through detection and response. On the Internet, this means active network monitoring.

As risky as the Internet is, companies have no choice but to be there. The lures of new markets, new customers, new revenue sources, and new business models are just so great that companies will flock to the Internet regardless of the risks. This, more than anything else, is why computer security is so important.

The Failure of Traditional Security

Network security is an arms race, and the attackers have all the advantages. First, the defender has to defend against every possible attack, while the attacker only has to find one weakness. Second, the immense complexity of modern networks makes them impossible to properly secure. And third, skilled attackers can encapsulate their attacks in software, allowing people with no skill to use them. It's no wonder CIOs can't keep up with the threat.

Security is a not a technology problem, it's a people problem. There is no computer security product that acts as magical security dust, imbuing a network with the property of "secure." It's not the way business works.

What's amazing is that no one else can either. Computer security is a 40-year-old discipline; every year there's new research, new technologies, new products, even new laws. And every year things get worse.

If there's anything computer security professionals have learned about the Internet, it's that security is relative. What's secure today may be insecure tomorrow. Even companies like Microsoft can get

hacked, badly. The way forward is not more products, but better processes. We have to stop looking for the magic preventive technology that will avoid the threats, and embrace processes that will help us manage the risks.

Security and Risk Management

Ask any network administrator how security technologies help, and he'll discuss avoiding the threats. This is the traditional paradigm of computer security, born out of a computer science mentality: figure out what the threats are, and build technologies to avoid them. The conceit is that technologies can somehow "solve" computer security, and the end result is a security program that becomes an expense and a barrier to business.

Security is a not a technology problem, it's a people problem. There is no computer security product that acts as magical security dust, imbuing a network with the property of "secure." It's not the way business works.

Businesses manage risks; network security is just one. More security isn't always better. You could improve the security of a bank by strip-searching everyone who walks through the front door. But if you did this, you would have no business. What all of these businesses are looking for is adequate security at a reasonable cost. It's the same for the Internet—security that allows a company to offer new services, to expand into new markets, and to attract and retain new customers. And the particular computer security solutions they choose depend on who they are and what they are doing.

Protection, Detection, and Response

Real-world security includes prevention, detection, and response. If the prevention mechanisms were perfect, you wouldn't need detection and response. But no prevention mechanism is perfect. This is especially true for computer networks. All software products have security bugs, most

network devices are misconfigured, and users make all sorts of mistakes. Without detection and response, the prevention mechanisms only have limited value. Detection and response are not only more cost effective but also more effective than piling on more prevention. On the Internet, this translates to monitoring.

That's real security. It doesn't matter how the attacker gets in, or what he is doing. If there are enough motion sensors, electric eyes, and pressure plates in your house, you'll catch the burglar regardless of how he got in. If you are monitoring your network carefully enough, you'll catch a hacker regardless of what vulnerability he exploited to gain access. And if you can respond quickly and effectively, you can repel the attacker before he does any damage. Good detection and response can make up for imperfect prevention – No bank ever says: “Our safe is so good, we don't need an alarm system.” Detection and response are how we get security in the real world, and they're the only way we can possibly get security on the Internet. CIOs must invest in network monitoring services if they are to properly manage the risks associated with their network infrastructure.

Monitoring Network Security

Network monitoring implies a series of sensors in and around the network. Every firewall produces a continuous stream of audit messages. So does every router and server. IDSs send messages when they notice something. Every other security product generates alarms in some way.

But these sensors by themselves do not offer security. You have to assume that the attacker is in full possession of the specifications for these sensors, is well aware of their deficiencies, and has tailored his attack accordingly. He may even have passwords that let him masquerade as a legitimate user. Only another human has a chance of detecting some anomalous behavior that gives him away.

The first step is intelligent alert. Network attacks can be subtle, and much depends on context. Software can filter the tens of megabytes of audit information a medium-sized network can generate in a day, but software is too easy for an attacker to fool. Intelligent alert requires people to:

- Analyze what the software finds suspicious;
- Delve deeper into suspicious events, determining what is really going on;
- Separate false alarms from real attacks;
- Understand context.

By itself, an alert is only marginally useful. More important is to know how to respond. This is the second step of good network monitoring. Software can only provide generic information; real understanding requires experts. Finally, the response must be integrated with organizational business needs.

All of this is detection and response as applied to computer networks. Network devices produce megabytes of audit information daily. Automatic search tools sift through those megabytes, looking for telltale signs of attacks. Expert analysts examine those telltales, understanding what they mean and determining how to respond. And the owner of the network—the organization—makes security decisions based on ongoing business concerns.

To make network monitoring work, people are needed every step of the way. Software doesn't think, doesn't question, doesn't adapt. Without people, computer security software is just a static defense. Marry software with experts, and you have a whole different level of security.

Outsourcing Monitoring

The key to a successful detection and response system is vigilance: attacks can happen at any time of the day and any day of the year. While it is possible for companies to build detection and response services for their own networks, it's rarely cost-effective. Staffing for security expertise 24 hours a day and 365 days a year requires five full-time employees; more, if you include supervisors and backup personnel with more specialized skills. Even if an organization could find the budget for all of these people, it would be very difficult to hire them in today's job market. Retaining them would be even harder: Attacks against a single organization don't happen often enough to keep a team of this caliber engaged and interested.

There's a reason you don't have your own fire department, even if you can afford one. When the fire department comes to your house, you want them to have practiced on the rest of the neighborhood.

In the real world, this kind of expertise is always outsourced. It's the only cost-effective way to satisfy the requirements. Aside from the aggregation of expertise, an MSM service has other economies of scale. It can more easily hire and train its personnel, simply because it needs more of them. And it can build an infrastructure to support them. Vigilant monitoring means keeping up to date on new vulnerabilities, new hacker tools, new security products, and new software releases. An MSM service can spread these costs among all of its customers.

An MSM provider also has a much broader view of the Internet. It can learn from attacks against one customer, and use that knowledge to protect all of its customers. And, from its point of view, attacks are frequent. There's a reason you don't have your own fire department, even if you can afford one. When the fire department comes to your house, you want them to have practiced on the rest of the neighborhood. To an MSM company, network attacks are everyday occurrences; as experts, they know exactly how to respond to any given attack, because in all likelihood they have already seen the same attack many times before. Security is important, complex, and distasteful; it is smarter to outsource than to do it yourself.

Monitoring First

Monitoring should be the first step in any network security plan. It's something that a network administrator can do today to provide immediate value. Policy analysis and vulnerability assessments take time, and don't actually improve a network's security until they're acted upon. Installing security products improves security, but only if they are installed correctly and in the right places. Monitoring ensures that security products are providing the type of security they were intended to provide.

Monitoring's best value is when a network is in flux—as all large networks always are—due to internal and external factors. Monitoring provides immediate security in a way that neither doing a vulnerability assessment nor dropping a firewall into a network never can provide. Monitoring provides dynamic security in a way that yet another security product can never provide. And as security products are added into a network—firewalls, IDSs, specialized security devices—monitoring only gets better.

Monitoring is what gives companies a window into their security. Monitoring is the feedback loop that makes all the other network security activities more effective. It's how you determine where to

install security devices, and whether or not they're doing any good. It's how you know if your security devices are configured correctly. It's how you ensure that your security doesn't degrade over time. And it needs to be done first.

Conclusion

The downside of being in a highly connected network is that we are all connected with the best and worst of society. Security products will not "solve" the problems of Internet security, any more than they "solve" the security problems in the real world. The best we can do is to manage the risks: employ technological and procedural mitigation while at the same time allowing businesses to thrive.

Computer security equals vigilance, a day-to-day process. It's been thousands of years, and the world still isn't a safe place. And no matter how fast technology advances, alarms and security services are still state-of-the-art.

The key to effective security is human intervention. Automatic security is necessarily flawed. Smart attackers bypass the security, and new attacks fool products. People are needed to recognize, and respond to, new attacks and new threats. It's a simple matter of regaining a balance of power: human minds are the attackers, so human minds need to be the defenders as well.

On the day you're attacked, you want the best possible defense. MSM combines people, processes, and products to create a security environment for the chaos of modern business networks. The reality of today's Internet makes MSM the most cost-effective way to provide resilient security.

###

For more information, please contact Counterpane's Managed Security Specialists.

Call Us: 888-710-8175

Email Us: info@counterpane.com

Visit Our Website: www.counterpane.com

