Bruce Schneier

CTO, Counterpane Internet Security

April 2002

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Counterpane™ Internet Security

Counterpane and Managed Security Monitoring

Talk Description:

Computer and network security has been viewed as an engineering problem, and companies have tried to solve it through the application of technologies. This approach is failing; even though technologies continue to improve, the security of the Internet continues to decline. The real problem is not one of technology, but of process. Network security is no different from real-world security. The correct paradigm is “risk management.” Strong countermeasures combine protection, detection, and response. The way to build resilient security is with vigilant, adaptive, relentless defense by experts (people, not products). There are no magic preventive countermeasures against crime in the real world, yet we are all reasonably safe, nevertheless. Counterpane Internet Security has brought this thinking to computer networks, by offering real-time detection and response using advanced correlation technology and expert human security analysts.

This presentation is available on-line at http://www.counterpane.com/presentation2.pdf

About the Author:

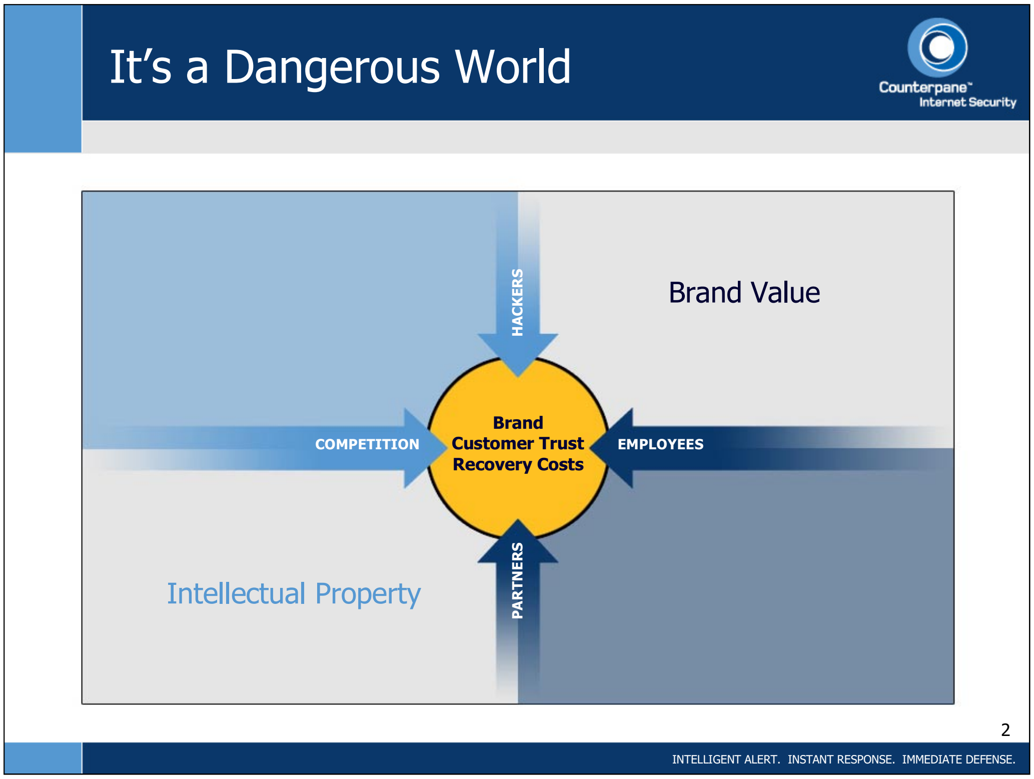
Internationally renowned security technologist and author Bruce Schneier is the Founder and the Chief Technical Officer of Counterpane Internet Security, Inc., the world leader in Managed Security Monitoring. Counterpane provides security monitoring services to Fortune 2000 companies world-wide. He is the author of six books on security and cryptography, including the security best seller, "Secrets & Lies: Digital Security in a Networked World." His first book, "Applied Cryptography," has sold over 150,000 copies world-wide, and is the definitive work in the field. Schneier designed the Blowfish and Twofish encryption algorithms, and writes the influential "Crypto-Gram" monthly newsletter. He is a frequent lecturer on computer security and cryptography.

Bruce Schneier’s biography is available on-line at http://www.counterpane.com/schneier.html

About Counterpane Internet Security, Inc.

Counterpane Internet Security, Inc. is the innovator and acknowledged leader in providing Managed Security Monitoring (MSM) services. MSM combines people and technology to safeguard businesses. Working from a network of technically sophisticated Secure Operations Centers (SOCs) and using progressive analysis tools, Counterpane has built the most advanced analysis, correlation, detection, and diagnosis technology, comprising of a Sentry monitoring probe on the customer's network and the Socrates knowledge base inside the SOCs. Using this technology, Counterpane's expert Security Analysts are able to detect security incidents-both external intrusions and insider attacks-in real time, and tailor immediate, effective responses for its customers. It has partnered with leading security companies, consulting organizations, and VARs to deliver MSM services world-wide. Counterpane is headquartered in Sunnyvale, CA, and has two operational SOCs: one in Mountain View, CA, and the other in Chantilly, VA.

More information about Counterpane is available on-line at http://www.counterpane.com/



It's a Dangerous World

Counterpane™ Internet Security

Brand Value

HACKERS

COMPETITION

Brand
Customer Trust
Recovery Costs

EMPLOYEES

PARTNERS

Intellectual Property

2

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

CSI's Computer Crime and Security Survey

For the past six years, the Computer Security Institute has conducted an annual computer crime survey. In 2001, 64% of respondents reported "unauthorized use of computer systems" in the last year. 25% said that they had no such unauthorized uses, and 11% said that they didn't know. The number of incidents was all over the map, and the number of insider versus outsider incidents was roughly equal. 70% of respondents reported their Internet connection as a frequent point of attack (this has been steadily rising over the six years), 18% reported remote dial-in as a frequent point of attack (this has been declining), and 31% reported internal systems as a frequent point of attack (also declining).

The types of attack range from telecommunications fraud to laptop theft to sabotage. 40% experienced a system penetration, 36% a denial-of-service attack. 26% reported theft of proprietary information, and 12% financial fraud. 18% reported sabotage. 23% had their Web sites hacked (another 27% didn't know), and over half of those had their Web sites hacked ten or more times (90% of the Web site hacks resulted in vandalism, and 13% included theft of transaction information).

What's interesting is that all of these attacks occurred despite the wide deployment of security technologies: 95% have firewalls, 61% an IDS, 90% access control of some sort, 42% digital IDs, etc.

The financial consequences are staggering. Only 196 respondents would quantify their losses, and those totaled $378 million. From under 200 companies! In one year! This is a big deal.

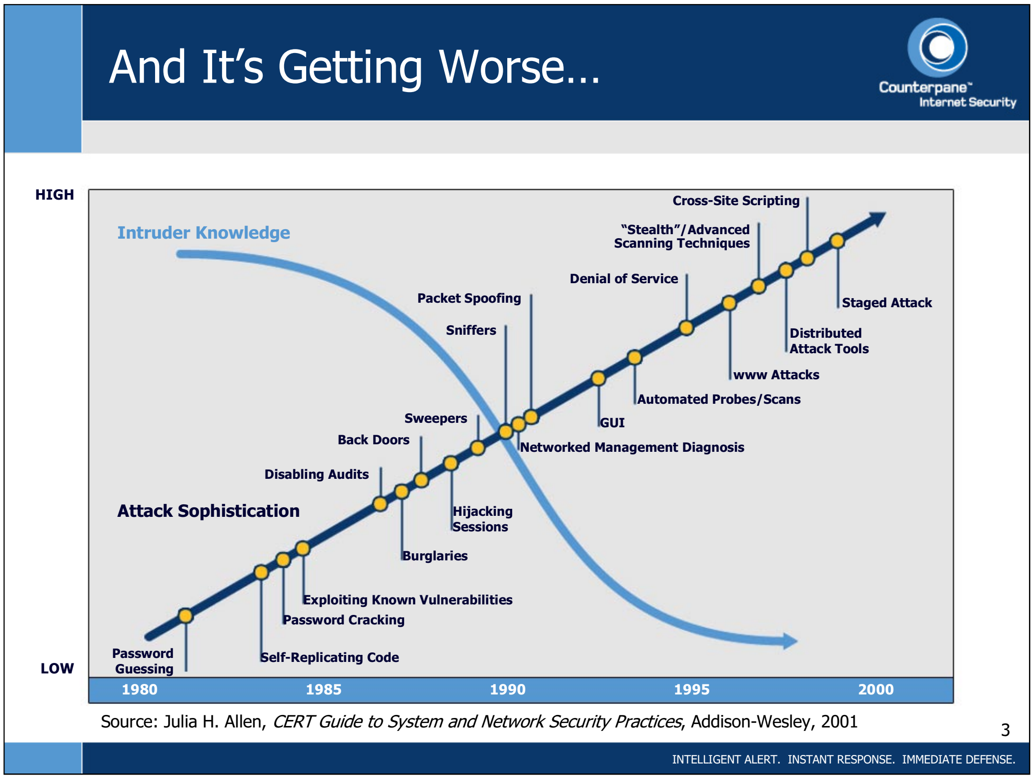
To get a copy of this survey, visit http://www.gocsi.com/prelea_000321.htm

The Honeynet Project

The Honeynet Project measures actual computer attacks on the Internet. According to their most recent results, a random computer on the Internet is scanned dozens of times a day. The life expectancy of a default installation of Red Hat 6.2 server, or the time before someone successfully hacks it, is less than 72 hours. A common home user setup, with Windows 98 and file sharing enabled, was hacked five times in four days. Systems are subjected to NetBIOS scans an average of 17 times a day. And the fastest time for a server being hacked: 15 minutes after plugging it into the network.

My essay on the Honeynet Project: http://www.counterpane.com/crypto-gram-0106.html#1

The Honeynet Project homepage: http://project.honeynet.org/



And It's Getting Worse…

Source: Julia H. Allen, *CERT Guide to System and Network Security Practices*, Addison-Wesley, 2001

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

The Importance of Security

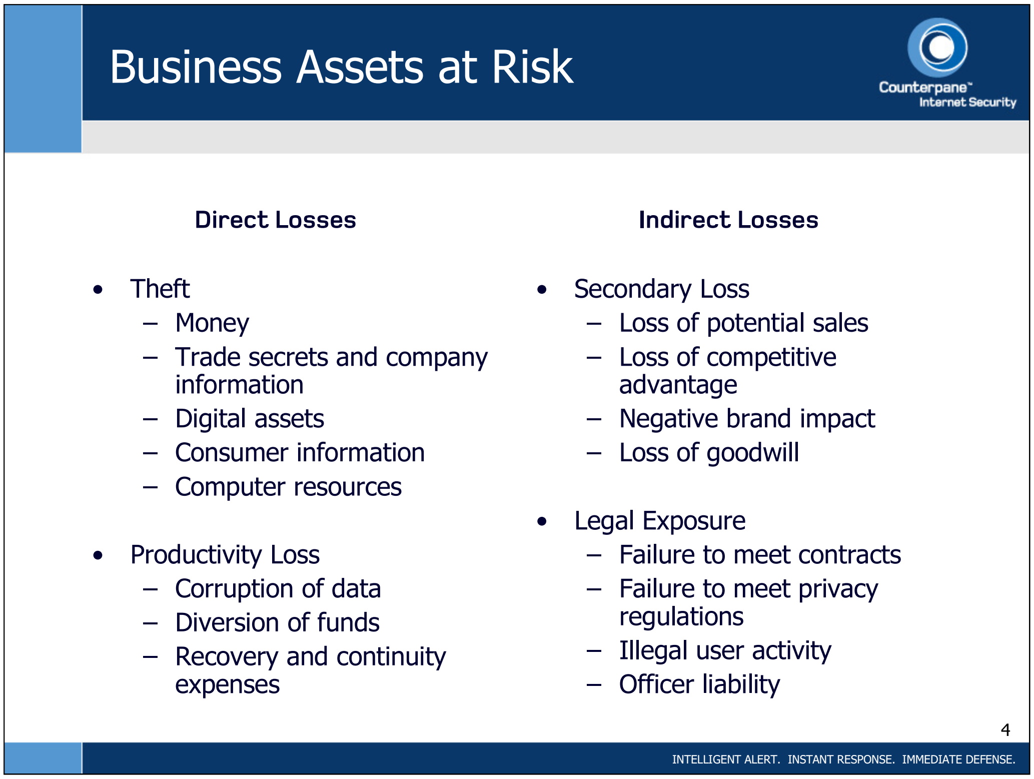
When I began working in computer security, the only interest was from the military and a few scattered privacy advocates. The Internet has changed all that. The promise of the Internet is to be a mirror of society. Everything we do in the real world, we want to do on the Internet: conduct private conversations, keep personal papers, sign letters and contracts, speak anonymously, rely on the integrity of information, gamble, vote, publish digital documents. All of these things require 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. Everyone talks about the direct risks: theft of trade secrets, customer information, money. People also talk about the productivity losses due to computer security problems. What's the loss to a company if its e-mail goes down for two days? Or if ten people have to scramble to clean up after a particularly nasty intrusion? 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. Regardless of how the million-credit-card-number theft at Egghead.com turned out, some percentage of customers decided to shop elsewhere. When CD Universe suffered a credit card theft in early 2000, it cost them dearly in their war for market share against Amazon.com and CDNow. In the aftermath of the Microsoft attack in October 2000, the company spent much more money and effort containing the public relations problem than fixing the security problem. The public perception that their source code was untainted was much more important than any effects of the actual attack.

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. We have not yet seen shareholder lawsuits against companies that failed to adequately secure their networks and suffered the consequences, but they're coming. Can company officers be held personally liable if they fail to provide for network security? The courts will be deciding this question in the next few years.

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. There is no alternative. This, more than anything else, is why computer security is so important.



Business Assets at Risk

Counterpane™ Internet Security

Direct Losses

- Theft
  - Money
  - Trade secrets and company information
  - Digital assets
  - Consumer information
  - Computer resources
- Productivity Loss
  - Corruption of data
  - Diversion of funds
  - Recovery and continuity expenses

Indirect Losses

- Secondary Loss
  - Loss of potential sales
  - Loss of competitive advantage
  - Negative brand impact
  - Loss of goodwill
- Legal Exposure
  - Failure to meet contracts
  - Failure to meet privacy regulations
  - Illegal user activity
  - Officer liability

4

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Security and Risk Management

Ask any network administrator what he needs security for, and he can describe the threats: Web site defacements, corruption and loss of data due to network penetrations, denial-of-service attacks, viruses and Trojans. The list seems endless, and an endless series of news stories proves that the threats are real.

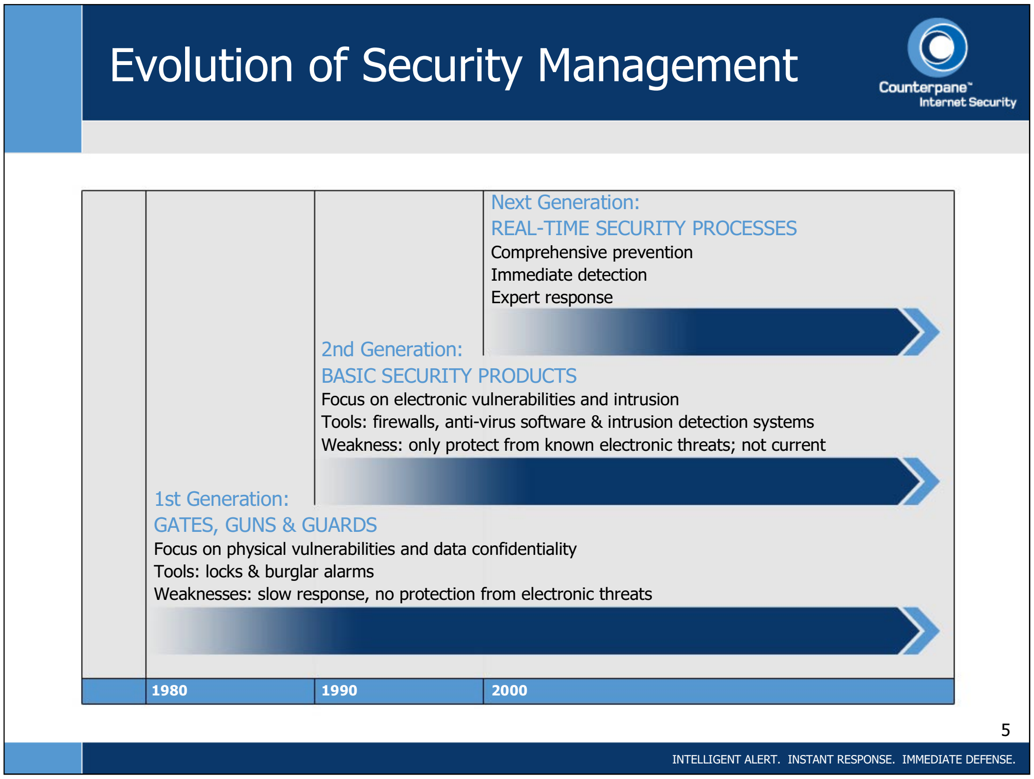
Ask that same network administrator how security technologies help, and he'll discuss avoiding the threats. This is the traditional paradigm of computer security, born out of a computer science mentality: figure out what the threats are, and build technologies to avoid them. The conceit is that technologies can somehow "solve" computer security, and the end result is a security program that becomes an expense and a barrier to business. How many times has a security officer said: "You can't do that; it would be insecure"?

This paradigm is wrong. Security is a people problem, not a technology problem. There is no computer security product-or even suite of products-that acts as magical security dust, imbuing a network with the property of "secure." It can't be done. And it's not the way business works.

Businesses manage risks. They manage all sorts of risks; network security is just another one. And there are many different ways to manage risks. The ones you choose in a particular situation depend on the details of that situation. And failures happen regularly; many businesses manage their risks improperly, pay for their mistakes, and then soldier on. Businesses are remarkably resilient.

To take a concrete example, consider a physical store and the risk of shoplifting. Most grocery stores accept the risk as a cost of doing business. Clothing stores might put tags on all their garments and sensors at the doorways; they mitigate the risk with a technology. A jewelry store might mitigate the risk through procedures: all merchandise stays locked up, customers are not allowed to handle anything unattended, etc. And that same jewelry store will carry theft insurance, another risk management tool.

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. Studies show that most shoplifting at department stores occurs in dressing rooms. You could improve security by removing the dressing rooms, but the losses in sales would more than make up for the decrease in shoplifting. What all of these businesses are looking for is adequate security at a reasonable cost. This is what we need on the Internet as well-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.



Evolution of Security Management

Next Generation:
REAL-TIME SECURITY PROCESSES
Comprehensive prevention
Immediate detection
Expert response

2nd Generation:
BASIC SECURITY PRODUCTS
Focus on electronic vulnerabilities and intrusion
Tools: firewalls, anti-virus software & intrusion detection systems
Weakness: only protect from known electronic threats; not current

1st Generation:
GATES, GUNS & GUARDS
Focus on physical vulnerabilities and data confidentiality
Tools: locks & burglar alarms
Weaknesses: slow response, no protection from electronic threats

5

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

The Business Case for Security Monitoring

Five years ago a firewall was all you needed for security on the Internet. Back then, no one had ever heard of denial-of-service attacks shutting down Web servers, let alone common gateway interface scripting flaws and the latest vulnerabilities in Microsoft Outlook Express. But in the wake of recent years came intrusion detection systems, public-key infrastructure, smart cards and biometrics. New networking services, wireless devices and the latest products regularly turn network security upside down. It’s no wonder CIOs can’t keep up.

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.

It’s not about the technology.

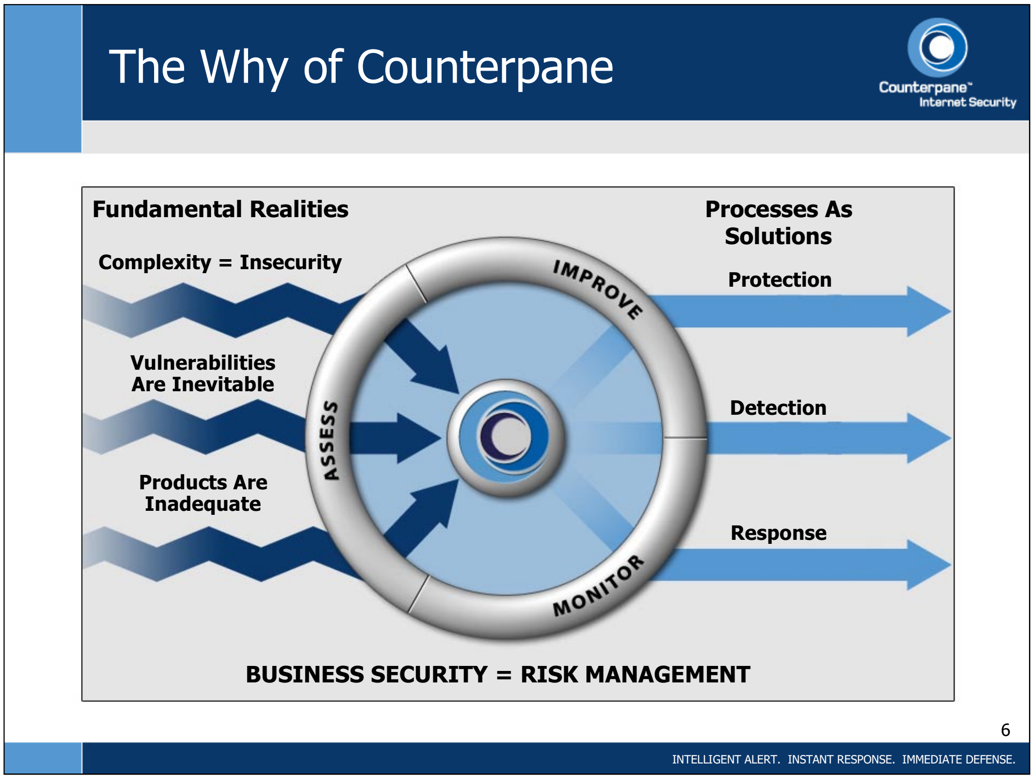
Network security is an arms race, where the attackers have all the advantages. First, potential intruders are in what military strategists call “the position of the interior”: the defender has to defend against every possible attack, while the attacker only has to find one weakness. Second, the immense complexity of modern networks makes them impossible to properly secure. And third, skilled attackers can encapsulate their attacks in automatic programs, allowing people with no skill to use them.

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 let us manage the risks. And that doesn’t mean more prevention; it means detection and response.

On the Internet this translates to constant monitoring of your network. In October 2000, Microsoft discovered that an attacker penetrated its corporate network weeks earlier, doing untold damage. Administrators discovered this breach when they noticed 20 new accounts being created on a server. Then they went back through their audit records and pieced together how the attacker got in and what he did. If someone had been monitoring those audit records—from the firewalls, servers and routers—in real time, the attacker could have been detected and repelled at the point of entry.

Monitoring also means vigilance; attacks come from all over and at all hours. It means that experts need to continuously monitor with the tools and expertise at hand to figure out what is happening. Throwing an intrusion detection system onto a network and handing a system administrator a pager isn’t monitoring, any more than giving a bucket to the guy at the other end of a fire alarm replaces a fire department.

Prevention systems are never perfect. No bank ever says: “Our safe is so good, we don’t need an alarm system.” No museum ever says: “Our door and window locks are so good, we don’t need night watchmen.” Detection and response are how we get security in the real world, and it’s the only way we can possibly get security on the Internet. CIOs must invest in monitoring services if they are to maintain security in a networked world.



The Why of Counterpane

Counterpane™ Internet Security

Fundamental Realities

Complexity = Insecurity

Vulnerabilities Are Inevitable

Products Are Inadequate

Processes As Solutions

Protection

Detection

Response

BUSINESS SECURITY = RISK MANAGEMENT

6

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

What is Managed Security Monitoring?

Counterpane's business is Managed Security Monitoring (MSM). In plain English, that means we watch over your network. And the watching is done by real people: expert security analysts who monitor your systems 24 hours a day. We take your existing security devices and software, and leverage their potential, with a powerful combination of unmatched technology and proven expertise. The result? Your network is protected from today's growing risks by a real- time, full-time security solution.

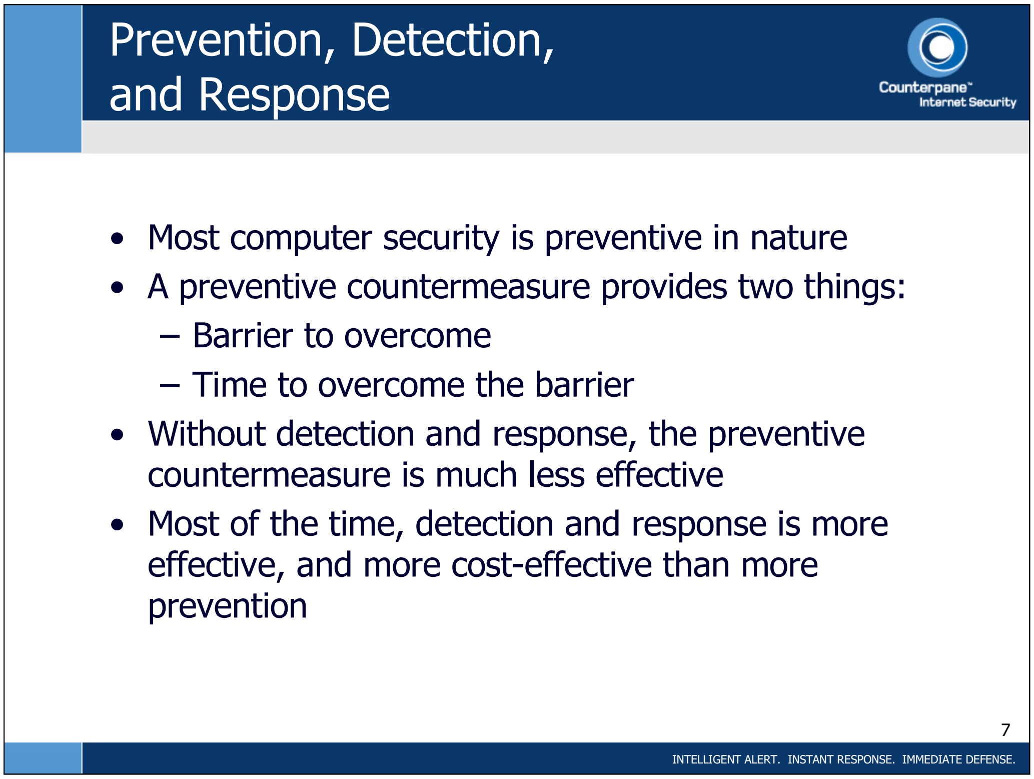
Counterpane's value is our unique combination of people and technology. Our Security Analysts are highly trained and singularly qualified experts who understand the need to protect your business assets. The data our Security Analysts receive starts with the Sentry, a monitoring device installed on your network. The Sentry collects data from the devices on your network, then sorts, analyzes, and correlates it using over 20,000 security filters and our own Analysis Engine, and sends the resulting alerts to one of our Secure Operations Centers. There Socrates, an expert software system developed by Counterpane, looks for suspicious patterns in the data, correlates your data with that of other customers, and matches symptoms with diagnoses, using our up-to-the- minute database of information on real-world security threats. The moment a threat to your network surfaces, Socrates alerts our analysts, who apply human judgment, intelligence, and flexibility to the problem. If the attack is not a false alarm, our analysts contact you immediately with detailed information about the threat and expert recommendations for corrective action. Our breadth of experience proves that at the moment you're attacked, what matters most is the caliber of people defending you.

Bruce Schneier’s Philosophy of Security and Monitoring:

http://www.counterpane.com/msm.html

Vulnerabilities, Patches, and the “Window of Exposure”:

http://www.counterpane.com/window.pdf



Prevention, Detection, and Response

Counterpane™ Internet Security

- Most computer security is preventive in nature
- A preventive countermeasure provides two things:
  - Barrier to overcome
  - Time to overcome the barrier
- Without detection and response, the preventive countermeasure is much less effective
- Most of the time, detection and response is more effective, and more cost-effective than more prevention

7

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Prevention, Detection, and Response

Most computer security is sold as a prophylactic: encryption prevents eavesdropping, firewalls prevent unauthorized network access, PKI prevents impersonation. To the world at large, this is a strange marketing strategy. A door lock is never sold with the slogan: “This lock prevents burglaries.” No one ever asks to purchase “a device that will prevent murder.” But computer security products are sold that way all the time. Companies regularly try to buy “\”a device that prevents hacking.” This is no more possible than an anti-murder device.

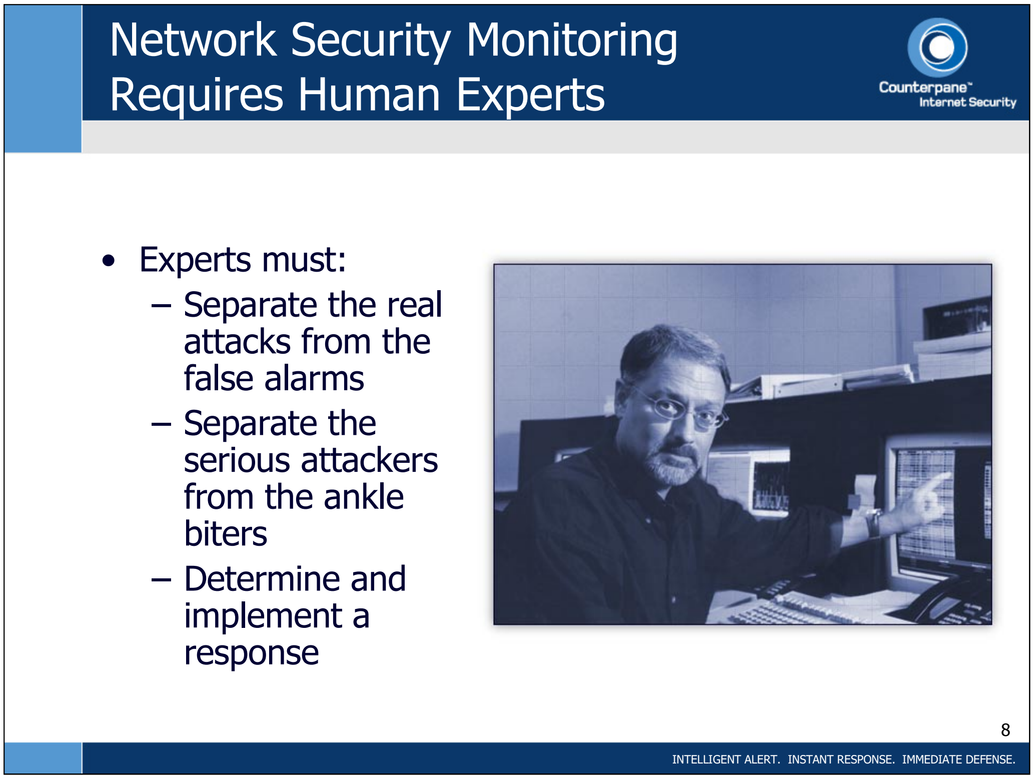
When you buy a safe, it comes with a rating. 30TL-30 minutes, tools. 60TRTL-60 minutes, torch and tools. What this means is that a professional safecracker, with safecracking tools and an oxyacetylene torch, will break open the safe in an hour. If an alarm doesn’t sound and guards don’t come running within that hour, the safe is worthless. The safe buys you time; you have to spend it wisely.

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. They’re fragile. And 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. When a forensics team investigates an intrusion, they comb through the audit logs of the network’s routers, servers, firewalls, etc. Using those logs, they piece together the attacker’s actions: how he got in, what he did, what he stole. If someone can monitor those audit logs in real time, he could figure out what the attacker IS DOING. And if he can respond fast enough, he can repel the attacker before he does real damage.

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.

And prevention systems are never perfect. No bank ever says: “Our safe is so good, we don’t need an alarm system.” No museum ever says: “Our door and window locks are so good, we don’t need night watchmen.” 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.



Network Security Monitoring Requires Human Experts

- Experts must:
  - Separate the real attacks from the false alarms
  - Separate the serious attackers from the ankle biters
  - Determine and implement a response

8

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Monitoring Network Security

Network monitoring implies several things. It implies a series of sensors in and around the network. Luckily, these are already in place. 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.

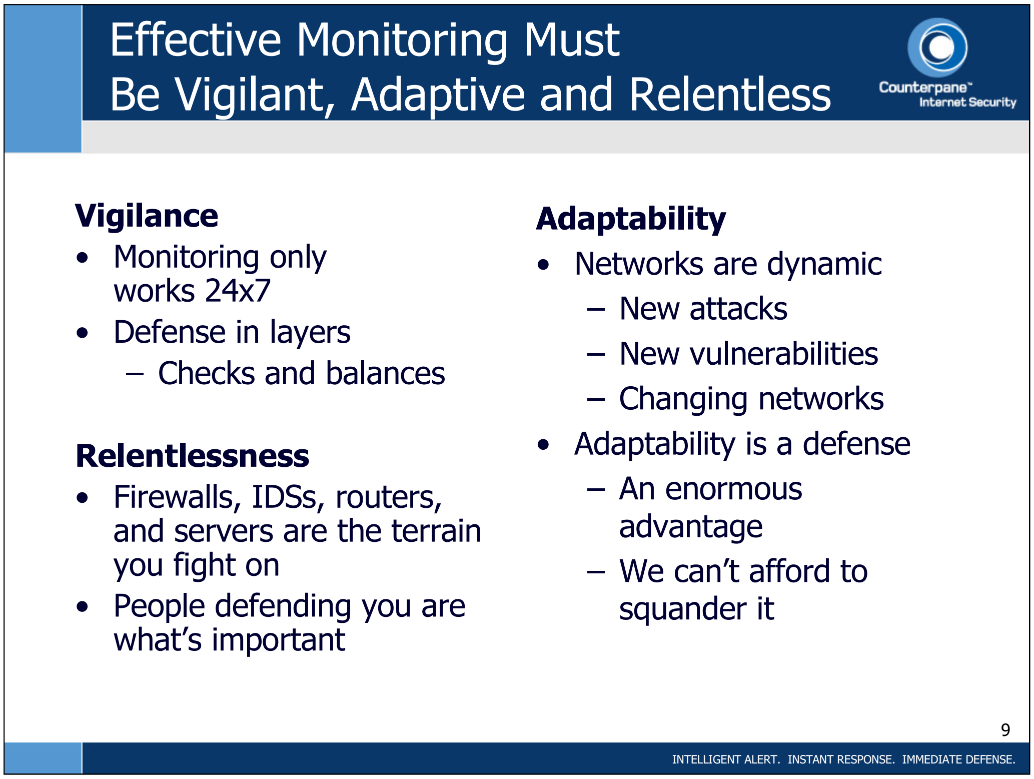
The first step is intelligent alert. Network attacks can be much more subtle than a broken window. Much depends on context. Software can filter the tens of megabytes of audit information a medium-sized network can generate in a day, but software is too easy for an attacker to fool. Intelligent alert requires people. People to analyze what the software finds suspicious. People to delve deeper into suspicious events, determining what is really going on. People to separate false alarms from real attacks. People who 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. Every attack has a response. It could be as simple as shutting off a particular IP address to repel an attacker. It could be as drastic as taking a corporate network off the Internet. Again, people are the key. Software can only provide generic information; real understanding requires experts.

And finally, the response must be integrated with the business needs of the organization. Security engineers only see half the information. They understand attacks and their security significance, but they don’t understand the business ramifications. A large e-business might keep its Web site up and running even if it is being attacked; preventing the loss of revenue may be more important than the site’s immediate security. On the other hand, a law firm may have the exact opposite response; the sanctity of its customers’ data might be more important than having its Web site available.

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 is just too easy to fool. 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.



Effective Monitoring Must Be Vigilant, Adaptive and Relentless

Vigilance

- Monitoring only works 24x7
- Defense in layers
  - Checks and balances

Relentlessness

- Firewalls, IDSs, routers, and servers are the terrain you fight on
- People defending you are what's important

Adaptability

- Networks are dynamic
  - New attacks
  - New vulnerabilities
  - Changing networks
- Adaptability is a defense
  - An enormous advantage
  - We can't afford to squander it

9

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Military History and Network Security

In warfare, the defender's military advantage comes from two broad strengths: the ability to quickly react to an attack, and the ability to control the terrain.

The first strength is probably the most important; a defender can more quickly shift forces to resupply existing forces, shore up defense where it is needed, and counterattack. Here we see the same themes from elsewhere in this booklet: how detection and response are critical, the need for trained experts to quickly analyze and react to attacks, and the importance of vigilance. I've built Counterpane's MSM service around these very principles, precisely because it can dramatically shift the balance from attacker to defender.

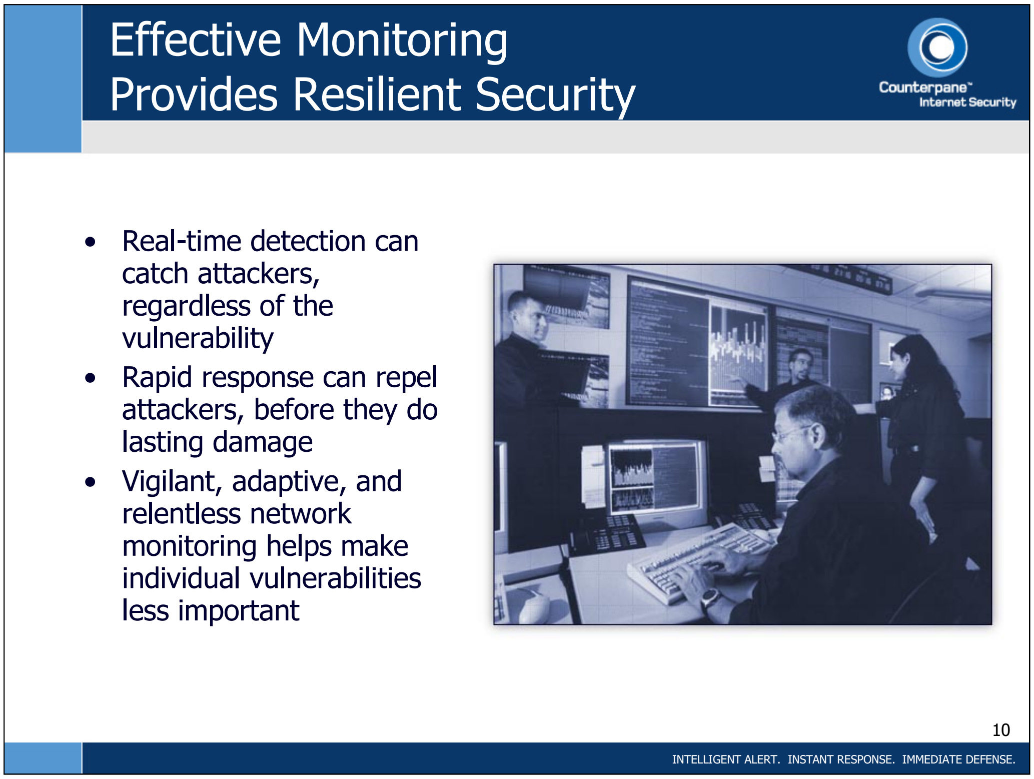
The defender's second strength also gives him a strong advantage. He has better knowledge of the terrain: where the good hiding places are, where the mountain passes are, how to sneak through the caves. He can modify the terrain: building castles or SAM batteries, digging trenches or tunnels, erecting guard towers or pillboxes. And he can choose the terrain on which to stand and defend: behind the stone wall, atop the hill, on the far side of the bridge, in the dense jungle. The defender can use terrain to his maximum advantage; the attacker is stuck with whatever terrain he is forced to traverse.

On the Internet, this second advantage is one that network defenders seldom take advantage of: knowledge of the network. The network administrator knows exactly how his network is built (or, at least, he should), what it is supposed to do, and how it is supposed to do it. Any attacker except a knowledgeable insider has no choice but to stumble around, trying this and that, trying to figure out what's where and who's connected to whom. And it's about time we exploited this advantage.

Think about burglar alarms. The reason they work is that the attacker doesn't know they're there. He might successfully bypass a door lock, or sneak in through a second-story window, but he doesn't know that there is a pressure plate under this particular rug, or an electric eye across this particular doorway. MacGyver-like antics aside, any burglar wandering through a building wired with alarms is guaranteed to trip something sooner or later.

Traditional computer security has been static: install a firewall, configure a PKI, add access-control measures, and you're done. Real security is dynamic. The defense has to be continuously vigilant, always ready for the attack. The defense has to be able to detect attacks quickly, before serious damage is done. And the defense has to be able to respond to attacks effectively, repelling the attacker and restoring order.

This kind of defense is possible in computer networks. It starts with effective sensors: firewalls, well-audited servers and routers, intrusion-detection products, network burglar alarms. But it also includes people: trained security experts that can quickly separate the false alarms from the real attacks, and who know how to respond. It includes an MSM service. This is security through process. This is security that recognizes that human intelligence is vital for a strong defense, and that automatic software programs just don't cut it.



Effective Monitoring Provides Resilient Security

- Real-time detection can catch attackers, regardless of the vulnerability
- Rapid response can repel attackers, before they do lasting damage
- Vigilant, adaptive, and relentless network monitoring helps make individual vulnerabilities less important

10

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Monitoring and Resilient Security

During the course of the year 2000, several groups of Eastern European hackers broke into at least 40 companies' Web sites, stole credit card numbers, and in some cases tried to extort money from their victims. The network vulnerabilities exploited by these criminals were known, and patches that closed them were available-but none of the companies had installed them. In January 2001, the Ramen worm targeted known vulnerabilities in several versions of Red Hat Linux. None of the thousands of infected systems had their patches up to date. In October 2000, Microsoft was molested by unknown hackers who wandered unchallenged through their network, accessing intellectual property, for weeks or months. According to reports, the attackers would not have been able to break in if Microsoft's patches had been up to date. The series of high-profile credit card thefts in January 2000, including the CD Universe incident, were also the result of uninstalled patches. A patch issued eighteen months previously would have protected these companies.

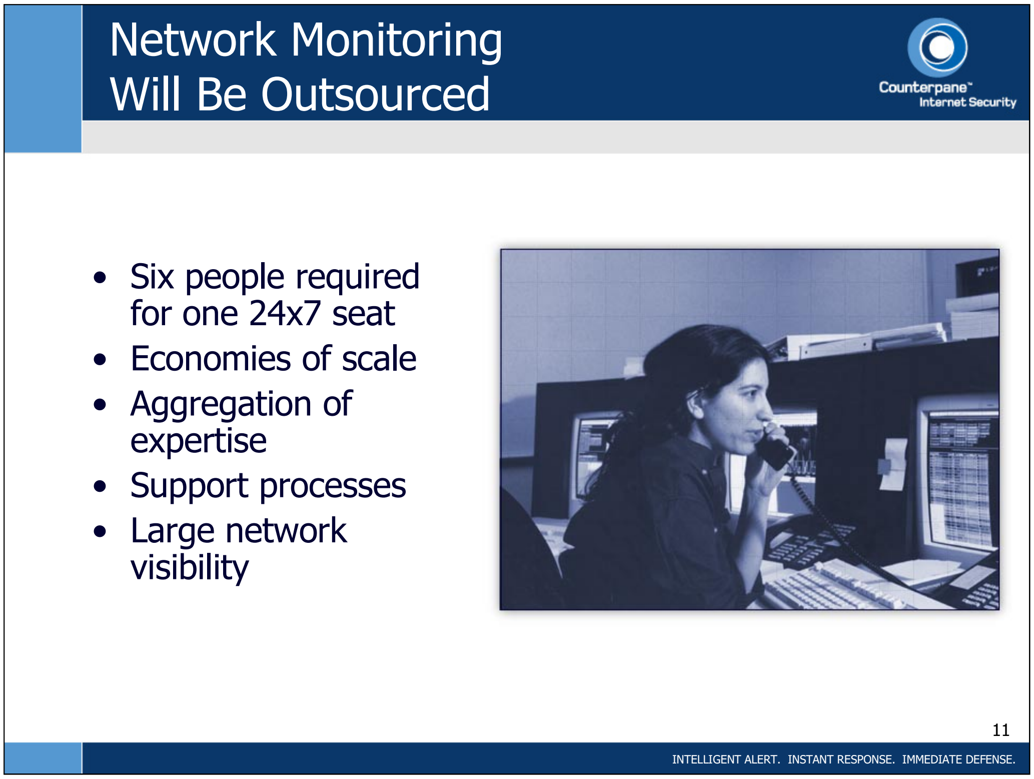
What's going on here? Isn't anyone installing security patches anymore? Doesn't anyone care?

What's going on is that there are just too damn many patches. It's simply impossible to keep up. I get weekly summaries of new vulnerabilities and patches. One alert service listed 19 new patches in a variety of products in the first week of March 2001. That was an average week. Some of the listings affected my network, and many of them did not. Microsoft Outlook alone had over a dozen security patches in the year 2000. I don't know how the average user can possibly install them all; he'd never get anything else done.

Security based on patches is inherently fragile. Any large network is going to have hundreds of vulnerabilities. If there's a vulnerability in your system, you can be attacked successfully and there's nothing you can do about it. Even if you manage to install every patch you know about, what about the vulnerabilities that haven't been patched yet? (That same alert service listed 10 new vulnerabilities for which there are no patches.) Or the vulnerabilities discovered but not reported yet? Or the ones still undiscovered?

Good security is resilient. It's resilient to user errors. It's resilient to network changes. And it's resilient to administrators not installing every patch. Managed Security Monitoring is an important part of that resilience. Monitoring makes a network less dependent on keeping patches up to date; it's a process that provides security even in the face of ever-present vulnerabilities, uninstalled patches, and imperfect products.

In a perfect world, systems would rarely need security patches. The few patches they did need would automatically download, be easy to install, and always work. But we don't live in a perfect world. Network administrators are busy people, and networks are constantly changing. Vigilant monitoring is by no means a panacea, but it is a much more realistic way of providing resilient security.



Network Monitoring Will Be Outsourced

- Six people required for one 24x7 seat
- Economies of scale
- Aggregation of expertise
- Support processes
- Large network visibility

11

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Outsourced Managed Security 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 six 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.

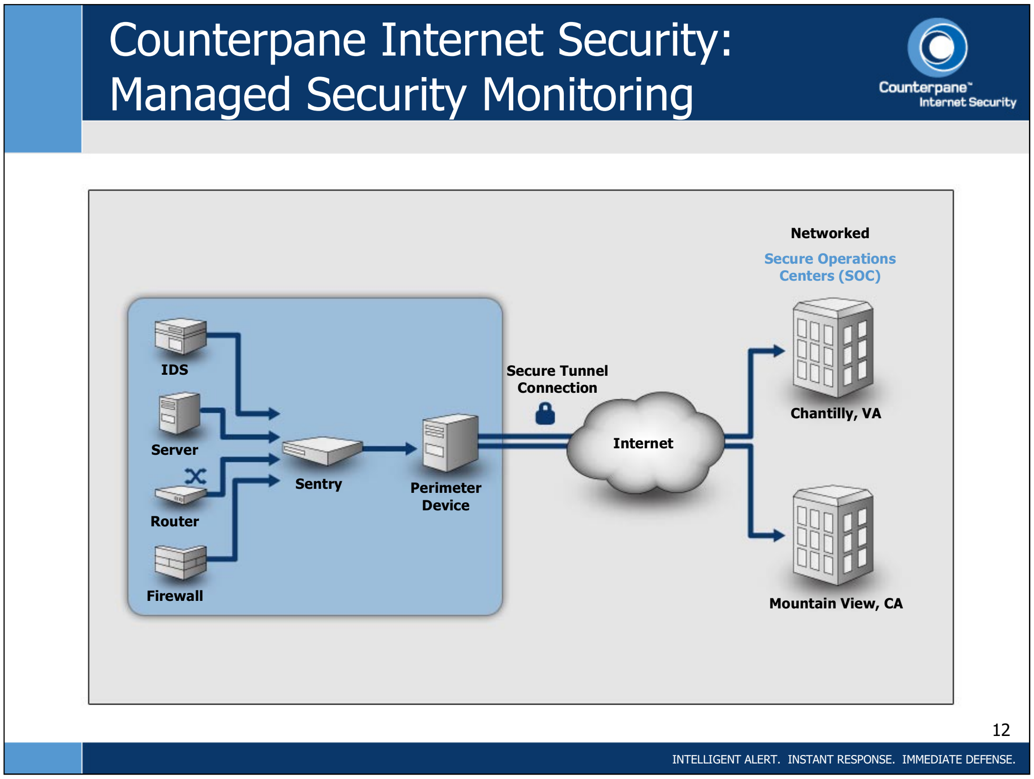
Retaining them would be even harder. Security monitoring is inherently bursty: six weeks of boredom followed by eight hours of panic, then seven weeks of boredom followed by six hours of panic. Attacks against a single organization don't happen often enough to keep a team of this caliber engaged and interested.

In the real world, this kind of expertise is always outsourced. It's the only cost-effective way to satisfy the requirements. I may only need a doctor twice in the coming year, but when I need one I may need him immediately. I may need specialists. Out of a hundred possible specialties, I may need two of them-and I have no idea beforehand which ones. I would never consider hiring a team of doctors to wait around until I happen to get sick. I outsource my medical needs to my clinic, my emergency room, my hospital. Similarly, a network needs to outsource its security monitoring to an MSM service.

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 it to have practiced on the rest of the neighborhood. To an MSM company, network attacks are everyday occurrences; its experts know exactly how to respond to any given attack, because in all likelihood they have already seen the same attack many times before.

In the real world, security is always outsourced. Every building hires another company to put guards in its lobby. Every bank hires another company to drive its money around town. Security is important, complex, and distasteful; it is smarter to outsource than to do it yourself.



Counterpane Internet Security: Managed Security Monitoring

12

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

How Does Counterpane Work?

At Counterpane, we believe that while all security products provide some level of protection, no set of products is infallible. Real security is achieved only when all network products, security and otherwise, work together. Real security is a combination of protection, detection, and response. We augment your network's protective countermeasures through Managed Security Monitoring (MSM).

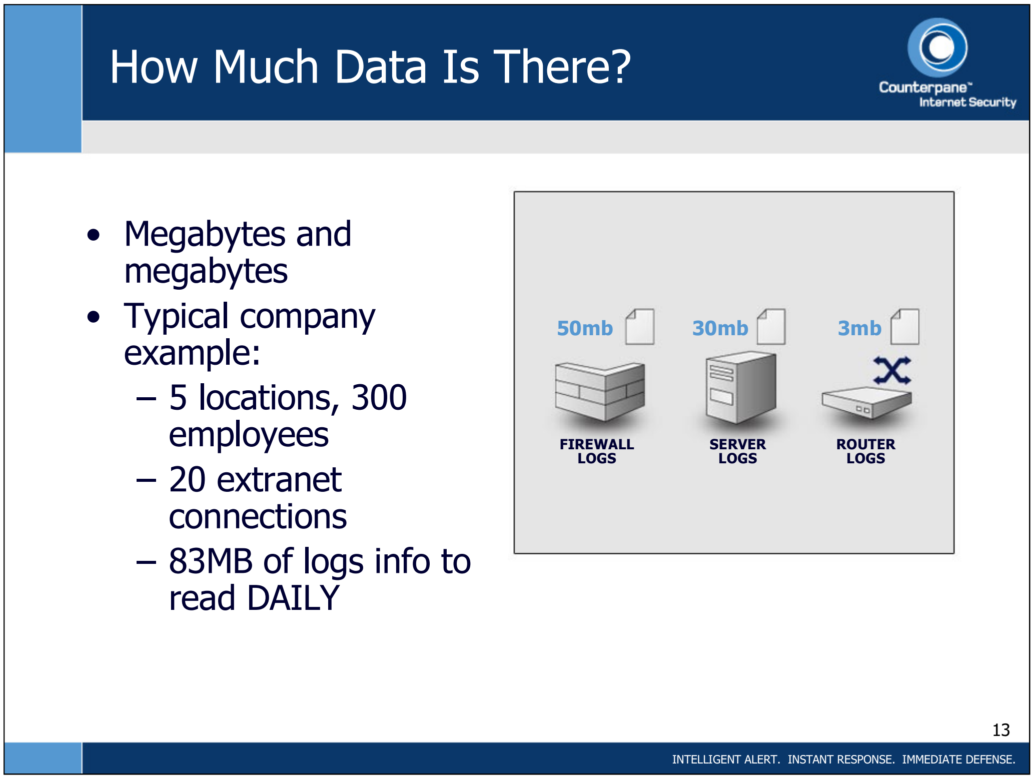
Counterpane's excellence is a combination of our people and our technology. Our security analysts are singularly qualified to evaluate security events and respond to attacks. And our technology provides unmatched data analysis and correlation. Working together, the combination can't be beat.

Security Analysts: Trained security analysts are at the core of Counterpane's service. Our analysts have a breadth of knowledge and skill cultivated by extensive training in network security and incident handling, and invaluable experience on the job. They respond to and learn from security attacks every day. Armed with this knowledge and perspective, and our sophisticated analysis and response software, our analysts are able to provide instant response: expert advice and coaching to help you repel the attacker and safeguard your network.

Sentry: The Sentry is a custom monitoring device, designed and built by Counterpane, and installed on your network. It is capable of processing millions of messages per day: input from all the devices on your network, including those that see internal threats. The Sentry filters the data it collects using an adaptive and proprietary set of rules, correlates that data with data from other devices and previous data, and sends the results via an encrypted tunnel to one of our Secure Operations Centers.

Socrates: Socrates is our proprietary software system that receives messages from Sentries on your network about suspected intrusions. These messages are turned into "tickets" within Socrates, and are correlated with information on the real- world threat environment, information about similar threats at other Counterpane customers, information about your network's normal operation, and response and escalation information. Socrates categorizes and prioritizes the tickets, weeds out false positives, stores the data for future audit, and presents information about critical tickets to our analysts -- allowing them to respond instantly.

Secure Operations Center (SOC): Our SOCs are the physical locations where Counterpane's analysts work, continually monitoring your networks. They are where the Socrates system is housed, and where data from the Sentries is received. The SOCs are physically hardened facilities, protected by access tokens, biometric access devices, and constant audio and video surveillance. To protect the integrity of your network, the SOCs are redundant: each constantly monitors the other and each can sever the other's connectivity and assume the other's workload in the event of a physical attack or system failure.



How Much Data Is There?

- Megabytes and megabytes
- Typical company example:
  - 5 locations, 300 employees
  - 20 extranet connections
  - 83MB of logs info to read DAILY

Counterpane™
Internet Security
50mb
30mb
3mb
FIREWALL LOGS
SERVER LOGS
ROUTER LOGS

13

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Counterpane Detects

Detection and correlation occurs automatically within the Sentry and Socrates, but the real work starts after that. Based on events occurring on the customer's network, Socrates presents the analyst with a "ticket" and all information it thinks could be relevant. Interesting security events don't fall neatly within a single alert, and expertise is required to separate the real attacks from the false alarms. Counterpane's analysts are experienced in figuring out what is really happening in a customer network, and determining what its ramifications are. Resilient detection requires experts, and Counterpane's analysts get more experienced every day.

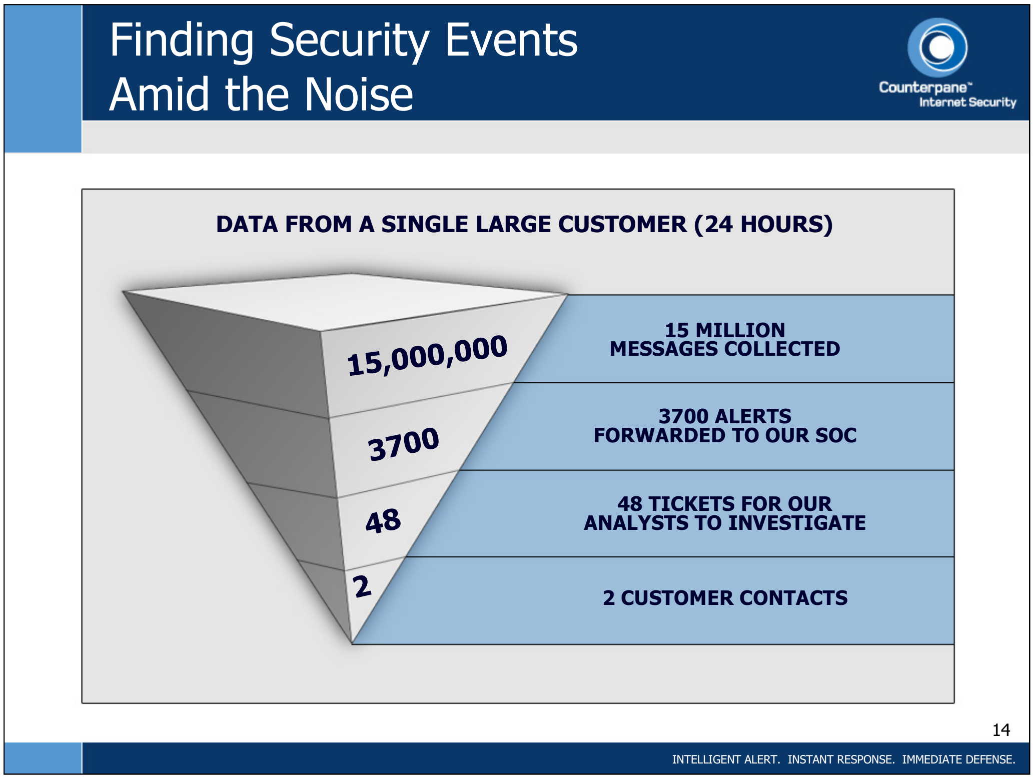
Some attacks require escalation. When an analyst detects something that he has never seen before, and can't dismiss as a false alarm, he has the option of escalating the ticket to an expert in the particular brand of firewall, IDS, operating system, applications software, etc. The analyst also has the ability to place the customer under heightened alert, until he is sure the danger has passed. This flexibility and deep expertise allows us to catch attacks that other monitoring companies miss.

Human expertise is also critical in detecting new attacks that have not yet been blocked by firewalls and IDSs, or insider attacks that can bypass these security devices. The Sentry collects new and unknown audit messages into what we call the "residue." After performing automatic analysis of the residue, the results are presented to analysts for even further analysis. This two-tiered residue analysis process regularly yields surprising and interesting results: insider attacks, new hacker tools, network insecurities.

Counterpane's MSM is not merely reactive; we believe that effective monitoring needs to be proactive as well. By monitoring hacker Web sites, newsgroups, and chat areas, we discover things that monitoring alone would never learn. We find new hacking tools before they're used against our customers, hear about planned attacks against our customers, and become familiar with attack tactics. Sometimes we even learn about successful attacks against parts of our customers' networks that we're not even monitoring.

24x7 Monitoring

Counterpane's systems are designed so that any customer event can be handled by any analyst. This is critical, since attacks can happen any hour of the day and any day of the year, and we cannot guarantee that a particular analyst will be on duty, and not otherwise engaged, at any time. Additionally, the analyst with the best expertise to deal with a given problem can change over time. Because some security incidents span multiple analyst shifts, regular Shift Change Reports and Shift Change Conference Calls ensure that our monitoring vigilance seamlessly crosses shift changes.



Finding Security Events
Amid the Noise

DATA FROM A SINGLE LARGE CUSTOMER (24 HOURS)

15,000,000 — 15 MILLION MESSAGES COLLECTED

3700 — 3700 ALERTS FORWARDED TO OUR SOC

48 — 48 TICKETS FOR OUR ANALYSTS TO INVESTIGATE

2 — 2 CUSTOMER CONTACTS

14

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Counterpane Responds

Managed Security Monitoring is much more than an alert service. Counterpane analysts are there to assist customers in responding to attacks. An analyst not only presents the customer his diagnosis of the security event, but his recommended actions to stop the attacker and restore network security. Socrates contains detailed and current best practices about how to defend against a particular attack, based both on industry recommendations and Counterpane's past experience. The analyst works with the customer to restore security, continually watching new data from the customer's network to ensure that security has indeed been restored. And the analyst keeps the ticket open until the customer is satisfied that security has been restored.

Through this process, a bond of trust develops between Counterpane analysts and customers. Even though they may work with different analysts, depending on the time or day of week, it quickly becomes a very personal relationship. Counterpane's vigilant response allows the customers' security personnel to perform the kinds of strategic tasks they did not have time to do when they were required to respond to every alarm.

Counterpane Adapts

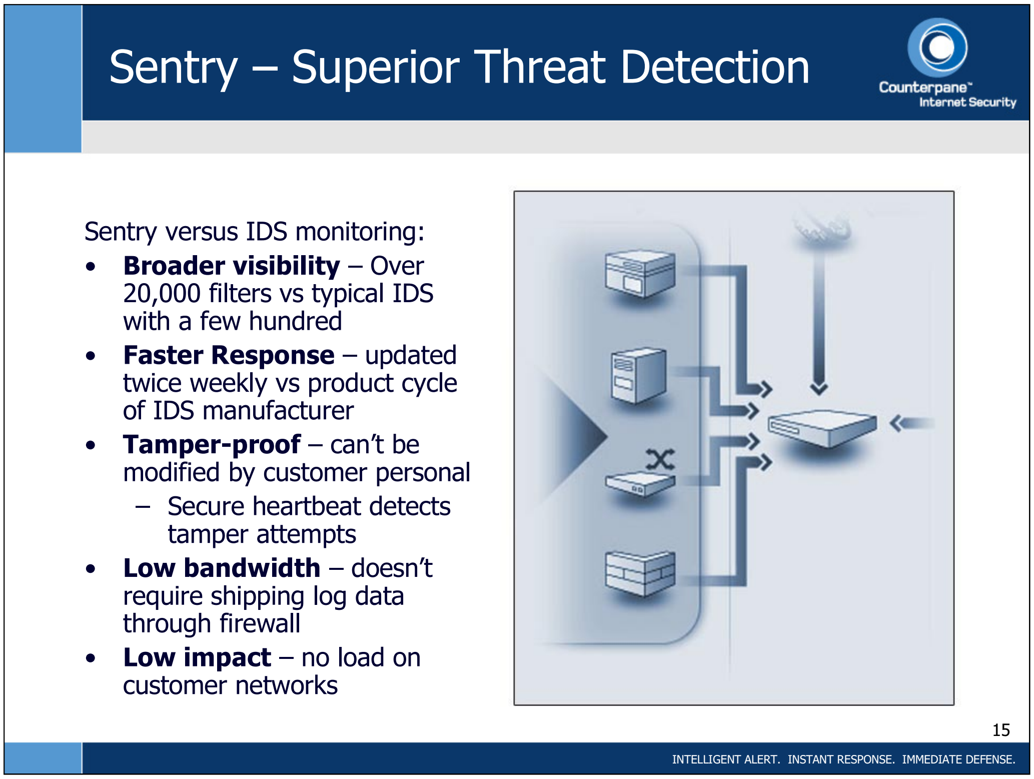
Security is constantly changing, and Counterpane's MSM service needs to continually adapt to the customer environment and the threats. The analysts have the ability to modify the Socrates database to reflect the changing needs of the customer. For example, most new customers request that we notify them in the event of a scan. Eventually- sometimes within days-the customers decide that they don't need to be notified immediately, and let that information be reflected in the Weekly Reports. Socrates can be updated with this new information. Similarly, a customer could inform the analyst that he wishes to be informed about more events, or that he wants to be put on heightened alert during a particularly critical period. Counterpane's analysts can make these changes, too.

The same process is used to update Socrates on the customer's network configuration. Networks change regularly, and we can't assume that the customer will always warn us of changes. Through this feedback process, Counterpane analysts can learn when a customer's network changes, when new sensors are brought online, and when a customer launches a new network service.

When an analyst successfully defends a customer against a particular attack, he can record his experience in Socrates. This information remains there, so that the next analyst can benefit from it when defending another customer against the same attack. In this way the entire analyst team benefits from the experience of each analyst.

The Sentries, too, are continuously updated with new filters and new information. Adaptability is critical when threats change so quickly. We update every Sentry at least twice a week, and within minutes of isolating a new threat in the wild.

The Network Intelligence group regularly adds information to the Counterpane system, based on both monitoring the hacker underground and examining the customer residue. Counterpane has the facilities to learn about new attack tools and techniques before they affect our customers, and can immediately incorporate that information into both Socrates and the Sentries.



Sentry – Superior Threat Detection

Counterpane™ Internet Security

Sentry versus IDS monitoring:

- **Broader visibility** – Over 20,000 filters vs typical IDS with a few hundred
- **Faster Response** – updated twice weekly vs product cycle of IDS manufacturer
- **Tamper-proof** – can't be modified by customer personal
  - Secure heartbeat detects tamper attempts
- **Low bandwidth** – doesn't require shipping log data through firewall
- **Low impact** – no load on customer networks

15

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Sentry

The Sentry is our custom-designed monitoring probe. It sits on the customer network, collects alerts from a wide variety of security and non-security devices, and sends relevant information back to the Counterpane SOC for further analysis.

The Sentry is a key component of Counterpane's MSM. Because it is a custom device, Counterpane can offer a level of monitoring that's impossible to achieve by companies who simply remote the existing monitoring capabilities of IDSs.

1. The Sentry is passive. It doesn't touch packets. It doesn't slow down your network. It doesn't require agents on all your servers. Our Sentry is a passive listening device: that's it's only function, and it does that better than anything else out there.

2. The Sentry's breadth of coverage is far beyond what any IDS is capable of. Monitoring works best when you're seeing data from a wide variety of sources. The Sentry was built, from the ground up, to provide comprehensive monitoring of all sorts of data types. Our Sentry has approximately 20,000 different filters, with a hundred or so being added each week.

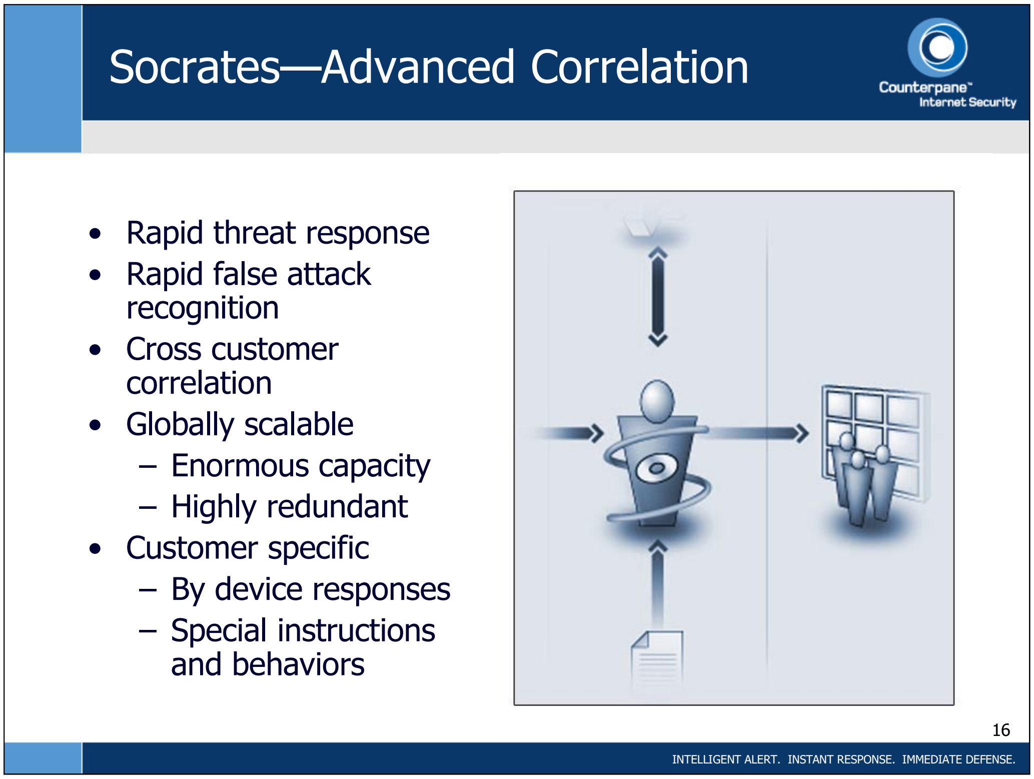
3. The Sentry provides distributed processing. Our Sentry was designed to analyze and correlate alerts, and not simply pass them back to a centralized facility. During an epidemic like Nimda, we see sustained activity levels at 10 times our normal load for a period of days, with peaks in short bursts at 100 times normal load. Counterpane's MSM was designed to scale. Companies that monitor IDSs have no way to keep up.

4. The Sentry is more immediate than anything anyone else provides. Counterpane's Sentry is designed to accept continual updates according to the needs of monitoring. We have two scheduled filter updates per week, and immediate updates when new attacks and attack tools are discovered. IDS vendors can take weeks to find out there's a new attack, plan the fix into their development schedules, and get it produced, debugged, and distributed. We do it the same day.

5. The Sentry is tamperproof. Because it's our own device, only we know how to update it. That IDS on your network can be attacked and modified by an attacker in ways that the Counterpane Sentry cannot. No customer configuration is possible on the Sentry; there's no interface. Again, because the Sentry is a custom-built special-purpose box, it's more secure than an IDS.

This difference shows itself most clearly in correlation. Correlation has two parts: data input, and pattern matching. Because our Sentry is not an IDS but a real network monitoring device, our data is broader. Because we're not monitoring what a single vendor thinks we should, our data is cleaner. Because we control our own filter updates, our data is more timely. Lots of companies now talk about correlation, but biased input yields biased output.

Counterpane is the only monitoring company that is truly vendor independent. We don't simply remote the reporting capabilities of existing products. We built our Sentry from the ground up as an integral component of our people-driven monitoring service; we don't use someone else's technology that was designed for something completely different. This gives us a monitoring capability that's fundamentally different from other companies'. And when you're being attacked, that difference is important.



Socrates—Advanced Correlation

- Rapid threat response
- Rapid false attack recognition
- Cross customer correlation
- Globally scalable
  - Enormous capacity
  - Highly redundant
- Customer specific
  - By device responses
  - Special instructions and behaviors

16

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Correlation and Trending

Correlation is critical to effective security monitoring. Since no security product is perfect, and every security and network product produces valuable information about the part of the network that it sees, the only way to provide effective security is to correlate the output of these disparate products. Counterpane was built from the ground up to facilitate correlation.

Counterpane's MSM monitors more devices on your network, so we have more raw data to work from than anyone else. And the more you can see, the better you can correlate.

Counterpane's Sentry was designed to facilitate correlation. Not only does it filter individual events, but it correlates multiple events from different devices. When the IDS detects an attack in progress, it correlates that alarm with the expected results on the target computer. When it sees multiple suspicious events, it correlates them to form a trend. The Sentry doesn't just correlate using individual event filters, but searches for trends from different devices using our proprietary Analysis Engine.

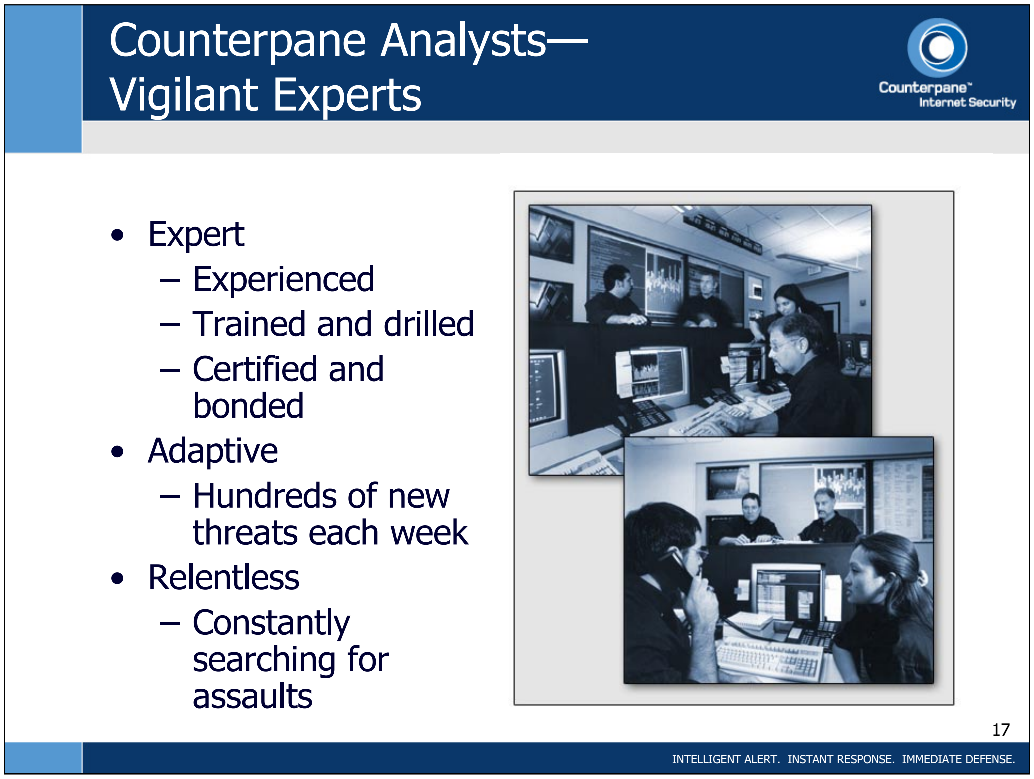
At our SOC, our proprietary knowledge base -- Socrates -- identifies long-term trends and further correlates data from different devices. And Socrates takes this kind of correlation to the next level, by analyzing data across multiple customers. The result is that we can see things faster and more clearly than anyone else, and we can detect Internet- wide trends before anyone else.

Finally, our trained security analysts are trained to look for the bigger picture amongst the data. No matter how good any technology is, some attack somewhere will get around it. This is where human intelligence comes in, and nobody has better trained and more experienced analysts than Counterpane.

Counterpane's correlation capabilities are singularly capable at finding attacks amongst the noise, and discounting false alarms from any individual product.

The problem can be most easily seen with IDSs. The reason IDSs fail so often is that they have a myopic view of the network; they only see network traffic at one point, and they have no way to correlate that with what is going on elsewhere in the network. Counterpane's MSM system correlates information from a variety of sensors: IDSs, firewalls, routers, servers, applications, niche security products, etc. This allows us to see events that any individual security product might miss, and make sense out of alerts that any one product might misdiagnose. Counterpane's monitoring process allows us to "read between the lines" and catch attacks that would escape conventional log consolidation and traditional monitoring processes.

Lots of companies talk about correlation, but they haven't built a system to do it. Counterpane has, and every day it works to protect our customers.



Counterpane Analysts—Vigilant Experts

Counterpane™
Internet Security

- Expert
  - Experienced
  - Trained and drilled
  - Certified and bonded
- Adaptive
  - Hundreds of new threats each week
- Relentless
  - Constantly searching for assaults

17

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Hiring, Training, and Drilling

Counterpane analysts are held to the highest knowledge, experience, and ethical standards. Comprehensive pre- employment screening is conducted on every analyst, including employment history background check, criminal history background check, education history verification, credit check, and California Personality Testing. New analysts must have network and security backgrounds, and two to four years of information security experience. Each is screened and tested for reliability, and after employment is bonded.

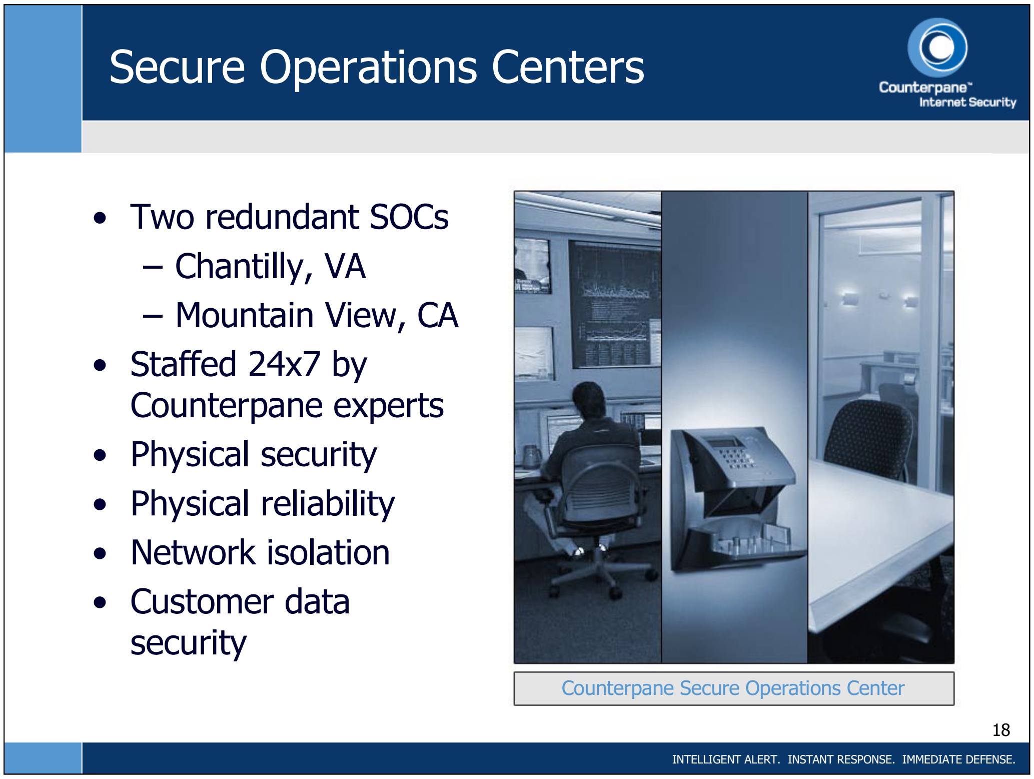
After they're hired, analysts receive both commercial security training and proprietary in-house Counterpane training. Most analysts are GIAC certified. Junior analysts are paired with senior analysts, who mentor them through the process. Counterpane analysts are tested and drilled constantly, to ensure that their skill level remains high. And Counterpane training specialists quantitatively measure the results of these drills and training, to make sure it is effective and not just an exercise.

Network Intelligence

Counterpane network intelligence experts gather information about network vulnerabilities by researching and testing new network products and updates, published vulnerabilities, and attack tools; by monitoring hacker newsgroups, Web sites, and bulletin boards; and by reviewing analysts' incident reports and information from the Sentry. Our network intelligence experts use this data to develop new detection capabilities for the Sentries, provide valuable new information to the analysts, and keep the Socrates system current.

We also generate an intelligence tool not available anywhere else: a database of real-world information on real-world attacks that helps us evaluate the success rate of previous responses. The result is an intelligent process that arms us with highly adaptive countermeasures to defend your network.

This knowledge base is vital to Counterpane's ability to recommend an instant and effective response to a customer in the event of an attack and to help us adapt quickly to spreading threats.



Secure Operations Centers

- Two redundant SOCs
  - Chantilly, VA
  - Mountain View, CA
- Staffed 24x7 by Counterpane experts
- Physical security
- Physical reliability
- Network isolation
- Customer data security

Counterpane Secure Operations Center

18

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Secure Operation Centers

Reliability and Redundancy

Each SOC has been built, from the ground up, for maximum reliability and redundancy. SOC facilities have backup power capacity that is not dependent on the local power grid in the event that electrical utilities go offline. Data connectivity is equally reliable. The WAN topology consists of multiple private networks from separate vendors that connect our sites. The SOCs have public access points that the Sentries are able to connect to. In the event of failure at one SOC, the Sentries are able to use the connections at another SOC.

The SOCs are designed for maximum redundancy. They are geographically separate. The physical plant, computer systems, and network infrastructure at each site are capable of supporting the customer monitoring service in the event that one of the sites fails or loses network connectivity. In the event of failure at a SOC, all traffic will automatically fail over another SOC. In the rare event that all SOCs are offline, a temporary SOC can operate while one of the primary SOCs is brought back online.

Network Isolation

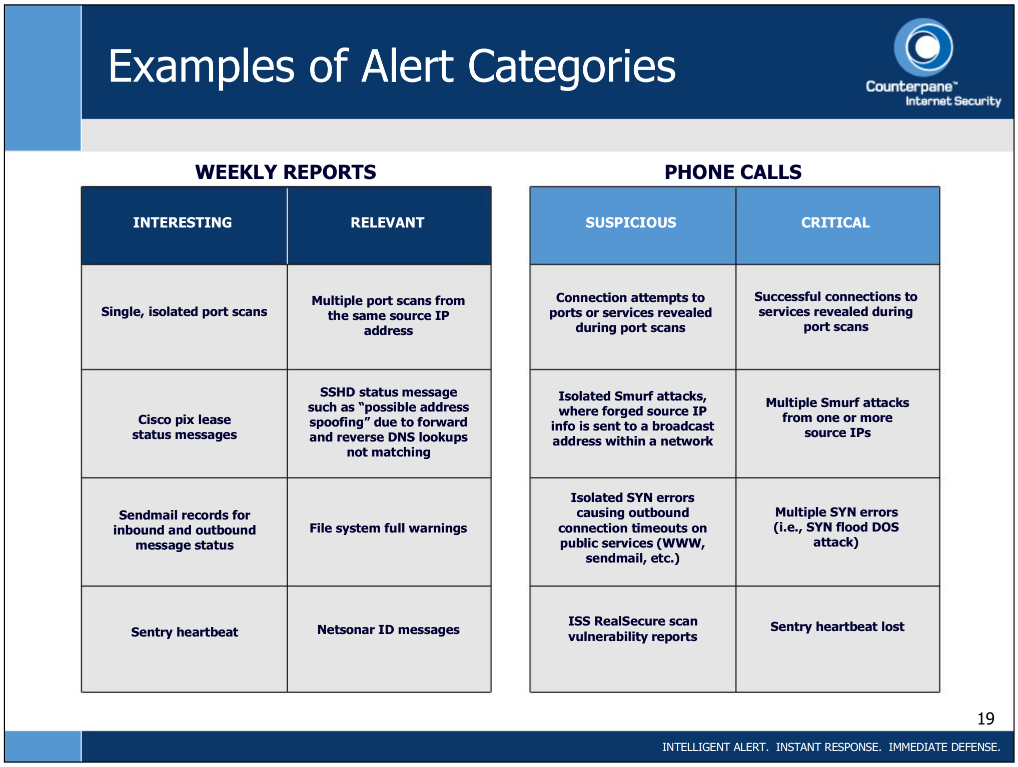
The Counterpane monitoring architecture is based on a non-interactive, SSL-based encrypted connection outbound from the customer network, across the Internet, to our Secure Operations Centers. Each Sentry is able to connect to one of multiple entry points per SOC; these connections allow for the exchange of security event data between the Sentry and the SOC. Sentries do not route traffic between the SOC and the customer network. Should a renegade customer compromise the security of the Sentry device, the renegade customer would be unable to access systems at the Counterpane SOCs or use the Counterpane SOCs to attack other customers.

Physical Security

Each SOC has multiple layers of physical security, utilizing memorized passwords, biometrics, and physical tokens. Access is permitted to only those whose job functions require it. The interior and exterior of the SOC are monitored around the clock with cameras. There are no computers in the SOC operations area, only keyboards, video monitors, and mice (KVMs). All computer systems are in a separately secured data center behind the operations area.

Customer Data Security

The SOCs do not contain any customer data except the data that has been forwarded by customer devices. These devices are configured by customer personnel, and Counterpane works with the customer to make sure that the devices only forward information that is relevant to monitoring customer systems. Counterpane does not see actual data packets as would be found on the customer’s network, nor can we modify any configurations on the customer’s network.



Examples of Alert Categories

Counterpane™
Internet Security

WEEKLY REPORTS		PHONE CALLS	
INTERESTING	RELEVANT	SUSPICIOUS	CRITICAL
Single, isolated port scans	Multiple port scans from the same source IP address	Connection attempts to ports or services revealed during port scans	Successful connections to services revealed during port scans
Cisco pix lease status messages	SSHD status message such as "possible address spoofing" due to forward and reverse DNS lookups not matching	Isolated Smurf attacks, where forged source IP info is sent to a broadcast address within a network	Multiple Smurf attacks from one or more source IPs
Sendmail records for inbound and outbound message status	File system full warnings	Isolated SYN errors causing outbound connection timeouts on public services (WWW, sendmail, etc.)	Multiple SYN errors (i.e., SYN flood DOS attack)
Sentry heartbeat	Netsonar ID messages	ISS RealSecure scan vulnerability reports	Sentry heartbeat lost

19

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Case Study: The Regence Group

The Regence Group, a major healthcare insurer in the Pacific Northwest, is an affiliation of Blue Cross/Blue Shield insurance companies in Washington, Oregon, Utah, and Idaho. A year and a half ago, the company decided to merge its individual IT security organizations into a single department and to consolidate corporate information security under one person. David MacLeod, Ph.D., CISSP, became The Regence Group's Chief Information Security Officer.

"The first thing I did is look at what we needed to do in order to have an effective information security program. I divided my tasks into two categories: what we should do internally and what we should outsource.

"Managed Security Monitoring rose to the top as something we needed to outsource. I didn't have the staff to man a monitoring station 24x7. I didn't have staff who knew enough about the diverse platforms throughout Regence Group. I didn't have people who could correlate and identify real threats, and weed out anomalies and scans."

Regence Chooses Counterpane

The Regence Group was attracted to Counterpane because they were the only company who offered the kind of comprehensive monitoring that the diverse network of The Regence Group required. "Lots of companies offered to monitor our firewalls and IDSs," said MacLeod, "but only Counterpane would monitor our entire network."

MacLeod was also impressed with Counterpane's endorsement from Lloyd's of London and the way the insurer viewed Counterpane's service offering. "It was clear that the predominant provider in this space was Counterpane."

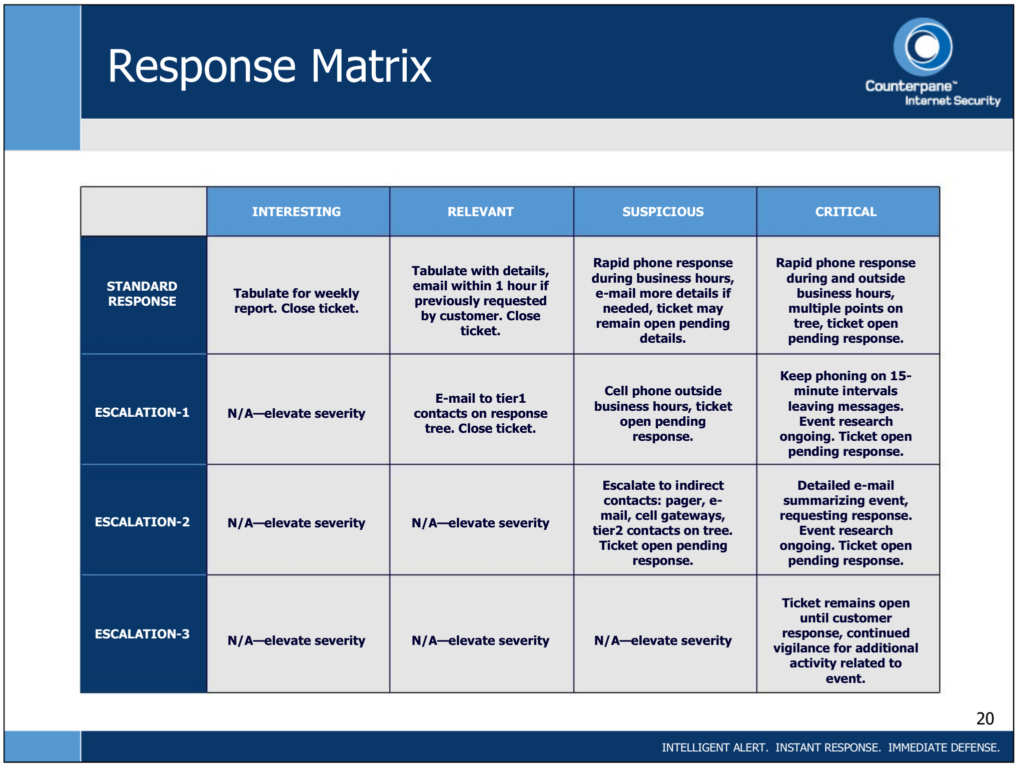
"Installation was a breeze," recalls MacLeod. "We were up and running within days. And installation continues to be easy. Whenever we have more devices that need monitoring, we just point their audit logs at the Sentry. We call Counterpane and tell them about the new devices, and we're monitored. And if we forget to call, Counterpane calls us as soon as they see the anomalous log data.

"In fact," said MacLeod, "one weekend a corporate Web server went down. Counterpane noticed the problem and called us, before we even knew about it."

Counterpane Provides Enormous Value

To Regence, Counterpane's value can be clearly demonstrated by the number of security incidents they had to deal with. MacLeod compiled statistics to present to his Board of Directors. In the fourth quarter of 2002, Regence's IDSs logged a total of 145,645 incidents. Of those, 12,875 were high-level alerts--serious attempts to compromise the Regence Group network. Another 12,300 were medium-level alerts, and the other 120,000 were low-level alerts. Counterpane's monitoring and filtering of events reduced that number to just over 200 incidents to which Regence had to respond.

(Continued on next page.)



Response Matrix

Counterpane™ Internet Security

	INTERESTING	RELEVANT	SUSPICIOUS	CRITICAL
STANDARD RESPONSE	Tabulate for weekly report. Close ticket.	Tabulate with details, email within 1 hour if previously requested by customer. Close ticket.	Rapid phone response during business hours, e-mail more details if needed, ticket may remain open pending details.	Rapid phone response during and outside business hours, multiple points on tree, ticket open pending response.
ESCALATION-1	N/A—elevate severity	E-mail to tier1 contacts on response tree. Close ticket.	Cell phone outside business hours, ticket open pending response.	Keep phoning on 15-minute intervals leaving messages. Event research ongoing. Ticket open pending response.
ESCALATION-2	N/A—elevate severity	N/A—elevate severity	Escalate to indirect contacts: pager, e-mail, cell gateways, tier2 contacts on tree. Ticket open pending response.	Detailed e-mail summarizing event, requesting response. Event research ongoing. Ticket open pending response.
ESCALATION-3	N/A—elevate severity	N/A—elevate severity	N/A—elevate severity	Ticket remains open until customer response, continued vigilance for additional activity related to event.

20

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Regence Case Study (cont.)

MacLeod explained. "I don't have the staff to handle 140,000 alerts. I don't even have the staff to handle 12,000 alerts. What Counterpane does is boil all that noise down to 200 real incidents that my team needs to respond to. Because Counterpane gives us only the information we need when we need it, we can concentrate on the attacks that matter. The value of that kind of service is enormous."

Counterpane's fast response also reduced the effects of those 200 attacks. "The FBI recently reported that roughly 1% of all Internet attacks were successful," said MacLeod. "So if you look at our 140,000 incidents, we should have seen 1400 successful attacks in the fourth quarter. Even if you use the number of high-level alerts--12,000--that should still translate to 120 successful attacks. Because Counterpane was monitoring, and because they were able to notify us so that we could respond to attacks as they were happening, we had only one serious breach during that time period. And that was Nimda."

Even Nimda, which devastated so many other companies, was swiftly contained within Regence's network because of Counterpane. "We got off easy," explains MacLeod. "Even before the Nimda storm crossed our network, Counterpane was on the phone with us explaining what was happening. We started shutting doors and updating our systems immediately, and as a result Nimda compromised only 10% of desktops and 5% of servers. I credit Counterpane."

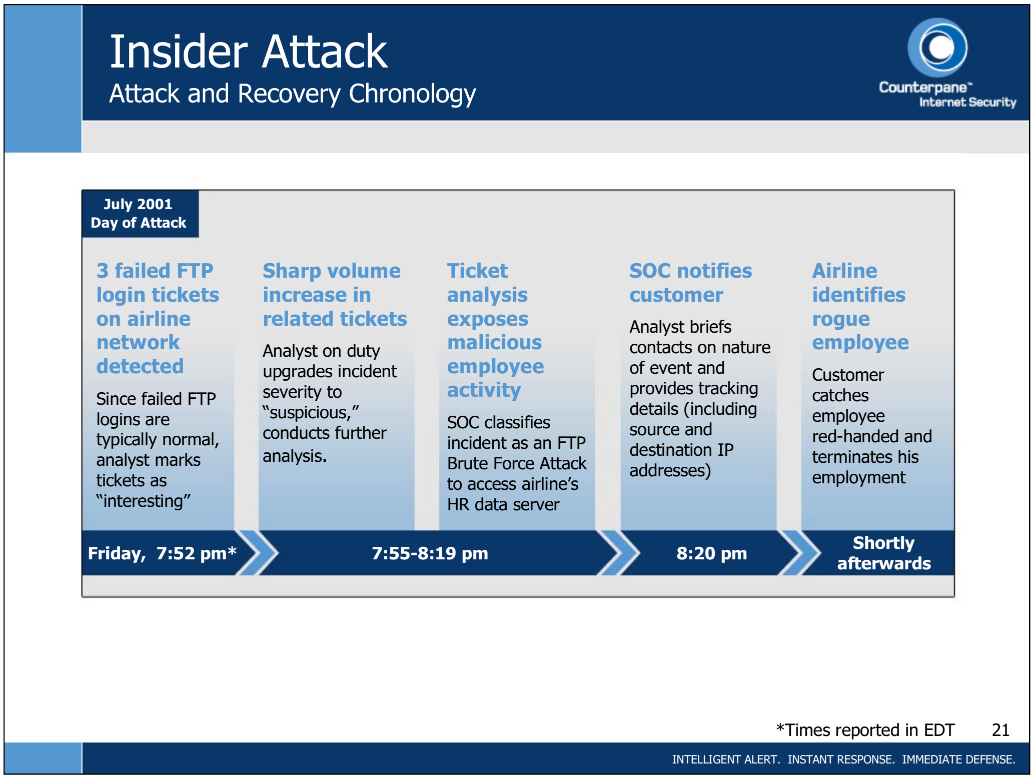
Counterpane's Global View

Regence entered into a two-year monitoring contract with Counterpane, with the expectation that they would use those two years to develop their own internal monitoring capabilities. Then, they would bring the function back in-house. But the first year proved that Regence could not replicate Counterpane's service and that continued outsourcing of Managed Security Monitoring to Counterpane remains the financially prudent approach.

MacLeod said: "When I look back at Code Red, Code Red II, and Nimda, what stands out in my mind is Counterpane's ability to respond before we were attacked. They regularly call us and tell us how we should respond, based on their experience with customers in earlier time zones."

"We could not possibly replicate Counterpane's service ourselves," continued MacLeod. "We couldn't staff it. And even if we could, we would not get the benefits of Counterpane's global view. They watch security incidents throughout the globe, and we benefit from that."

"Today, we can't do our jobs effectively without Counterpane," said MacLeod.



Insider Attack

Attack and Recovery Chronology

Counterpane™
Internet Security

July 2001
Day of Attack

3 failed FTP login tickets on airline network detected

Since failed FTP logins are typically normal, analyst marks tickets as "interesting"

Sharp volume increase in related tickets

Analyst on duty upgrades incident severity to "suspicious," conducts further analysis.

Ticket analysis exposes malicious employee activity

SOC classifies incident as an FTP Brute Force Attack to access airline's HR data server

SOC notifies customer

Analyst briefs contacts on nature of event and provides tracking details (including source and destination IP addresses)

Airline identifies rogue employee

Customer catches employee red-handed and terminates his employment

Friday, 7:52 pm* | 7:55-8:19 pm | 8:20 pm | Shortly afterwards

*Times reported in EDT 21

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Case Study: Womble Carlyle

Womble Carlyle Sandridge and Rice, PLLC is a 450-attorney law firm, with nine offices in the U.S. According to CIO Sean Scott, security is not only important for the firm's lawyers and clients, but is essential for the future success of the firm.

"As a law firm that serves high tech clients and prominent businesses, keeping up-to-date with technology-particularly security-is not an option, it's a necessity. Womble Carlyle strives to honor client privacy through a secure network. This is one of Womble Carlyle's competitive advantages."

Monitoring as a Solution

Womble Carlyle renewed research into security products last year. In addition to intensifying the sophistication of the firm's security, Womble Carlyle wanted a security audit. Several securities firms recommended Womble Carlyle contact Counterpane about security monitoring, as a way to provide long-term business security.

"By the time we called Counterpane in for a meeting, we were well-educated about the issues and were ready to do business," says Scott. "We realized that these guys knew what they're talking about, more so than some of the other security vendors we talked with. Scott added that he appreciated Counterpane's security expertise, honesty and candor.

Womble Chooses Counterpane

"We met with Vigilinx, RipTech, ISS, Symantec, Guardent, and a several other companies. Scott says. "Counterpane met our needs best. They offered competitive pricing and were vendor neutral." For Womble Carlyle, a vendor-neutral solution was critical.

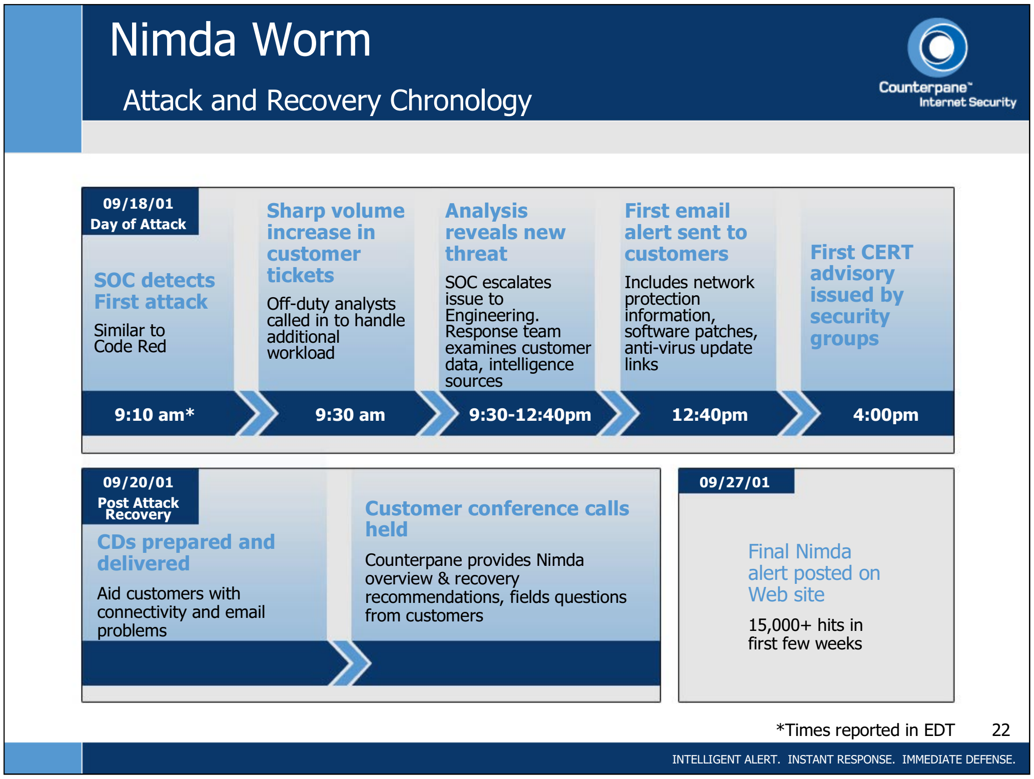
"Talking to the other vendors gave us a good reality check and starting point," Scott added. "But Counterpane was the company we chose to do business with." Womble Carlyle was impressed not only with Counterpane's technical ability and its monitoring service, but by the fact that they did not also engage in consulting or sell hardware.

"Because Counterpane only does monitoring, we felt confident that they had our best interests in mind," Scott says. "They didn't try to sell us any hardware, software or consulting services. Others wanted to make money by selling us additional hardware and software."

Counterpane: The First Month

Installing the Counterpane service was painless. Scott recalls: "The installation was done in five hours, at most. I was shocked that something like that happened so quickly, with no ill affect on my network." Counterpane started monitoring Womble Carlyle immediately.

(Continued on next page.)



Nimda Worm

Attack and Recovery Chronology

09/18/01
Day of Attack

SOC detects First attack

Similar to Code Red

9:10 am*

Sharp volume increase in customer tickets

Off-duty analysts called in to handle additional workload

9:30 am

Analysis reveals new threat

SOC escalates issue to Engineering. Response team examines customer data, intelligence sources

9:30-12:40pm

First email alert sent to customers

Includes network protection information, software patches, anti-virus update links

12:40pm

First CERT advisory issued by security groups

4:00pm

09/20/01
Post Attack Recovery

CDs prepared and delivered

Aid customers with connectivity and email problems

Customer conference calls held

Counterpane provides Nimda overview & recovery recommendations, fields questions from customers

09/27/01

Final Nimda alert posted on Web site

15,000+ hits in first few weeks

*Times reported in EDT 22

Counterpane™ Internet Security
INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Womble Case Study (cont.)

Initially, Counterpane analysts called Womble Carlyle often about security events. "My security engineers got a number of calls from Counterpane in the first week and a half," says Scott. "We would apply patches and fix problems in our network."

During the first month, Counterpane and Womble Carlyle worked together to get a more accurate picture of the Womble Carlyle network: to figure out what worked, what didn't, what was good, and what was bad. Security at Womble Carlyle soon improved. Scott says: "IT still get e- mails from Counterpane. But we don't get any more phone calls at night."

Counterpane Helps Make Security Easy

Counterpane is currently monitoring 150 devices on the Womble Carlyle network, including every Internet portal. Every time Womble Carlyle adds a new office, Counterpane monitoring is added. "Counterpane is as integral in our network as Cisco routers," adds Scott.

The most significant benefit that Womble Carlyle can point to is that Counterpane makes network security easier. "Counterpane gives IT the information we need to figure out what's important from a security perspective. Before Counterpane, we didn't always have the most comprehensive information," says Scott. Network security operates much more efficiently now.

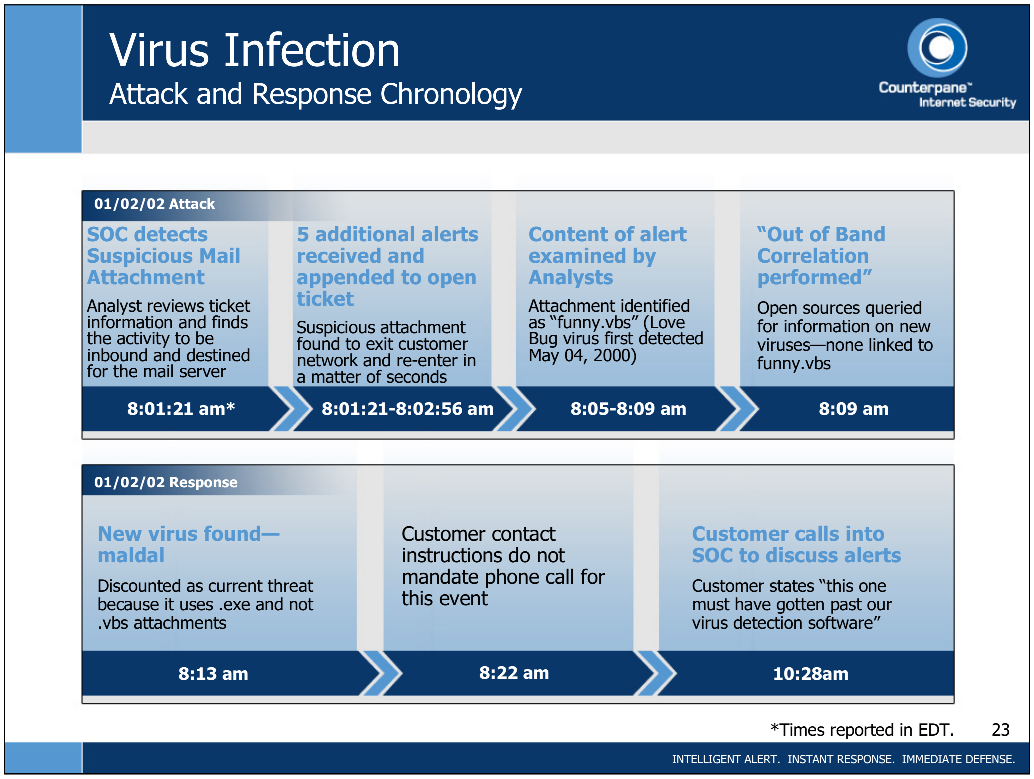
Counterpane also gives Scott piece of mind. "If we were to be threatened by some breach, I know we would be alerted by Counterpane and advised on how to react. Womble Carlyle's IT professionals can now focus more of their time on providing attorneys with technical service in other areas.

End Results

Counterpane monitoring gives Scott and his security staff time to improve Womble Carlyle's security. Because they're spending their time more efficiently, they can concentrate on strategically adding security products and policies internally. "There are still fires to put out, but we put them out quickly and effectively," says Scott.

"If we didn't have Counterpane monitoring us, we would be going through the process of adding security internally, while at the same time we would have to monitor the workings inside our network, including improper activities."

Scott concluded: "If you don't keep up with security, you're finished. We all live in the age of data wreckage. People try to raid corporate e-mail, steal client lists, disrupt network operations. We are a law firm committed to protecting our data. To best serve our clients and the firm at large, IT must protect data security. Counterpane's an integral part of that security."



Virus Infection

Attack and Response Chronology

Counterpane Internet Security

01/02/02 Attack

SOC detects Suspicious Mail Attachment

Analyst reviews ticket information and finds the activity to be inbound and destined for the mail server

8:01:21 am*

5 additional alerts received and appended to open ticket

Suspicious attachment found to exit customer network and re-enter in a matter of seconds

8:01:21-8:02:56 am

Content of alert examined by Analysts

Attachment identified as "funny.vbs" (Love Bug virus first detected May 04, 2000)

8:05-8:09 am

"Out of Band Correlation performed"

Open sources queried for information on new viruses—none linked to funny.vbs

8:09 am

01/02/02 Response

New virus found—maldal

Discounted as current threat because it uses .exe and not .vbs attachments

8:13 am

Customer contact instructions do not mandate phone call for this event

8:22 am

Customer calls into SOC to discuss alerts

Customer states "this one must have gotten past our virus detection software"

10:28am

*Times reported in EDT. 23

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Case Study: Corio

Corio is a leading enterprise application service provider, offering world-class application management services to large, global enterprises. Corio takes end-to-end responsibility for customer's mission critical enterprise applications and delivers superior speed, reliability visibility, control and economics - Corio SRVCE™.

Corio's philosophy is simple: They are fully accountable to their customers for an end-to-end solution. The customer's experience must be seamless. To that end, Corio only partners with the industry leaders in areas such as computers, networks, security, and enterprise applications.

Corio's trust model must extend to its customers, in every aspect of its business and not just in security. Discovering problems is a base requirement, but proactive monitoring enables Corio to deliver superior service. This holistic approach to security permeates every aspect of Corio's business.

The Security Challenge

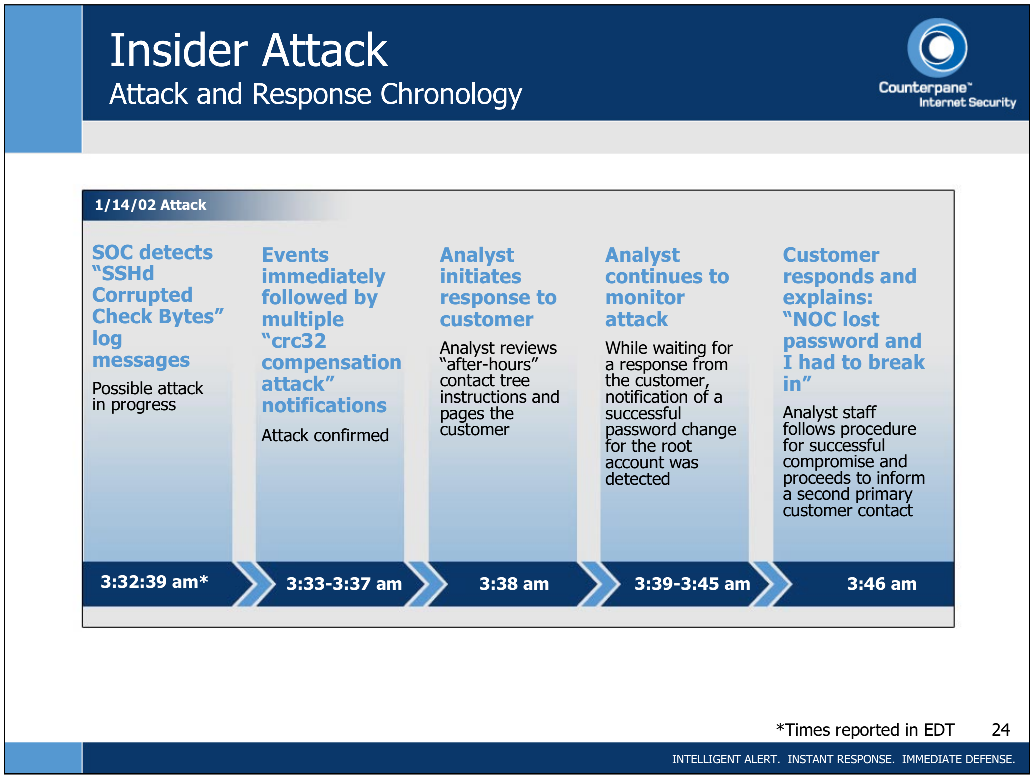
Corio has the application expertise to integrate, deploy, and manage best-in-class enterprise applications to enable mission-critical business processes. They need a security solution that can scale to support very large enterprises, with the flexibility, levels of support, and global reach that they require. Staying abreast of security changes is both a complex and challenging task, especially when the company focus is on value-added services for its customers. Reducing vulnerabilities is a key aspect of Corio's business, and they turned to Counterpane's security experts for assistance.

Most security implementations in large corporations are little more than huge firewall systems: cumbersome, porous, and static. Corio's business requires a much more dynamic model; they need security to be flexible and adaptable. Corio's customers must trust Corio, and they are very concerned about secure connections between them and Corio, as well as between Corio and its partners.

Corio's Choices

Corio Security developed a matrix of selection criteria delineating the different services and security features available from each vendor: IDS, firewalls, VPNs, access control, user authentication, vulnerability assessment, and comprehensive 24/7 enterprise network monitoring. This matrix is still used today in the selection of current and future vendors, as part of Corio's multi-layered security solution.

(Continued on next page.)



Insider Attack

Attack and Response Chronology

1/14/02 Attack

SOC detects "SSHd Corrupted Check Bytes" log messages

Possible attack in progress

3:32:39 am*

Events immediately followed by multiple "crc32 compensation attack" notifications

Attack confirmed

3:33-3:37 am

Analyst initiates response to customer

Analyst reviews "after-hours" contact tree instructions and pages the customer

3:38 am

Analyst continues to monitor attack

While waiting for a response from the customer, notification of a successful password change for the root account was detected

3:39-3:45 am

Customer responds and explains: "NOC lost password and I had to break in"

Analyst staff follows procedure for successful compromise and proceeds to inform a second primary customer contact

3:46 am

*Times reported in EDT 24

Counterpane Internet Security
INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Corio Case Study (cont.)

Why Counterpane

Corio chose Counterpane for several reasons. First and foremost, Counterpane dominates the monitoring field. Corio could state to its customers that Counterpane was monitoring Corio's, and by extension its customers' security. Additionally, the two companies have similar security philosophies: manage risk instead of endlessly searching for the right technologies and products to "solve" the security problem. Both companies believe that there is no bulletproof security solution, and that a risk-management analysis is the only way to determine the right level of security. Both companies also understand that people are a critical component of good enterprise security. Counterpane's expert security analysts were a perfect match for Corio's own security staff.

Results

Counterpane's Managed Security Monitoring is a key component of the value-added service offered by Corio to their ASP customers. Combining Counterpane's always-on- watch "radar" with Corio's in-house security expertise has put Corio in an excellent security position; it gives Corio the capability to be more proactive in its security, rather than simply reactive. And this reduces the risk, both to Corio and to its customers, of doing business electronically. It automates the labor-intensive and time-consuming log collection and analysis process in addition to cross correlating all the sensor log information to provide timely intelligence of what is happening across the Corio enterprise.

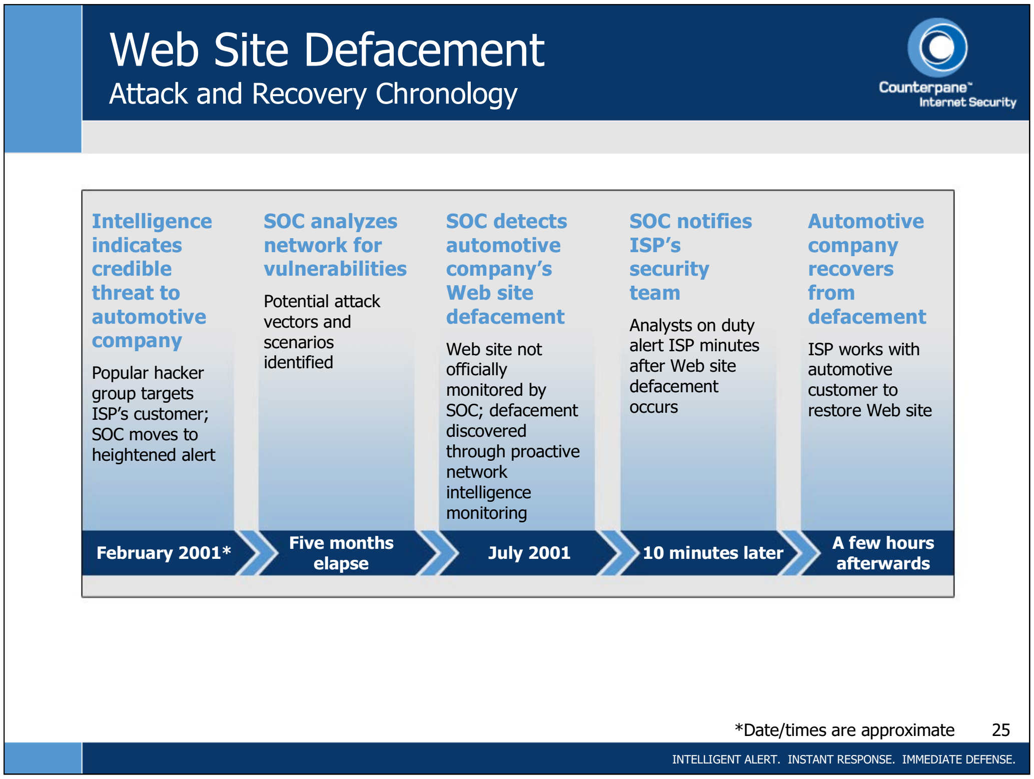
Working with Counterpane means that Corio is not locked into a single vendor solution. Corio has the ability to choose best-of-breed security products, confident that they can be monitored.

Corio's Experience

Corio has been a user of Counterpane's MSM service from the very beginning. Their combined collaboration and responsiveness has yielded a strong partnership and, through Counterpane's capabilities, one of the most innovative business models in the ASP industry.

More case studies can be found at:

http://www.counterpane.com/experiences.html



Web Site Defacement

Attack and Recovery Chronology

Intelligence indicates credible threat to automotive company	SOC analyzes network for vulnerabilities	SOC detects automotive company's Web site defacement	SOC notifies ISP's security team	Automotive company recovers from defacement
Popular hacker group targets ISP's customer; SOC moves to heightened alert	Potential attack vectors and scenarios identified	Web site not officially monitored by SOC; defacement discovered through proactive network intelligence monitoring	Analysts on duty alert ISP minutes after Web site defacement occurs	ISP works with automotive customer to restore Web site
February 2001*	Five months elapse	July 2001	10 minutes later	A few hours afterwards

*Date/times are approximate 25

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

SOC Event Reports

The following are examples of events detected and responses taken at the Counterpane SOC. To protect the privacy of our customers, the dates, customer names, and other identifying network information have been altered or deleted.

Responding to a Concerted Attack: Customer Beta

Socrates detected that an attacker in China was probing Beta's network, attempting to find the system file cmd.exe. The analyst notified Beta that they were being actively probed, and that if one of these probes was successful, it could lead to the system being compromised. The analyst suggested that Beta make sure that all the patches on the server were up to date, and that perhaps they should block the source network. An administrator from Beta called back shortly thereafter, and the analyst suggested that he check the access and error logs to ascertain whether any of the access attempts had been successful. If Counterpane had not been monitoring, the probes would not have been detected, and there would have been no evidence of a problem until Beta's system was actually compromised.

Detecting a Worm Infection: Customer Epsilon

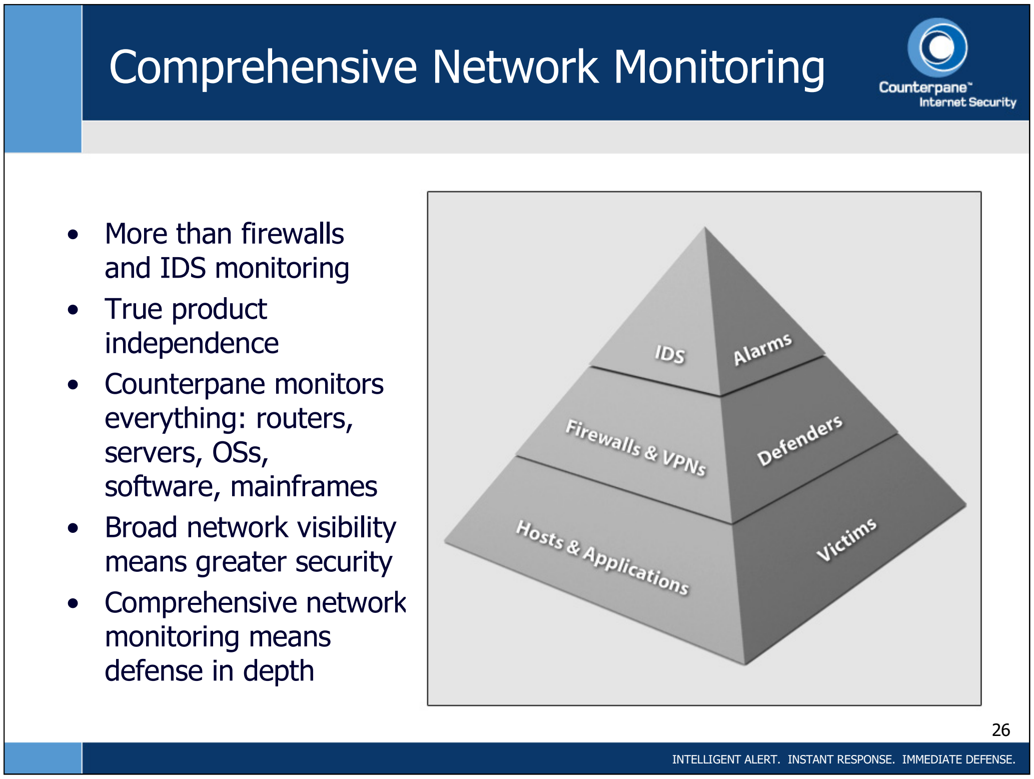
Socrates detected that a host running on Epsilon's corporate network was in the process of being infected by the Ramen worm, and alerted the Counterpane analyst. According to Epsilon's security policy, alerts of this type were supposed to be ignored. Because of the seriousness of the attack, the analyst called the customer anyway. Further investigation revealed that the host under attack was a personal Web server run by a company employee. The Counterpane analyst assisted the customer in removing the Ramen worm and returning the network to a secure state. Had this event not been detected, the attacker would have compromised the Web server and could have used it as a foothold to attack other parts of the corporate network. The fact that this Web server was not controlled and authorized by Epsilon's network administrators increased the danger.

Updating a Customer Profile Based on Monitoring Information: Customer Eta

One of Counterpane's customers has a sysadmin who repeatedly mistypes his password. On a regular day this individual can enter it five or six times (the record is 21). The IDS reports this as a brute-force attack against the server. Since the user is attempting to obtain root access, this generated a trouble ticket. Eta was called, and after some internal investigation they realized that it was their own fat-fingered sysadmin. Since this could happen over 10 times a day, Eta now has Counterpane log the event but not make a call.

Determining an Attack was a False Alarm: Customer Iota

Socrates detected an attacker attempting to install the BackOrifice Trojan onto a Web server on Iota's network and notified the Counterpane analyst. Further investigation revealed that the attack targeted a system that the customer was not running. While the attack was a false alarm, the persistence of the attacker led the analyst to put Iota's network on heightened alert. E-mail notification was sent to the Iota contact, since this was not an immediate emergency.



Comprehensive Network Monitoring

Counterpane™ Internet Security

- More than firewalls and IDS monitoring
- True product independence
- Counterpane monitors everything: routers, servers, OSs, software, mainframes
- Broad network visibility means greater security
- Comprehensive network monitoring means defense in depth

IDS
Alarms
Firewalls & VPNs
Defenders
Hosts & Applications
Victims

26

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

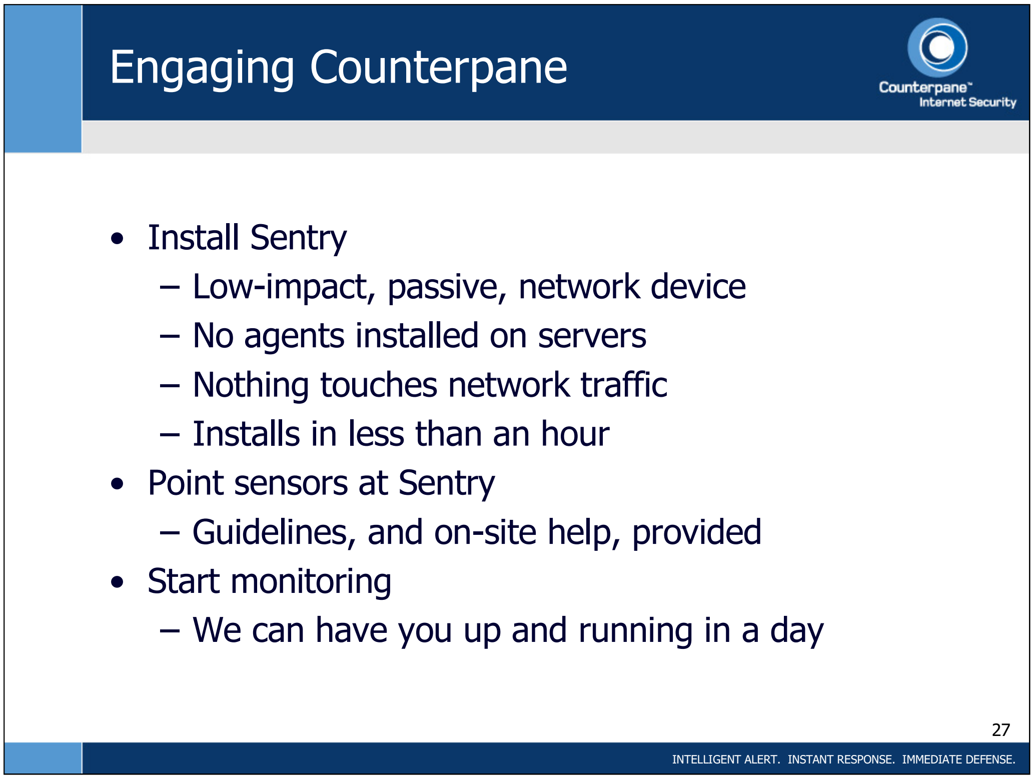
We Monitor Everything

No security product is perfect. They all add value in some areas, and have deficiencies in others. The only way to provide good network security is to monitor a wide variety of products. This gives defense in depth, and is the best way to provide resilient security.

Traditionally, corporate security teams tend to focus the majority of their efforts and budgets on perimeter security systems: firewalls, network-based intrusion detection systems, and virtual private networking servers. However, by themselves, perimeter systems present a very skewed image of malicious or damaging activity on a corporate network. Firewalls and VPNs typically only record information about the success or failure of a particular network connection attempt. Without a lot of additional context and processing -- including comparison to the company's appropriate use policy, long- term trend analysis and thresholding -- network connections aren't very interesting. Intrusion detection systems are tuned to detect content-based attacks and a variety of other malicious activity, but they're really only an early warning system. Once the IDS alarm has gone off, someone has to investigate the targeted machine and decide whether or not the attack was successful. And perimeter devices are usually located on the outer edges of the network, with limited visibility to activity and systems within the heart of the corporate infrastructure. So they'll frequently only detect the first wave of an attack, and not the subsequent, frequently normal looking, activity undertaken by an attacker once they're in.

It's like trying to build a pyramid by starting at the top, rather than the bottom. No matter how hard you try, you're doomed to failure.

What separates Counterpane from its competitors is our ability to monitor devices throughout the network, not just at the perimeter. By combining IDS and firewall logs with logs from the routers, servers, and applications in our customers' environments, we have the unique ability to understand the network and to find attacks that "fly below the radar" of individual products. Some attacks only affect the target computer, and are invisible to everything else on the network. What about attacks that originate inside the firewall's perimeter? What about attacks that the IDS can't differentiate from normal traffic? What about attacks that target vulnerabilities in these products, or simply don't register in either of these products' audit logs? Trojans are often introduced into a network by human error, and might not register as malicious code. By monitoring the entire network, Counterpane can detect these attacks. By monitoring the entire network Counterpane can separate a real attack from a false alarm, understand what risks the attack poses, and recommend a suitable response. We can easily decide whether a buffer overflow attack against a UNIX print server was successful. We can dismiss IDS alarms for attacks on Microsoft's Internet Information Server because we know you're running Apache. We can tell you what the attacker did once he got in, and help you repair the damage. We've built our monitoring service to collect all the data your network generates, not just the data on the top of the pyramid. This is why Counterpane's MSM service is unmatched in the industry.



Engaging Counterpane

- Install Sentry
  - Low-impact, passive, network device
  - No agents installed on servers
  - Nothing touches network traffic
  - Installs in less than an hour
- Point sensors at Sentry
  - Guidelines, and on-site help, provided
- Start monitoring
  - We can have you up and running in a day

27

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Weekly Reports

All MSM customers receive a weekly report from Counterpane outlining all security events during the previous seven days, as well as trend data from previous weeks. These reports allow customers to see how well their security is working, and to identify aspects that need improvement. Every incident that requires a Counterpane analyst to contact the customer is summarized in the report.

The report consists of two basic parts: a weekly summary and trending data. The weekly summary is a quick summary of security-related activity on the customer's network. This includes information about events detected and how they have been resolved, and all events not important enough to require immediate customer contact. Trending data includes tables of security-related events for the previous 7, 30, and 60 days. Detailed information includes the security-related events for each individual sensor: firewall, IDS, router, server, application, etc.

Counterpane's weekly reports are a summary and listing of security events and other metrics over the period of a week. These reports provide a helpful visual representation of what the analysts are seeing from a customer's network weekly. They are also the vehicle by which Counterpane conveys non-critical suggestions to the customer, such as IDS tuning.

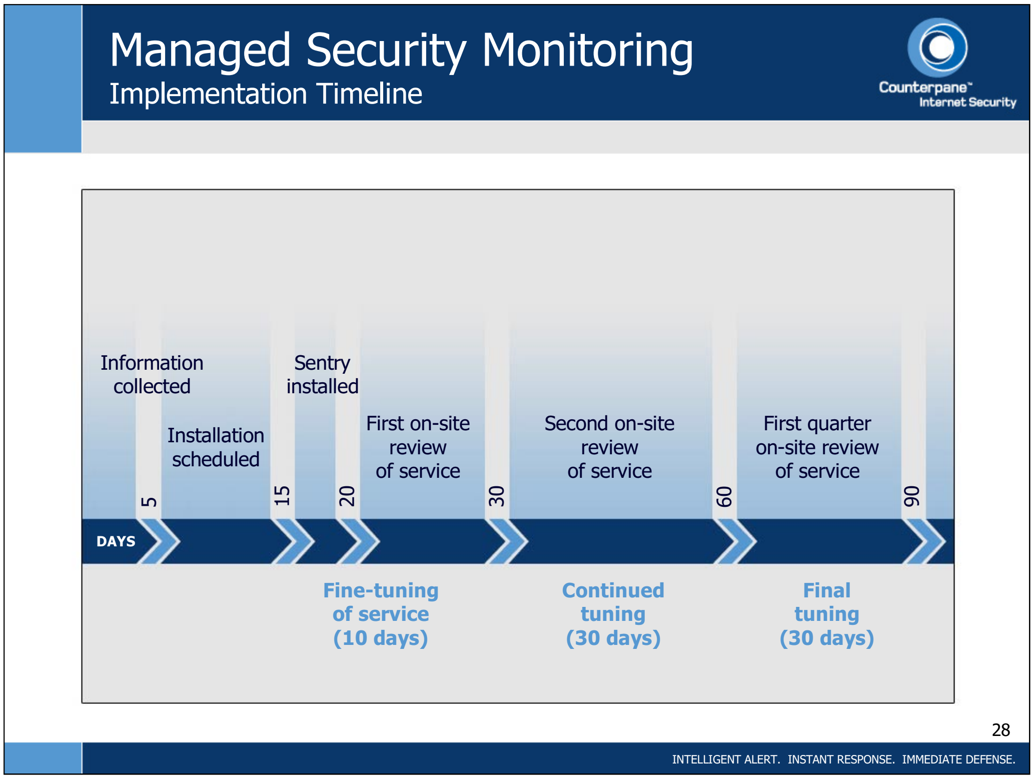
The sections of this report include:

1. Weekly Summary -- Describes counts of alerts grouped by severity, tickets that Counterpane analysts have contacted customer point of contacts (POCs) about, and high volume alerts.

2. Trending Data -- Breaks alert volume down over last 7-, 30-, and 60-day periods; quantifies events grouped by customer's sensor addresses reporting events; groups events by symptom names and sensor reporting for 7-, 30-, and 60-day period.

3. Incident Details -- List tickets reported during previous 7 days, including customer interaction (e-mail or synopsis of phone conversation between analysts and customer POC).

4. Message Exceptions -- Lists changes in severities to messages made by Counterpane over the last 7 days. This is usually downgrading recurring false positive events so that they will no longer create tickets for the analysts to contact the customer on, but occasionally upgrades alerts so that customer will receive a phone call/e-mail each time the alert generates a problem ticket.



Managed Security Monitoring

Implementation Timeline

Counterpane™ Internet Security

DAYS

5 Information collected

Installation scheduled

15 Sentry installed

20 First on-site review of service

30 Second on-site review of service

60 First quarter on-site review of service

90

Fine-tuning of service (10 days)

Continued tuning (30 days)

Final tuning (30 days)

28

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

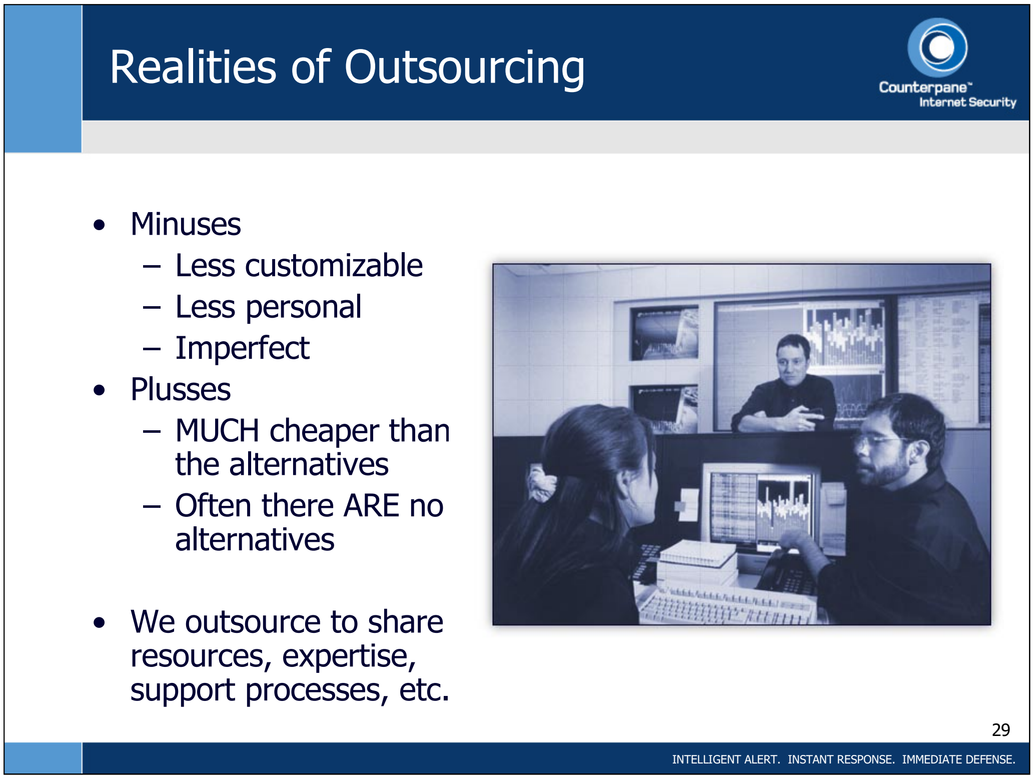
Installation and Integration

The first 90 days is called the "integration phase." During this time, there are recurring reviews with the financial stake holder at 30, 60, and 90 day increments. Although there is a technical component to these meetings, they are designed to address the business and process issues of integrating the Counterpane monitoring solution into the customer's environment. During these meetings the customer will be informed as to how well the integration process is proceeding and how effective the Counterpane/customer partnership is at meeting integration and monitoring goals. As an example, at the 30-day review, Counterpane will discuss the success of the installation process, the status of special customer requests, how well customer requirements are being interpreted, SOC responsiveness, and how responsive customer contacts are to SOC notifications. At he 60-day review, Counterpane will address those topics as well as any action items that are the result of the first meeting. The 90-day review will be a closing meeting describing final status and the transition to monthly technical report reviews and ongoing monitoring.

We Monitor Anything

Counterpane's MSM service is designed to monitor anything. We don't have a short list of security products that we support. We don't have a list of required configurations for your security products. We don't demand to manage, or otherwise control, your network. We monitor your network, as it is today and however you choose to change it tomorrow.

Corporate networks are ever evolving, and Counterpane continually adapts to that evolution. When you're being monitored by Counterpane, we expect you to add devices under our monitoring umbrella. We may not be part of the planning; you might not have told us you're changing things. We expect that we will see devices in our monitoring stream that we've never seen before, and we've built a process to understand and monitor those new devices.



Realities of Outsourcing

- Minuses
  - Less customizable
  - Less personal
  - Imperfect
- Plusses
  - MUCH cheaper than the alternatives
  - Often there ARE no alternatives

- We outsource to share resources, expertise, support processes, etc.

29

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Outsourcing Security

If the decision to outsource network security is a difficult one, the decisions of what to outsource and where seem impossible. The stakes are high. On the one hand, the promises of outsourced security seem so attractive: the potential to significantly increase your network's security without hiring half a dozen people or spending a fortune is impossible to ignore. On the other hand, there are the stories of managed security companies going out of business, and bad experiences with outsourcing other areas of IT. It's no wonder that paralysis is the most common reaction to the whole thing.

I believe that network security will continue to be outsourced, because there's no other way to deal with the shortage of skilled computer security experts, the increasing requirements for businesses to open their networks, and the ever-more-dangerous threat environment. For the Internet to succeed as a business tool, security has to scale. Outsourcing is how it will do that.

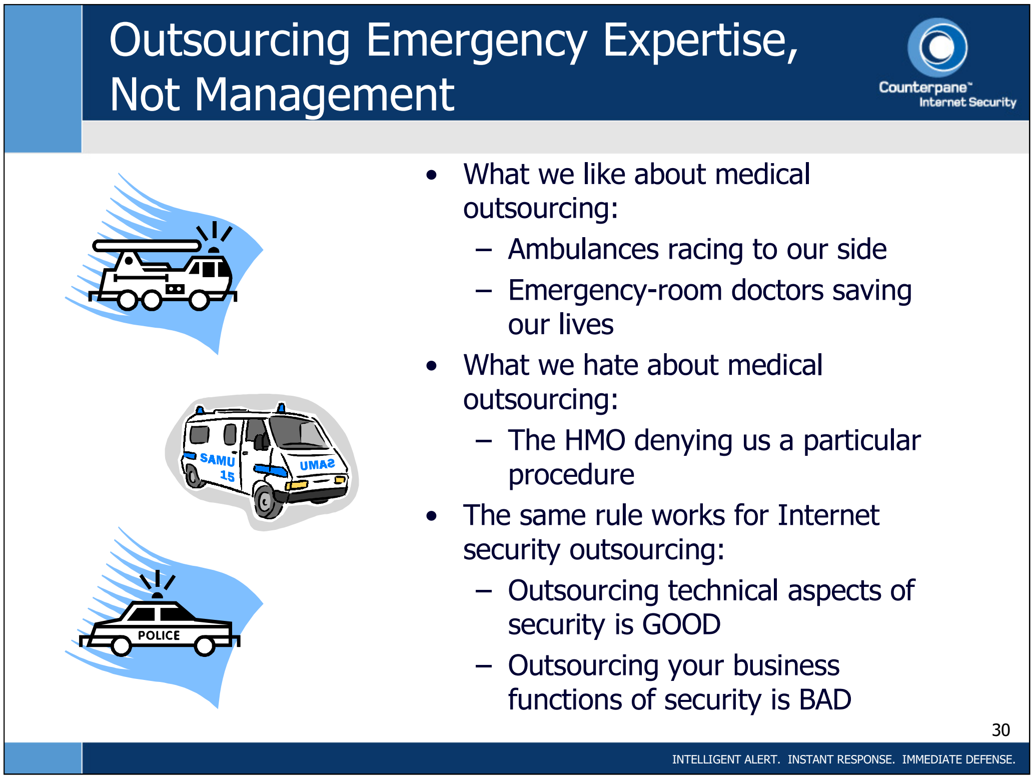
Over the past few years, we've seen many different companies offering different capabilities under the general category of "managed security services." The field is so confusing that even the industry analysts can't agree on how to categorize them. This company offers to manage your firewall. That company offers periodic vulnerability scans. Another offers to manage your security policy, or monitor your network, or install your IDS, or host your computers. Some of these businesses make sense, and some of them don't. Some will survive, and some of them won't. Knowing which is which is the first step.

What to Outsource

You won't outsource everything, because some things just don't outsource well. Either they're too close to your business, or they're too expensive for an outsourcing company to deliver efficiently, or they simply don't scale well. Knowing the difference is important.

Medical care is a prime example of outsourcing that we can use for comparison. Everyone outsources healthcare; we don't act as our own doctor. More to the point, no one hires a private personal doctor. And we all know what aspects of medical care we like: the ambulance picks up in seconds and rushes us to the hospital, a team of medical experts spares no expense in running tests to figure out what's wrong and in doing whatever it takes to cure us, someone else paying the bill. And we all know what aspects we don't like: ill-equipped and ill-staffed hospitals, HMOs telling us that we can't have that particular test or that a specialist isn't warranted in this case, getting stuck with the bill. When I imagine the wonders of healthcare in the future, I think of automatic monitoring systems that watch our every heartbeat and automatically alert doctors if there's a problem. When I imagine future healthcare horrors, I think of decisions about our health made by accountants and being forced to accept the decisions of others.

The aspects of outsourced healthcare we like involve immediate access to experts. Any medical emergency requires experts, and the faster they can pay attention to us the better off we'll be. The aspects of outsourced healthcare we don't like involve management. Our healthcare is our responsibility, and we don't want someone else making life and death decisions about us.


SAMU
15
SAMU
POLICE

Outsourcing Emergency Expertise, Not Management

Counterpane™ Internet Security

- What we like about medical outsourcing:
  - Ambulances racing to our side
  - Emergency-room doctors saving our lives
- What we hate about medical outsourcing:
  - The HMO denying us a particular procedure
- The same rule works for Internet security outsourcing:
  - Outsourcing technical aspects of security is GOOD
  - Outsourcing your business functions of security is BAD

30

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Outsourcing Security (cont.)

Network security is no different. Outsource expert assistance: vulnerability scanning, monitoring, consulting, forensics. Don't outsource management.

This truism has been borne out in the industry. Salinas Network Services was the largest firewall management company. For a price, Salinas would manage your firewall. Earlier this year, it disappeared. There just wasn't a business in managing firewalls for other companies. The companies demanded too much individual attention for the money they were willing to pay. Firewall management is just too core to a business. They had no choice but to treat their Salinas contacts as employees.

Pilot Network Services offered secure network management. It's business was to host your computers securely, manage all security devices, test your applications before putting them up on the network...effectively becoming your security management group. They're gone now too - same problem.

Some consulting companies are doing well and some are not. This is more a function of is the quality of the service they offer. Consulting is, and always will be, a profitable business. Outsourcing occasional requirements for expertise transcends any single area.

Outsourced security companies that are doing well are the ones that offer well-defined services that companies need. For example:

· consulting companies like @Stake and Foundstone for expert advice and assistance: strategic security consulting, penetration testing, forensics, etc.

· security VARs for product installation and configuration

· TruSecure for certification and expert assistance

· Counterpane for network security monitoring

In all of these cases, the company buying the outsourced services retains control of its own security. This is important for the company purchasing the services, but it is also important for the vendor. By not demanding a management role, the security companies can offer a useful, effective, and scalable service.

Arguments for Outsourcing

The primary argument for outsourcing is financial: a company can get the security expertise it needs much more cheaply by hiring someone else to provide it. Take monitoring, for example. The key to successful security monitoring 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.

High Risk Outsourcing

31

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Outsourcing Security (cont.)

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 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. Security monitoring is inherently erratic: six weeks of boredom followed by eight hours of panic, then seven weeks of boredom followed by six hours of panic. Attacks against a single organization don't happen often enough to keep a team of this caliber engaged and interested.

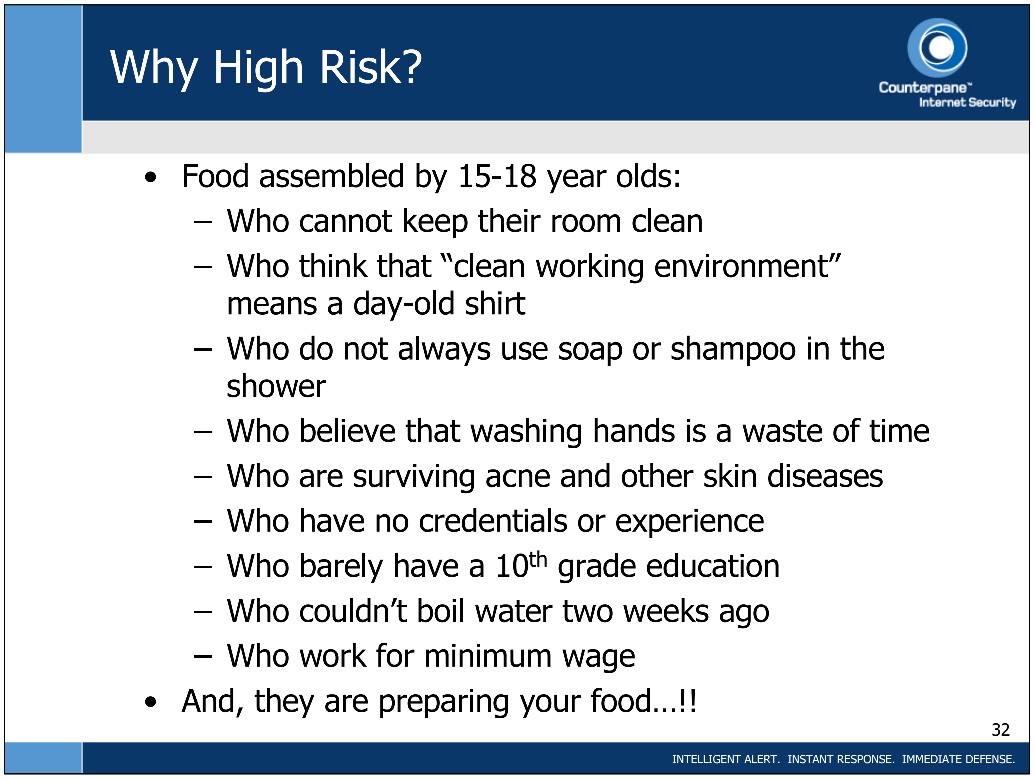
This is why outsourcing is the only cost-effective way to satisfy the requirements. Think about healthcare again. I may only need a doctor twice in the coming year, but when I need one I may need him immediately, and I may need specialists. Out of a hundred possible specialties, I may need two of them -- and I have no idea beforehand which ones. I would never consider hiring a team of doctors to wait around until I happen to get sick. I outsource my medical needs to my clinic, my emergency room, my hospital. Similarly, a network will outsource its security monitoring.

Aside from the aggregation of expertise, an outsource monitoring service has other economies of scale. It can more easily hire and train its personnel, simply because it needs more employees. 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. Outsourced security companies can spread these costs among all of their customers.

An outsource company 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. No matter how wealthy you are, you do not hire a doctor to sit in your living room waiting for you to get sick. You get better medical care from a doctor that sees patient after patient, learning from each one. To an outsource security company, network attacks are everyday occurrences; its experts know exactly how to respond to any given attack, because in all likelihood they have already seen it many times before.

How to Choose an Outsourcer

This is difficult, because it's hard to tell the difference between good computer security and bad computer security. But by the same token, it's hard to tell the difference between good medical care and bad medical care. If we're not health experts ourselves, we can sometimes be led astray by bad doctors that appear to be good. So, how do you choose a doctor? Or a hospital? I choose one by asking around, getting recommendations, and going with the best I can find. Medical care involves trust; I need to be able to trust my doctor.



Why High Risk?

Counterpane™
Internet Security

- Food assembled by 15-18 year olds:
  - Who cannot keep their room clean
  - Who think that "clean working environment" means a day-old shirt
  - Who do not always use soap or shampoo in the shower
  - Who believe that washing hands is a waste of time
  - Who are surviving acne and other skin diseases
  - Who have no credentials or experience
  - Who barely have a 10th grade education
  - Who couldn't boil water two weeks ago
  - Who work for minimum wage
- And, they are preparing your food…!!

32

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Outsourcing Security (cont.)

Security outsourcing is no different; you should to choose a company you trust. To determine which one, talk with others in your industry or ask analysts. Go with the industry leader. In both security and medical care, you don't use a little-known maverick unless you're desperate.

Watch companies that have conflicts of interest. Some outsourcers offer security management and monitoring. This worries me. If the outsourcer finds a security problem with my network, will the company tell me or try to fix it quietly? Companies that both sell and manage security products have the same conflict of interest. Consulting companies that offer periodic vulnerability scans, or network monitoring, have a different conflict of interest: they see the managed services as a way to sell consulting services. There's a reason companies hire outside auditors: it keeps everyone honest. I believe that outsourcers that offer combined management/monitoring services will be among the next to disappear. And if a company decides to outsouce its security-device management, it is essential that it outsource its monitoring to a different company.

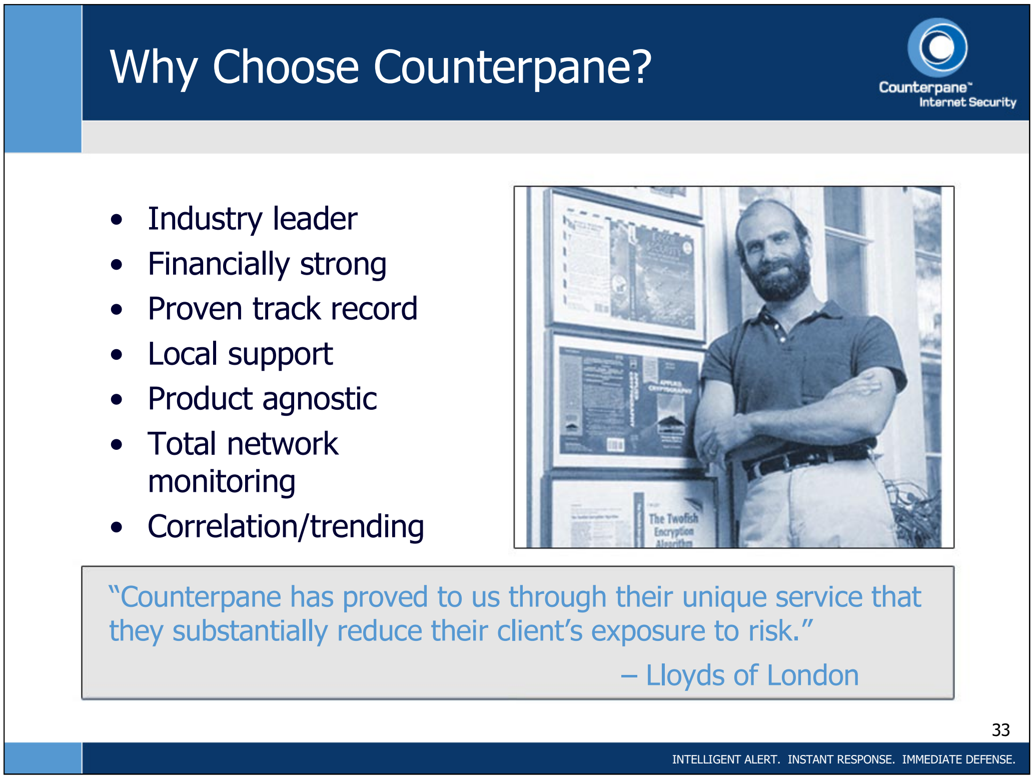
In any outsourcing decision that involves an ongoing relationship, the financial health of the outsourcer is critical. The last thing you want is to embark on a long-term medical treatment plan, only to have the hospital go out of business in the middle. Companies that entrusted their security management to Salinas and Pilot were left stranded when those companies went out of business. Companies that choose the wrong security consulting group will have the same problem. Look for companies that: 1) are leaders in their fields, 2) do one thing well, not those that try to do everything, and 3) have a history.

The Future of Outsourcing

Modern society is built around specialization; more tasks are outsourced today then ever before. We outsource fire and police services, government (that's what a representative democracy is), and food preparation. In general, we outsource things that have one of three characteristics: it's complex, important, or distasteful. In business we outsource tax preparation, payroll, and cleaning services. Outsourcing security is nothing new: all buildings hire another company to put guards in their lobbies, and every bank hires another company to drive its money around town.

Computer security is all three: complex, important, and distasteful. Its distastefulness comes from the difficulty, the drudgery, and the 3:00 a.m. alarms. Its complexity comes out of the intricacies of modern networks, the rate at which threats change and attacks improve, and the ever-evolving network services. Its importance comes from this fact of business today: companies have no choice but to open up their networks to the Internet.

Doctors and hospitals are the only way to get adequate medical care. Similarly, outsourcing is the only way to get adequate security on today's networks.


The Twofish Encryption Algorithm

Why Choose Counterpane?

- Industry leader
- Financially strong
- Proven track record
- Local support
- Product agnostic
- Total network monitoring
- Correlation/trending

"Counterpane has proved to us through their unique service that they substantially reduce their client's exposure to risk."

– Lloyds of London

33

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Scalability

Counterpane's Managed Security Monitoring was designed with scalability in mind. Our distributed architecture and automatic redundancy ensure that we can scale seamlessly and almost indefinitely.

Analysts: Counterpane has demonstrated that we can quickly hire and train new analysts. We are constantly hiring new analysts and bringing them up through the Counterpane ranks, and we know our methodology is scaleable.

Analyst consoles: Each analyst console is capable of monitoring about fifty Sentries. We currently have twenty analyst consoles in two SOCs, and are capable of adding more consoles at the existing SOCs or in a new SOC.

Socrates: The Socrates system is already fully redundant. The underlying third-party systems-an Oracle database and a Remedy trouble ticket system- are already used for distributed systems much larger than Counterpane's, and can easily scale.

SOC Architecture: We have built our SOC architecture to facilitate scalability and reliability. There are no bottlenecks or single points of failure. Everything can be replicated multiple times without any system degradation.

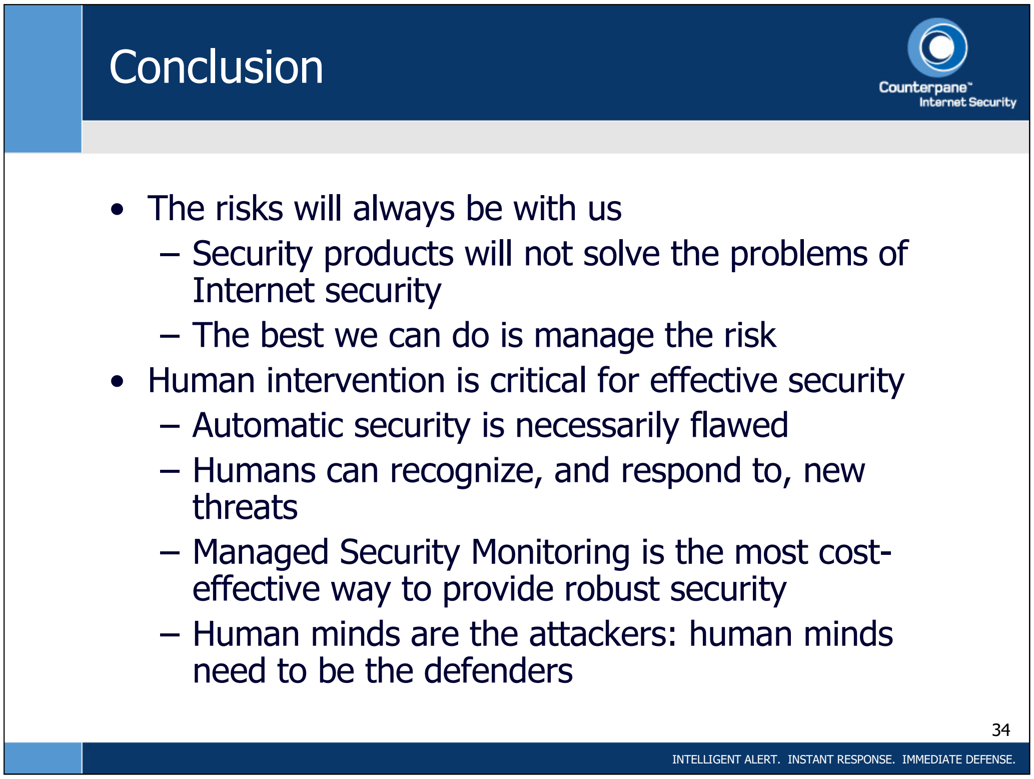
SOCs: Counterpane has demonstrated that we can build and staff a SOC, from a standing start, in four months. We have tested and debugged this process, and we can replicate it anywhere in the world.

SOC-Sentry Connectivity: The Sentries are designed to recognize multiple SOCs, and can automatically switch from one to the other. This capability ensures scalability.

SOC-Sentry Bandwidth: Since most of the event processing and analysis occurs on the Sentry, there is no bandwidth barrier to scalability. This is an important consideration; IDS monitoring companies are forced to send all events back to their SOC for analysis, consuming huge amounts of bandwidth in the process. Because Counterpane has built a distributed monitoring architecture, we do not have these constraints.

Sentry: Counterpane can easily install multiple Sentries if a customer location needs additional processing.

Our experience with Nimda demonstrates our scalability. During the first hours of Nimda, our Sentries saw a hundred-times increase in event volume. Both SOCs immediately increased capacity to support the additional alerts, and we brought up our third SOC within four hours once we saw the increasing activity. Nothing about Nimda had a damaging impact on the architecture. We could still see what we needed to, and alerted customers throughout accordingly. In short, Counterpane's MSM service can scale in ways no one else's can. We can monitor customers, large and small, around the globe. We continually build our monitoring capability in advance of demand to ensure that we can always serve our customers. On 1 January 2002, Counterpane's distributed architecture monitored alerts at a rate of 4000 per second, 14 million per hour, 10 billion per month, 120 billion per year. In one month, we see more events than anyone else has ever seen, ever, and this rate is steadily increasing as we bring more customers on line.



Conclusion

- The risks will always be with us
  - Security products will not solve the problems of Internet security
  - The best we can do is manage the risk
- Human intervention is critical for effective security
  - Automatic security is necessarily flawed
  - Humans can recognize, and respond to, new threats
  - Managed Security Monitoring is the most cost-effective way to provide robust security
  - Human minds are the attackers: human minds need to be the defenders

34

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Counterpane Internet Security, Inc.

Counterpane's Technology:

http://www.counterpane.com/technology.html

Customer Experiences:

http://www.counterpane.com/experiences.html

Key Benefits and Deliverables:

http://www.counterpane.com/keybenefits.html

Seven Questions You Should Ask Any MSM Vendor:

http://www.counterpane.com/questions.html

Counterpane Protected Service:

http://www.counterpane.com/protected.html

Counterpane today delivers Managed Security Monitoring to some of the most well-known corporations in e-commerce, finance, healthcare, hosting, insurance, manufacturing, pharmaceuticals, and transportation. The vast majority of our customers prefer not to be identified publicly, but here are a few of those who have consented to having their names appear in public: Abbot Labs, CareGroup Healthcare System, Corio, Currenix, Metratech, Nagrastar, Nationwide Insurance, NetSpend, OilSpace, Regence Group, and United Devices.

To see more current information about Counterpane's customers, visit:

http://www.counterpane.com/customers.html

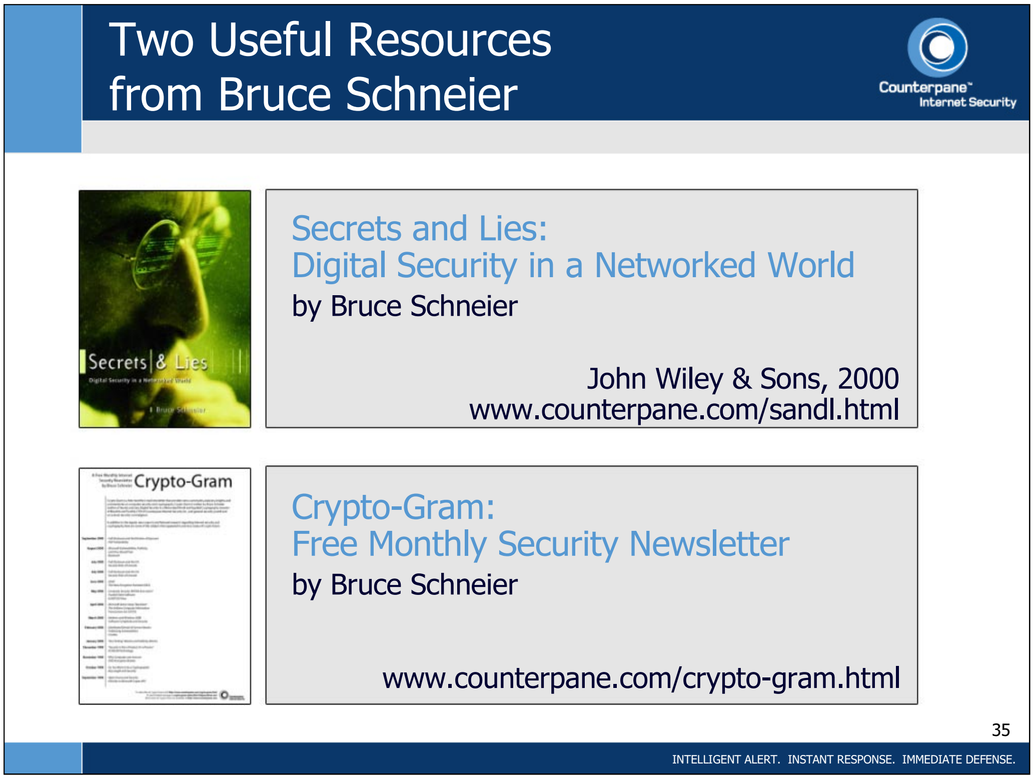
To read customer case studies and actual SOC war stories, visit:

http://www.counterpane.com/experiences.html

Giga Information Group, one of the industry's leading analysts, has published two short papers on Counterpane:

http://www.counterpane.com/giga2.pdf

http://www.counterpane.com/giga.pdf



Two Useful Resources from Bruce Schneier

Secrets and Lies:
Digital Security in a Networked World
by Bruce Schneier

John Wiley & Sons, 2000
www.counterpane.com/sandl.html

Crypto-Gram:
Free Monthly Security Newsletter
by Bruce Schneier

www.counterpane.com/crypto-gram.html

35

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Secrets & Lies
Crypto-Gram

Crypto-Gram, by Bruce Schneier

Crypto-Gram is a free monthly e-mail newsletter that provides news, summaries, analyses, insights, and commentaries on computer security and cryptography. In addition to the regular news reports regarding Internet security and cryptography, here are some of the subjects that appeared in previous issues of Crypto-Gram:

- The Security Patch Treadmill
- Hard-Drive-Embedded Copy Protection
- A Cyber UL?
- Voting and Technology
- Why Digital Signatures Are Not Signatures
- AES
- Full Disclosure and the Window of Exposure
- Bluetooth
- Full Disclosure and the CIA
- Microsoft SOAP
- Computer Security: Will We Ever Learn?
- ILOVEYOU Virus
- UCITA
- Software Complexity and Security
- Publicizing Vulnerabilities
- Insurance and the Future of Network Security
- Internet Voting vs. Large-Value e-Commerce
- Code Signing in Microsoft Windows
- Digital Safe-Deposit Boxes
- Microsoft Hack (the Company, not a Product)
- Semantic Attacks: The Third Wave of Network Attacks
- PGP Vulnerability
- Microsoft Vulnerabilities, Publicity, and Virus-Based Fixes
- Security Risks of Unicode
- The Data Encryption Standard (DES)
- Trusted Client Software
- Microsoft Active Setup “Backdoor”
- Kerberos and Windows 2000
- Distributed Denial-of-Service Attacks
- Cookies

To subscribe to Crypto-Gram, visit http://www.counterpane.com/crypto-gram.html

Or send a blank message to crypto-gram-subscribe@chaparraltree.com

Back issues of Crypto-Gram are available at http://www.counterpane.com

INTELLIGENT ALERT. INSTANT RESPONSE. IMMEDIATE DEFENSE.

Counterpane Internet Security, Inc.

19050 Pruneridge Ave.
Cupertino, CA 95014

1.888.710.8175
www.counterpane.com

Notes: