TechTarget | SearchNetworking

E-guide

PRO+ Content

Network Security 101

Your expert guide to securing the network as it gets more complex

In this e-guide

In this e-guide:

Securing the network is trickier than ever. While the threats are evolving and multiplying, the very the nature of the network is changing, too. No longer is it enough to lock down the in-house enterprise system: Employees now work from everywhere and on all sorts of devices, both company-owned and personal.

This essential guide gathers in one place the latest information and guidance to help you achieve the best network security possible for your enterprise. Learn about everything from network security best practices to the latest types of tools available to make your job at least a bit easier.

In this e-guide

Section 1: Best practices

Network security best practices

The best way to achieve network security is to practice good network-security habits right from the start. The articles collected here explore key obstacles to network security and the latest means for battling these security threats.

In this e-guide

Beyond the Page: Network security at the edge

David Strom, Contributor, SearchSecurity

Network security at many organizations has moved beyond "four walls." The traditional methods that used signature-based security technologies to lock down network perimeters to protect against threats from Internet connectivity and malicious traffic are no longer enough. The question for many enterprises now is what constitutes secure perimeter design in modern work environments? This Beyond the Page looks at enterprise strategies for network perimeter security and next-generation tools such as network access control, single sign-on, encryption certificates and more. Is the concept of the network perimeter dead or is it being redefined? Veteran technology journalist David Strom explores the issue from the outside in, including four ways to protect today's perimeter and six means to improve internal policy regarding personally owned devices.

Feature

Network security in the cloud and mobile era

Technological advances have forever broken the boundaries of the network perimeter, and security professionals have responded with new network-edge protection strategies. Strom examines four concrete ways today's

In this e-guide

infosec pros are protecting these "new" perimeters, approaches that range from a focus on the applications layer to single sign-on integration and encryption. The network edge is becoming ever more fluid, thanks to advanced attack methods and modern mobile technology; learn how the security pros interviewed in this article are coping with the situation.

Tech tip

Six ways to improve your BYOD policy

You can greatly improve security of your network by implementing a strong bring your own device policy. To create a BYOD policy that's effective requires a combination of securing physical devices, tightening up the user login process, securing the applications on personal devices, and controlling network access granted to the devices. Sometimes accomplishing all this takes more than just one security product. In this tip, Strom reviews policy-driven security controls and outlines the key questions security managers should ask vendors when evaluating their tools.

Next article

In this e-guide

Scour your enterprise with network security monitoring tools

Lisa Phifer, Owner, Core Competence Inc.

In the high-stakes, cat-and-mouse game of cybersecurity, the only real constant is change. The number of new threats is escalating, and the attack surface is growing, too. Businesses today rely more extensively than ever on Internet-connected devices, services and data -- from machine-to-machine communication and the Internet of Things (IoT), to bring your own devices (BYODs) and bring your own cloud (BYOC) applications.

One thing this tidal wave of new targets has in common? Their exposure to network-borne threats is 24/7. From Heartbleed to FREAK, criminals continually exploit low-hanging fruit by finding new bugs in widely deployed software and old gaps that resurface in new technologies.

Effectively spotting and stopping these evolving network threats requires not just vigilance, but new approaches. It's unrealistic to expect enterprise defenses to block all attacks or eliminate all vulnerabilities. Furthermore, manual threat assessment and intervention simply cannot scale to meet these challenges. Network security monitoring that is more pervasive, automated and intelligent is critical to improve situational awareness and drive timely threat response.

In this e-guide

The Importance of Network Threat Visibility

According to the Ponemon Institute's "2014 Cost of Cyber Crime: United States," the most costly cybercrimes are those caused by denial of service attacks, malicious insiders and malicious code, leading to 55% of all costs associated with cyberattacks. Not surprisingly, costs escalate when attacks are not resolved quickly. Participants in Ponemon's study reported the average time to resolve a cyberattack in 2014 was 45 days, at an average cost of $1,593,627 -- a 33% increase over 2013 cost and 32-day resolution. Worse, study participants reported that malicious insider attacks took on average more than 65 days to contain.

The increasing frequency, diversity and complexity of network-borne attacks is impeding threat resolution. Cisco's 2015 Annual Security Report found that criminals are getting better at using security gaps to conceal malicious activity; for example, moving beyond recently fixed Java bugs to use new Flash malware and Snowshoe IP distribution techniques (increasing spam by 250%) and exploiting the 56% of Open SSL installations still vulnerable to Heartbleed, and others, or enlisting end users as cybercrime accomplices.

In this era of BYOD, BYOC, IoT and more, achieving real-world security for business-essential connectivity requires more visibility into network traffic, assets and patterns. "By understanding how security technologies operate," Cisco's report concluded, "and what is normal (and not normal) in the IT environment, security teams can reduce their administrative workload while

In this e-guide

becoming more dynamic and accurate in identifying and responding to threats and adapting defenses."

Be aware of the risks

According to Gartner analyst Earl Perkins, speaking at the Gartner Security & Risk Management Summit in June 2015, advanced threat defense combines near-real-time monitoring, detection and analysis of network traffic, payload and endpoint behavior with network and endpoint forensics. More effective threat response begins with advanced security monitoring -- including awareness of user activities and the business resources they access, on-site and off. However, security professionals are also experiencing information overload. Advanced visibility therefore comes from more intelligent use of information through prioritization, baselining, analytics and more.

Perkins recommends deploying network security monitoring technologies based on risk. At a minimum, every enterprise should take fundamental steps, including properly segmenting networks and defending business assets with traditional network firewalls, intrusion prevention systems (IPS), secure Web gateways and endpoint protection tools. These defenses serve as sentries -- armed guards stationed at key entrances to ward off basic threats and sound alarm at the first sign of attack. For threat-tolerant businesses with low-risk, these fundamentals may be sufficient.

However, most organizations at risk will want to consider more advanced network security monitoring tools and capabilities such as next-generation

In this e-guide

and application firewalls, network access control (NAC), enterprise mobility management (EMM), and security information and event management (SIEM). These technologies go deeper by examining more traffic content or endpoint characteristics. They broaden visibility by monitoring more network elements, including mobile devices and activities. Ultimately, they can produce more actionable intelligence by knitting together disparate events into more cohesive threat alerts -- especially for advanced persistent threats that might otherwise be missed entirely.

Finally, risk-intolerant organizations may wish to go even further, using network and endpoint forensics to routinely record all activity, enabling look-back traffic, and payload and behavior analysis. Unlike real-time monitoring technologies, forensics tools focus on identifying past compromises -- but this can be important to spot, for example, those long-running insider attacks. Forensics can also help enterprises identify gaps in their defenses, enabling them to adapt and to better prevent future attacks.

Put Network Security Monitoring Tools to Work

To take advantage of new advanced network security monitoring tools, it can help to get a handle on industry advances and why new technologies and capabilities have emerged.

Let's start with that staple of network monitoring, the traditional network firewall. Single-function firewalls long ago morphed into unified threat management (UTM) platforms, which combine firewall, IPS, VPN, Web gateway, and antimalware capabilities. However, even UTMs tend to focus

In this e-guide

on network traffic inspection. When application payload is examined, it's for a specific reason such as blocking a blacklisted URL, content type or recognized malware.

In contrast, next-generation firewalls are application-aware. That is, they attempt to identify the application riding over a given traffic stream -- even an SSL-encrypted session -- and apply policies specific to that application and perhaps to the users, groups or roles. For example, a next-generation firewall isn't limited to blocking all traffic to Facebook. It can allow only marketing employees to post to Facebook, but not to play Facebook games. Or it can simply monitor how workers interact with Facebook and generate alerts when activity deviates from that baseline. This granularity is only possible because the firewall can identify applications and their features -- including new applications it will learn about in the future. Increasingly, next-generation firewalls are learning through machine-readable feeds that not only deliver new threat signatures but intelligence about new attacks and IPs, devices or users with bad reputations. This ability to *adapt and learn* is key to keeping up with new cyberthreats.

While intrusion prevention remains a cornerstone of network monitoring, it has expanded in several dimensions. First, as enterprise networks move from wired to wireless access, wireless IPS has become essential. At a minimum, enterprises can use rogue detection built into wireless LAN controllers. Risk-averse enterprises may invest in wireless IPS to scan the network 24/7 for threats, including some otherwise hidden IoT and unauthorized BYOD communication.

In this e-guide

Second, intrusion prevention now extends beyond the enterprise network to mobile devices. For example, EMMs can be used to routinely assess mobile device integrity, alerting administrators to jailbroken, rooted or malware-infected devices and automatically protect the enterprise by removing network connections or business applications from those devices. The ability to look beyond the traditional enterprise network edge is key to avoiding blind spots.

SIEM technologies have also evolved from simply aggregating and normalizing events produced by enterprise network-connected systems and applications; now it combs that data with contextual information about users, assets, threats and vulnerabilities to enable correlation and analysis. According to Gartner, SIEM deployment is growing, with breach detection now overcoming compliance as the primary driver. As a result, SIEM vendors have expanded capabilities that target breach detection, such as threat intelligence, anomaly detection and network-based activity monitoring -- for example, integrating NetFlow and packet capture analysis. SIEM not only helps enterprises pull monitored data together, but now it can intelligently sift through that haystack to pinpoint internal and external threats.

A new market segment has started to emerge: breach detection systems (BDS). These technologies are being driven by startups that are working to apply big data analytics to monitored information, profiling user- and device-behavior patterns to detect breaches and facilitate interactive investigation. According to NSS Labs, a BDS can identify pre-existing breaches as well as malware introduced through side-channel attacks -- but should be considered a "last line of defense against breaches that go undetected by current security technologies, or are unknown by these technologies." Risk-

intolerant enterprises that have tried other advanced security monitoring tools but are plagued by advanced, persistent threats may wish to investigate this new technology.

When attacks inevitably break through enterprise network defenses and evade real-time detection, another advanced monitoring tool can be helpful: network forensics appliances. Network forensics also analyzes monitored data, but in a different way, for a different purpose. Like a network DVR, these passive appliances record and catalog all ingress and egress traffic. By delivering exhaustive full-packet replay, analysis and visualization quickly, network forensics appliances support cybercrime investigation, evidence gathering, impact assessment and cleanup. Here, the idea is to avoid limitations associated with real-time monitoring -- that is, having to spot everything important right when it happens. Network forensics makes it possible to go back and take a second look, to find what other monitoring systems might have missed.

The Bottom Line

As we have seen, advanced network security monitoring cannot be accomplished through isolated static tools. Rather, monitoring must occur at many locations and levels through the enterprise network and beyond, create a comprehensive data set that an increasingly smart and dynamic collection of analysis tools then scours. Only in this way can we respond quickly and effectively to emerging cyberthreats that have learned how to fly under the traditional network radar.

In this e-guide

Postcards from the perimeter: Network security in the cloud and mobile era

David Strom, Contributor, SearchSecurity

With distributed workforces and mobile technologies, the network perimeter has evolved beyond the physical limits of most corporate campuses. The days when the perimeter was an actual boundary are a fond memory. Back then, firewalls did a decent job of protecting the network from outside threats, and intrusion prevention tools protected against insiders. But over time, the bad guys have gotten better: Spear phishing has made it easier to infiltrate malware, and poor password controls have made it easier to exfiltrate data. This means that the insiders are getting harder to detect, and IT assets are getting more distributed and harder to defend.

Complicating matters, today's data centers are no longer on-premises. As cloud and mobile technologies become the norm, the notion of a network edge no longer makes much sense. New network security models are required to define what the network perimeter is and how it can be defended.

CIOs and enterprise security managers are using different strategies to defend these "new" perimeters, as corporate data and applications travel on extended networks that are often fragmented. The borders between trusted internal infrastructure and external networks still exist, but the protection strategies and security policies around network applications, access control,

In this e-guide

identity and access management, and data security require new security models. Here we look at four network edge-protection strategies in use today: protecting the applications layer, using encryption certificates, integrating single sign-on technologies and building Web front-ends to legacy apps.

1. Provide application-layer protection.

While next-generation firewalls have been around for some time, what's new is how important their application awareness has become in defending the network edge. By focusing on the applications layer, enterprises can better keep track of potential security abuses because IT and security teams can quickly see who is using sensitive or restricted apps.

One way to do this is to develop your own custom network access software that works with firewalls and intrusion detection systems. This is what Tony Maro did as the CIO for medical records management firm EvriChart Inc., in White Sulphur Springs, W.Va.

"We have some custom firewall rules that only allow access to particular networks, based on the originating device. So, an unregistered PC will get an IP address on a guest network with only outside Internet access and nothing else. Or, conversely, a PC with personal health information will get internal access but no Internet connection," Maro says. "This allows for a lot more fine-grained control than simple vLANs. We also monitor our DHCP leases and notify our help desk whenever a new device shows up on that list."

In this e-guide

Another method is to incorporate real-time network traffic analysis. A number of vendors, including McAfee, Norse Corp., FireEye Inc., Cisco, Palo Alto Networks Inc. and Network Box Corp. use this analysis as part of their firewall and other protective devices.

2. Make proper use of encryption and digital certificates.

A second strategy is to deploy encryption and digital certificates widely as a means to hide traffic, strengthen access controls and prevent man-in-the-middle attacks. Some enterprises have come up with rather clever and inexpensive homegrown solutions, while others are making use of sophisticated network access control products such as MobileIAM from Extreme Networks Inc. that combine certificates with Radius directory servers to identify network endpoints.

"We use certificates for all of our access control because simple passwords are useless," says Bob Matsuoka, the CTO of New York-based CityMaps.com. The company found it needed more protection than a user name and password combination to its Web servers, and providing certificates meant they could encrypt the traffic across the Internet as well as strengthen their authentication dialogs. While this approach increases the complexity of Web application security for his developers and other end users, it also has been very solid.

In this e-guide

"Over the past three years we haven't any problems," Matsuoka says. One of the trade-offs is his company is still operating in startup mode. "You can have too much security when you are part of a startup, because you risk being late to market or impeding your code development."

Several vendors of classic two-factor tokens such as Vasco Data Security Inc. and xAuthentify are also entering this market by developing better certificate management tools that can secure individual transactions within an application. This could be useful for financial institutions that want to offer better protection and yet not something that is intrusive to their customers. Instead, these tools make use of native security inside the phone to sign particular encrypted data and create digital signatures of the transaction, all done transparently to the customer. To some extent, this is adding authentication to the actual application itself, which gets back to an application-layer protection strategy.

3. Use the cloud with single sign-on tools.

As the number of passwords and various cloud-based applications proliferates, enterprises need better security than just re-using the same tired passphrases on all of their connections. One initiative that seems to be gaining is the use of a cloud-based single sign-on (SSO) tool to automate and protect user identities. Numerous enterprises are deploying these tools to create complex, and in some cases unknown, passwords for their users.

SSO isn't something new: We have had these products for more than a decade. What is new is that several products combine both cloud-based

In this e-guide

software as a service logins with local desktop Windows logins, and add improved two-factor authentication and smoother federated identity integration.

Also helping is a wider adoption of the open standard *Security Assertion Markup Language*, which allows for automated sign-ons via exchanging XML information between websites. As a result, SSO is finding its way into a number of different arenas to help boost security, including BYOD, network access control and mobile device management tools.

Post Foods LLC in St. Louis, MO, is an adherent to SSO. The cereal maker uses Okta's security identity management and SSO service. Most of their corporate applications are connected through the Okta sign-in portal. Users are automatically provisioned on the service (they don't have to even know their individual passwords), so they are logged in effortlessly, yet still securely.

Brian Hofmeister, vice president of architecture and operations for parent company, Post Holdings, in St. Louis, says that the consumer goods company was able to offer the same collection of enterprise applications, across its entire corporation of diverse offerings quicker through the use of SSO and federated identities, and still keep the network secure.

4. Consider making legacy applications Web-based.

A few years ago the American Red Cross was one of the more conservative IT shops around. Most of its applications ran on its own mainframes or were

In this e-guide

installed on specially provisioned PCs that were under the thumb of the central IT organization based in Washington, D.C.

But then people started to bring their own devices along to staff the Red Cross' disaster response teams. The IT department started out trying to manage users' mobile devices -- and standardize on them. But within two or three months, the IT staff found the mobile vendors came out with newer versions, making their recommendations obsolete. Like many IT shops, the Red Cross found that the emergency response teams would rather use their own devices, and these devices would always be of more recent vintage, anyway. In the end, they realized that they had to change the way they delivered their applications to make them accessible from the Internet and migrate their applications to become more browser-based. The Red Cross still has its mainframe apps, just a different way to get to them. And their end users are happier because they don't have to tote around ancient laptops and smartphones, too.

By building a Web front-end to their mission-critical apps, the Red Cross was able to move security to inside the application itself and not depend on the physical device that was running the application.

Connections are made over SSL encryption so that data transferred from device to their mainframes is protected. And their IT staff no longer has to worry about obsolete smartphones and can focus on building and "webifying" other applications.

"You have to be able to adapt to the changing mobile environment," says John Crary, CIO for the American Red Cross. "It is moving rapidly.

In this e-guide

Businesses are going toward being more mobile-centric, and we need to be much quicker and much more adaptable."

Certainly, breaking traditional boundaries with these four strategies isn't the only way you can set up a more secure network edge. But by tying network security more closely to applications, certificates and transactions, you have a better chance at stopping the bad guys.

Next article

In this e-guide

Can behavioral detection improve enterprise network security?

Kevin Beaver, Principle Logic, LLC

I heard about a new security technology that leverages multifunction, multi-session behavioral detection and traffic analysis to improve network security. How is this type of technology different from traditional perimeter security, and is it something enterprises should consider implementing?

The Metaflows Security System (MSS), by Metaflows Inc., is designed to combat advanced malware in that it "detects and prevents cyberthreats using multiple collaborative intelligence sources at once, rather than using a traditional single-source, proprietary intelligence feed," according to the company's website. In essence, it looks for multiple characteristics of network hosts that could indicate an infection or related anomaly.

I'm not a product expert on every offering in the advanced malware space; however, I do know that certain technologies already in existence offer similar features. These include:

- Security information and event management technologies from vendors such as Intel or Splunk Inc.;
- Intrusion prevention system technologies from vendors such as Sourcefire (Cisco) or Extreme Networks Inc.; and

In this e-guide

- Advanced malware detection/prevention technologies from vendors such as FireEye Inc. or Damballa Inc.

However, Metaflows is different from these technologies as it uses what it refers to as "Multiple Session Correlation" to analyze what's mapped and scored against a malware infection lifecycle model to help confirm what is actually taking place and limit false positives.
Technologies such as MSS are wonderful because of how they leverage multiple technologies to look at the bigger picture. Such tools should certainly be part of the security controls of any enterprise network -- especially those on the larger end where complexity and lack of visibility prove to be challenging.

It's hard to argue against the reality of advanced malware attacks and the trouble they can bring to any sized business. If MSS and other similar technologies mean that organizations can move away from traditional antimalware and perimeter protection and towards more reasonable security controls, I'm all for them.

Next article

In this e-guide

IT's biggest challenge? Preventing a network breach

Jessica Scarpati

At a time when anyone from Anthem Inc. to the Internal Revenue Service to JP Morgan Chase is vulnerable to a network breach, it's no surprise that maintaining network security is a high priority for organizations around the globe.

Indeed, according to TechTarget's 2015 purchasing intentions survey, network security is the biggest challenge most enterprises say they face. More than half, or 56% of the 1,560 networking pros worldwide polled in the SearchNetworking study, identified it as their main hurdle. Network security was also the No. 1 networking priority for 43% of respondents and the top area of investment, up from the 31% who gave the same answer in 2013, the last time TechTarget measured purchasing intentions.

"Security is dominating network discussions today," said Zeus Kerravala, founder and principal analyst of ZK Research, who consulted for TechTarget on the survey. "I haven't seen security have this much momentum in a long time."

Gone are the days of lone wolf hackers merely looking to flaunt their skills or break into a network for fun. Data breaches are often carried out by organized crime or state interests, with purloined information advertised

In this e-guide

through flourishing online marketplaces where crooks sell sensitive data for profit. There were 2,122 confirmed data breaches in 2014, according to Verizon's 2015 Data Breach Investigations Report.

Thomas Holt, a criminal justice professor at Michigan State University, found in 2013 that stolen bank account information, on average, fetched $187.44 per account on the black market. A single "data dump," which typically includes a debit or credit card number along with some of the cardholder's personal information, was worth $102.60 on average. A card verification value -- the three- or four-digit security code on the back of credit cards -- went for an average of $26.21.

Multiply those prices by the millions of compromised accounts in even one large data breach and it's easy to see why this black market is thriving -- and why networking pros subsequently feel a greater sense of urgency to better protect their assets.

Vendors that didn't traditionally emphasize security in their networking are now eager to get in on the game, said Kerravala.

"Look at a company like Gigamon, who is a network management vendor historically. Most of their leads are coming in through security," Kerravala said. "You're going to see more and more of that, even with the wireless vendors trying to position themselves as security vendors."

The need to boost security permeates every angle of networking with 37% of respondents saying they plan to purchase some type of network security and threat detection product over the next 12 months. On the mobile front, 28% of respondents plan to buy security products to shore up their wireless

In this e-guide

LAN protection. And of the 171 respondents planning to buy routers this year, 36% said the move is driven by a need to integrate security in the wide area network.

But the efficacy of traditional network security products against today's threats is in question as end users' susceptibility to phishing scams and social engineering becomes a more attractive attack vector. Experts say this shift has put a greater emphasis on context-aware security and threat intelligence.

Networking trends

While network security remains the biggest area of focus for enterprises today, it isn't the only one networking pros are setting their sights on in the coming year. Among the most significant trends:

Enterprises hunger for bandwidth. The need for more bandwidth ranked as the second-biggest challenge this year, with 44% of respondents citing it as one of their main obstacles. When asked to identify their networking priorities for the next 12 months, 32% pointed to their plans to obtain additional bandwidth and telecom services.

Most networking budgets have been increasing. More than half of the survey respondents (52%) said they received a bigger networking budget this year, up from 42% in 2013. Among the remaining respondents from this year's crowd, 27% said their networking budgets were staying the same, while 14% didn't know and 7% said theirs had decreased.

In this e-guide

Three out of four not changing vendors. Respondents seem happy with their current suppliers, with 74% reporting no plans to switch out their networking vendors over the next year.

In WLAN, 802.11n still reigns. Despite the abundance of faster 802.11ac access points (APs) becoming commercially available, only 38% of respondents investing in their wireless LAN (WLAN) plan to deploy them over the next 12 months. APs using the previous wireless standard, 802.11n, will be deployed over the next year by 49% of respondents. When asked why they weren't upgrading to 11ac, the top reasons cited were expense (30%), no need for that much capacity (17%) and lack of an easy upgrade path from existing 11n APs (17%).

Network management remains fragmented. A third of respondents (33%) said they intend to purchase network monitoring and management software in the next 12 months. But despite pleas for a single pane of glass that would allow ubiquitous monitoring of all network components, that all-in-one platform doesn't yet exist, according to Kerravala. The lack of a de facto leader also complicates the market. "There are so many network management vendors that do things well [and] they get lumped into the same bucket, so it's difficult for customers to understand one tool versus the others," he said. Pricing models are also changing, resulting in increased traction for freemium models, which enable customers to use a vendor's app for free with limited functionality and/or for a limited time.

Data center is hot, but fabric education needed. The ballooning growth of east-west traffic is driving new demands for systems designed to support the flow of data traffic between data center servers. That said, organizations

In this e-guide

remain slow to deploy technologies such as fabrics and network functions virtualization (NFV) until they get more comfortable with the concept. "Fabrics are attractive because they make networks agile," Kerravala said. "But for companies not deploying them, it's because they don't know enough about them. I would argue that vendors haven't done a good job explaining what [a fabric] is and how it works." In a similar vein, Kerravala said enterprises are leery about NFV until they get more solid information. "There is a lack of knowledge out there," he said about the use of NFV. "Where we see traction is in the carrier space."

Next section

In this e-guide

Section 2: Access control

Network access control

The security landscape is changing fast, and a big part of achieving the best network security possible is controlling who accesses the network. This section explores the challenges for controlling both on-site and remote access, the impact of recent developments like the Internet of Things, network access and new means and methods like behavior analysis.

In this e-guide

Secure remote access? Security-related remote access problems abound

Eric Parizo, Senior Analyst

An attacker seeking to penetrate an enterprise's defenses typically has many "easy" options to choose from: unpatched Windows machines, website cross-site scripting flaws, or social engineering against employees.

So it's impossible to ignore the irony that enterprise remote access services -- technologies constructed to provide authorized employees and partners with managed, secure remote access to corporate networks and data -- have become one of the most exploited IT resources in use today.

For the information security industry, it's disheartening. Many enterprises, large and small, have made huge investments in remote access services, but recent findings suggest these technologies come with a variety of inherent problems and few easy answers.

The most recent and perhaps most powerful evidence of remote access problems comes in the 2012 Verizon Data Breach Investigations Report, the industry bellwether for data breach trends. Verizon found that in 2011, remote access services were involved in 88% of all hacking breaches in its data set, and of all the reported incidents involving malware last year, compromised remote access paved the way for infections 95% of the time.

In this e-guide

In the DBIR, Verizon references remote access services such as Virtual Network Computing (VNC) and Remote Desktop Protocol (RDP), but the remote access security problem is far broader. Consider the following:

- Many enterprises permit (or fail to regulate) the use of third-party file storage services to facilitate remote access to data, but when files end up in cloud-based repositories, enterprises lose control. When Dropbox left user accounts wide open last June without realizing it, it's likely many ad-hoc enterprise data repositories were exposed.
- Screen sharing and remote administration software weaknesses are an increasing concern. A 2011 report from Trustwave found remote management software was one of the most commonly used attack vectors. And good luck to anyone using Symantec Corp.'s Norton pcAnywhere software; the ambiguous technical document released last month does little to assuage fears that the product has been completely compromised in the wake of Big Yellow's 2006 source code breach. Plus, recent research by Rapid7 CSO HD Moore found thousands of systems using pcAnywhere with open ports that could be accessed by an attacker.
- VPNs risks can't be ignored either. Trustwave also found a VPN or similar remote access method was exploited in more than half of the data breaches it investigated last year. Few though were as devastating and public as the Gucci network attack, in which a former employee used a VPN connection to wreak network havoc from afar.

Insecure or insecurely used remote access technologies – mechanisms that most security teams assume pose little risk – in reality offer an abundance of options for attackers to infiltrate enterprises.

In this e-guide

"The biggest concern is that attackers will exploit that remote access connection as a jumping-off point, a hop along the way, to get deeper into an organization," said Chris Hopen, co-founder of TappIn, a secure file-sharing vendor. Few understand remote access better than Hopen, one of the inventors of the SSL VPN and CTO and co-founder of VPN pioneer Aventail, which was acquired in 2007 by SonicWall.

What's confounding, said Hopen, is that the largest underlying problem with remote access technologies isn't with remote access; it's poor identity validation and weak authentication.

"There have been so many purported solutions to this end-user identity and authentication challenge over the years, with millions and millions of dollars spent," Hopen said. "We've never found a solution people could live with that's cost-effective and adds an enhanced layer of security over traditional passwords. To me, that kicks me in the stomach."

The problem is more acutely felt in small and midsize businesses, especially those that operate point-of-sale (PoS) systems. As Verizon's 2012 DBIR points out, SMBs have proven highly vulnerable because they commonly outsource PoS management to third-party solution providers, many of which fail to properly secure the remote access technologies they use to "help" their customers.

"The message I've been trying to get out there is, if you're a VAR or reseller providing that service, it's to your competitive advantage to have security be in the upper tier of your priorities," said Ed Moyle, co-founder of Amherst, N.H.-based consultancy SecurityCurve and a former PCI DSS QSA.

In this e-guide

He said this year's DBIR should serve as an opportunity for solution providers to reach out to their SMB customers to talk about these kinds of security problems and ways to improve them.

Moyle stressed security fundamentals to keep remote access usage in check, such as monitoring for remote access system traffic that isn't being transmitted over HTTP, and restricting admin rights on workstations. "It's not a panacea," Moyle said. "It's something everyone already knows about, but few actually do it."

Hopen said organizations should consider emerging security products that offer enhanced forensic analysis and directory and data monitoring capabilities to better detect when remote access technologies are being used in support of an attack. However, even with better supplemental security products, he said enterprises must shift more of the responsibility for proper use of remote access products to their end users.

"You've got to have better solutions to drive up productivity while mitigating and managing risk," Hopen said, "but I think end users who are given access to these services are a big part of the equation in enhancing and maintaining trust."

Next article

In this e-guide

Three reasons to deploy network access control products

Rob Shapland, Senior Penetration Tester, First Base Technologies LLP

Network access control (NAC) is a system that allows organizations to restrict access to resources on their internal network. Primarily used by financial institutions, corporations with high security requirements and some universities, NAC has (so far) failed to become the mainstream security product some thought it would when the technology first entered the market at the end of 2003.

Times are changing, however.

Thanks to the advent of bring your own device (BYOD) and the integration of NAC technology into mobile device management (MDM) products, NAC is enjoying a rise in popularity among enterprises in general. That's because a growing number of organizations are evaluating NAC as a useful IT security tool to better control device access to their networks.

Large organizations are the primary group showing an increased demand for NAC. This is due to the unique demands enterprises have in regards to number of employees and granting access to contractors, visitors and third-party suppliers. As awareness of the risk of breaches associated with these groups grows, so too does the demand for NAC to help mitigate the risk. Most NAC vendors are also reporting an increase in demand in the small and

In this e-guide

medium-sized enterprise (SME) market. This has largely been driven by media reports of breaches and the potential reputational damage they engender.

However, NAC is an expensive investment, particularly for SMEs, so organizations must consider whether it will provide a tangible security benefit before deciding to purchase network access control products. It is especially important to assess the risk to the organization from BYOD, weak access permissions and advanced persistent threats (APT).

NAC scenario #1: BYOD threats

BYOD is the key reason NAC is increasingly becoming an in-demand technology. That's because securely handling mobile devices is a key concern for CISOs tasked with providing secure network access with minimal disruption to end users.

As the line between personal and professional time blurs, end users are demanding to use not just corporate-owned devices (smartphones, tablets, laptops, among others.), but personal ones for business as well. This greatly complicates endpoint and network security for organizations, which -- meanwhile -- need to support not just employees connecting devices to the network, but devices from third parties (e.g., visitors, partners and contractors) as well.

There are hundreds of combinations of device type, model and operating system versions out there today; and mobile devices can be configured in

In this e-guide

innumerable ways with a vast selection of installed apps. Personal devices, meanwhile, generally do not have enterprise-level MDM and antivirus products installed. Users quite commonly disable basic security settings, or install apps that appear to be genuine but may actually perform actions that compromise the security of the device.

All of this creates a unique challenge for organizations regarding how to allow these devices to connect and not compromise the security of the network; the more devices that connect, the greater the risk that the network can be compromised. Mobile devices, meanwhile, are increasingly being targeted by criminals, and apps containing malware have become a popular attack vector.

This is where NAC can play a vital role -- the top NAC products on the market today support Apple iOS, Android and Windows devices -- in automatically identifying devices as they connect to the network, and providing access that does not potentially compromise security. For example, when a personal mobile device connects, it can be granted access only to the Internet and not to any corporate resources.

NAC scenario #2: Delivering role-based network access

While NAC is generally thought of as a security technology that either allows or denies access to the network, one of the major advantages of it is the ability to deliver network access on a granular basis. This can be integrated

In this e-guide

with Active Directory controls to provide network access only to areas of the network that allow the particular owner of the device to perform their job role.

As most IT managers are aware, managing both Active Directory group membership and network share permissions in a large network is an often insurmountable task, and inevitably leads to excessive network permissions. Being able to manage this centrally through a NAC product can allow greater control and flexibility for delivering access to shared folders.

For example, on most internal network penetration tests I've been involved in, weak controls on network shares are a key vulnerability that NAC products would have gone a long way toward solving. They either directly provide access to personally identifiable information or provide access to data that allows further enumeration of network resources. In one test, a misconfigured IT share allowed access to passwords for a number of key databases that contained customer names, addresses, dates of birth and payment card details. NAC technology would have mitigated the risk posed to this data.

NAC scenario #3: Reduce the risk from APTs

Although NAC does not provide functions that directly detect and thwart APTs -- malicious software that establishes remote, persistent access to a network to extract data in a stealthy manner over a period of time to limit the risk of detection -- it can stop the source of the threat from connecting to the network. Some NAC systems even integrate with APT detection

In this e-guide

products (such as FireEye), and automatically isolate affected systems before attackers can further access the network.

Using the famous example of the attacks against Target in 2013, the original infection occurred when a third-party vendor that sold heating and air conditioning connected to Target's IT network. Hackers targeted the third party, whose connection was in turn used to attack and exploit Target's network.

NAC would have made it possible to automatically restrict access to the Target network by the HVAC vendor, thereby restricting access that the APT had to corporate data and resources. This would make it much more difficult for the attack to have the same level of impact it had, saving Target a lot of money and both the retail behemoth and its customers a ton of hassle.

Key questions to ask before deploying NAC products

NAC is not suitable for all businesses. The larger an organization -- and therefore the more devices that will connect to the network -- the more useful network access control products will be. That's why it is important to not just understand the use cases for NAC technology outlined above, but to also ask a few important questions when deciding whether or not to deploy NAC products:

In this e-guide

- Do I know how many devices are connected to my network? What they are and who owns them?

If you don't know the answers to all these questions, then an organization probably feels like it has little control over what is already connected to its network, and what will be connecting in the future. In this case, NAC is strongly worth considering, as it will provide visibility to existing infrastructure and any new devices connecting to the network.

- Who will be looking at the alerts generated by NAC?

The organization needs IT staff capable of interpreting these alerts and ensuring that network access is delivered securely but with minimum disruption to legitimate users. Bear in mind that this may be a full-time job dependent on how many endpoints are being managed by the NAC system. At the very least, the IT team will need to be assigned specific time for monitoring alerts generated by the NAC system.

- Do I feel I have control over the data leaving my network?

Devices connecting to the network are obviously one of the key ways that data then leaves the network. If an organization is concerned about what data is being removed from the network -- and specifically what type of data -- NAC could help deliver network access to only the data required for the specific purpose a user is connecting. In this way, if a malicious user accesses the network, the NAC system would restrict their access, limiting the damage done by the compromise.

In this e-guide

- Do I have current security systems that would need to integrate with NAC?

Consider what security systems are already present on the network. Are these being used effectively, or are they just white noise? If an organization chooses to implement NAC, it should ensure it integrates with, for example, its MDM or security information and event management (SIEM) products. This will save the additional overhead of managing different IT security systems on separate platforms.

- Does the business need the ability to scale up deployment?

NAC products are often sold on a per-endpoint basis. Organizations will therefore need to consider the cost of adding more endpoint licenses as its infrastructure expands. For example, say an organization of 1,000 endpoints purchases a NAC product. However, because NAC licensing is delivered on a per-endpoint basis, if the organization expands greatly to 5,000 endpoints, the cost of the NAC product will increase dramatically as well.

Obstacles to NAC product deployment

Before deploying network access control products, consider the following obstacles:

1. Ensure there is sufficient time available to monitor alerts. Without monitoring and interpretation of alerts, the data provided by the system can

In this e-guide

be at best wasted and -- at worst -- disrupted (if network access is blocked for a user that requires it).

2. Look at the connections into the organization's network. Do users connect via SSL VPN, or over a product such as Citrix? Ensure the NAC system integrates with the systems already established on the network or it won't work to full effect.

Choosing to implement NAC can drastically improve an organization's network security posture by allowing for greater control over what devices are accessing the network, and what they are granted access to. By effectively sandboxing untrusted parties (such as visitors or third parties) into protected areas of the network, the risk of an intentional or accidental breach can be reduced.

Consider whether the main benefits of NAC -- such as greater control over BYOD, more granular access to network shares and better protection against APTs -- is worth the investment. Take into account that implementing NAC not only requires upfront expenditure, it also entails ongoing investment in the form of additional licenses, training, monitoring of the NAC system and responding to alerts.

And, don't forget, NAC also needs to work harmoniously with existing IT security systems. A number of network access control products integrate directly with existing MDM or SIEM systems, which have central management consoles, and reduce costs associated with administration and training.

In this e-guide

The next article in this series will outline the criteria organizations should consider when looking to procure a NAC product.

Next article

In this e-guide

NAC tools evolve to help enterprises with IoT endpoints

Gina Narcisi, Former Senior News Writer

Network access control tools that used to manage only desktops and laptops are evolving into systems for protecting networks from new security threats brought on by the increasing number of Internet of Things endpoints and employees using their own mobile devices for work.

With the variety of devices connecting to networks expanding, network access control (NAC) technology is becoming a new category called endpoint visibility, access and security (EVAS), Cisco said in its recently released Annual Security Report.

The evolution has reenergized the NAC market, which has been stagnant for years. In 2014, NAC sales rose to $552 million from $399 million in 2013, according to analyst firm Frost and Sullivan. The increase is due to the advantages EVAS tools bring to enterprises.

How EVAS works

The improvements include dropping the installation of code snippets, or agents, that establish communications between traditional NAC systems and each endpoint. This makes EVAS tools better suited for emerging

In this e-guide

trends like the Internet of Things (IoT), which will expand the assortment of endpoints to include any Internet-enabled device, such as printers, sensors and even medical monitoring systems.

"Any device that interacts with your network has the potential to cause harm or have malicious capabilities," said John Pironti, president of consulting firm IP Architects LLC.

EVAS tools from companies like ForeScout Technologies, Aruba Networks and Cisco gather endpoint data from multiple sources, including switches, active directory, and endpoint security systems in a single appliance. This approach gives enterprises more visibility into devices on the network. It lets companies gather contextual data and spot anomalies that could indicate malware or an unauthorized person trying to log in, experts said. In addition, EVAS systems profile data traffic at a granular level in real-time to monitor whether device activity is within corporate policies.

"A device could have malware injected onto it after it's already connected to the network, and it wouldn't be reevaluated [in traditional NAC] until it disconnects and tries to reconnect to the network," Pironti said. "Now, NAC is about more granularity and constant monitoring."

EVAS tools are particularly useful to enterprises that need to monitor much more than traditional PCs and mobile devices. Unlike traditional NAC tools, EVAS technology is not dependent on the operating system running on the endpoint. As a result, the systems can be used to monitor traffic from manufacturing equipment and industrial control systems, network engineer and blogger Nick Buraglio said.

In this e-guide

EVAS shortcomings

Along with the improvements they bring to endpoint security, EVAS tools also carry weaknesses. They lack a core universal feature set that experts say should include asset management, role-based access and secure guest-network access.

The tools should also include features to help companies monitor compliance with legal mandates and government regulations, said Joe Schumacher, senior security consultant at Neohapsis Inc., a security consulting company now owned by Cisco.

In recent years, vendors like Cisco, Aruba and Aerohive have scooped up NAC players, integrating their technology into wireless portfolios. While this has left enterprises with fewer standalone NAC vendors to choose from, the market consolidation has made it easier to work with only one vendor for deploying and maintaining the technology.

"Most enterprises are going to start with [EVAS] for wireless devices anyway, and then they can migrate over to wired [endpoints]," Pironti said.

Next article

In this e-guide

Advanced threat protection: Behavior-profiling network communications

Sally Johnson

Advanced threat protection technology uses behavior profiling to study enterprise network communications and detect sophisticated cyberattacks.

Malicious hackers have become so skilled at evading traditional signature-based network security that it's critical to detect and stop advanced malware as quickly as possible to minimize the risks of a full-blown breach.

Vendors such as FireEye, Damballa and RSA NetWitness have developed next-generation security technologies that profile normal enterprise network communications versus abnormal communications to detect the presence of advanced malware and infections.

What is an advanced threat?

Imagine that a criminal has a key to your house and can go inside without your knowledge. Advanced threats target enterprises in a similar way, in the sense that they're infections inside a network. And the attacker's goal is to steal data and evade detection.

In this e-guide

"The real risk to an enterprise is that an attacker outside the network is able to control infected devices in your network -- without your knowledge," said Stephen Newman, vice president of products at Damballa. "That's the general concept of the advanced threat, but there are varying degrees of who the attacker in control of the device might be and what they may want to do with their access to your data and network."

Malware can be slipped in using many techniques, but attackers generally target the path of least resistance. All those ridiculous emails you get, especially at work, with horrible misspellings and *Viagra* somewhere in the subject line are targeted malware intended to fly under the radar and get you to click on a link.

"As firewalls and IPS were made stronger in the network, bad guys kept coming up with more ways to evade detection," said Greg Young, Gartner research VP and lead analyst for network security. "Firewalls and IPS have to run at wire speed and can't inspect executables or related content, so occasionally that kind of malware slips through."

How can advanced threat protection find malware?

Advanced malware can give itself away, because it must use the network to communicate with its command and control system.

"Malware shows weird behavior by sniffing around on the network," explained Rob Rachwald, senior director of research at FireEye Inc. "That's not normal network behavior. Malware also needs initiate and perform a

In this e-guide

'callback' to the attacker -- essentially picking up the phone from inside a trusted network and establishing a connection by dialing out."

Studying network communications can reveal unusual behavior and infected devices as they're acting. "You can discover a lot of these hidden infections in your network based on their network communications," said Newman. "We can zero in and pinpoint infected devices -- even though we may never see the malware or the infection vector."

Many enterprises realized that their security solutions today, which are predominantly prevention-based, aren't foolproof. "Infections are going to happen. So it helps to have techniques and automated solutions that can unearth and discover infections hidden inside their networks," said Newman.

By reducing the time between infection and detection, you can greatly reduce the odds of a full-blown security breach.

Advanced threat protection: Behavioral analysis tools study network activity

Since many forms of malware exhibit distinctly nonhuman behavior on the network, behavior analysis tools are essential for advanced threat protection.

From an analytic perspective, it's extremely important to look beyond signatures to behavior. "Signatures only give you insight into a slice of time, whereas behaviors provide much more in the way of nuance associated with

In this e-guide

an attack vector," explained Will Gragido, senior manager, RSA FirstWatch advanced research intelligence at RSA NetWitness. "We spend a lot of time conducting analysis on attackers, as well as on malicious code and content. We're zeroing in on their behavioral patterns as well as what they're actually doing."

When a human accesses a database, they do it at human scale with a mouse and keyboard. If malware is doing accessing the database, it's very automated, fast, with high-volume click rates. "Nothing about it looks or smells human," said FireEye's Rachwald. "But we're also starting to see attackers create malware that acts more human to evade detection."

Once suspicious activity is identified, it's critical to look at where the malware is communicating to, the content of the communications and the overall behavior of the device's communication.

Then a virtual version of the laptop or device suspected of having an infection can be created to check the behavior of emails and other files.

"We can take a copy of the file and run it in our dynamic analysis engines, in our 'sandbox' virtual environments to capture all of the network communications," explained Damballa's Newman. "We buffer and store all the communications the device is making. If there's a statistical match between the network communications when we ran it in the sandbox and on the device it was headed toward, we can determine whether that device is infected or not."

At the end of the day, a human element plays the strongest role in the process of advanced threat protection. Enterprises need security analysts

equipped with advanced tools and training to identify threats the technology flags, according to RSA's Gragido.

Extra layer of security

Although everyone is subject to an attack, not everyone can afford an extra security product or spare the people needed to manage it.

"To date, we've seen the most security aggressive companies with lots of staff, who are forward-leaning on managing their security, pursue this technology," Young said. "But many enterprises can't afford extra spending in security right now or have someone spend extra hours doing the monitoring and analysis. It's a great technology and if you have the resources, investigate it."

Many enterprises, 25%, have a firewall only and don't have an IPS, according to Gartner data. "Before the really advanced technology, enterprises need to ensure they're able to deal with the bulk of attacks first by using a firewall and IPS," Young said.

Enterprises must also instrument their advanced threat protection systems properly.

"Advanced threat protection can only protect the network connections it's attached to. While the technology can be put in-line, enterprises tend to use it on a SPAN port on a switch to mirror traffic coming from the public Internet to the device," said John Kindervag, Forrester principal analyst

In this e-guide

serving security and risk professionals. "But malware can also come through other connections, such as VPN, wireless and WAN. Protecting all these points of ingress can be a challenge for enterprises."

Next section

In this e-guide

Section 3: Intrusion detection

Network intrusion detection

A key product to keep watch over network security is an intrusion detection system (IDS). It sets off an alarm when there is a security breach, violation of company network security policy or some other indication that there's a security issue with the network. Read on to learn about the benefits and best uses for an IDS and how to select one.

In this e-guide

When is a breach detection system better than an IDS or NGFW?

Kevin Beaver

How would you describe the difference between a breach-detection system and a traditional intrusion detection/prevention system or next-generation firewall, particularly from the perspective of how each type of device interacts with network traffic? In which enterprise settings would a breach-detection system be more appropriate to leverage?

There's definitely a difference between traditional network security controls such as intrusion prevention systems or next-generation firewalls and actual breach detection. The former security controls can provide information and insight (oftentimes too much) into what's taking place on the network such as network scans, denial-of-service attacks and blocked intrusions. Breach detection systems can go a step further and actually confirm that a breach has occurred by using things like heuristics, traffic analysis and predefined security policies.

The interesting thing I have found over the years is that many network admins and even executives that are privy to what's happening on the network are quick to quote how many times their network is attacked or "hacked" every single day. It's usually a number in the thousands or tens of thousands range. However, this does not paint an accurate picture of actual information risk. In the end, what matters the most is actual

In this e-guide

detection/confirmation of security breaches and, of course, the prevention of such incidents.

It seems that breach detection is the new "cybersecurity" -- yet another vendor-born rebranding to stir up interest in the market. There's no doubt to the validity of "response is the new prevention" approach to breach detection. I'm just not convinced it's another technology we must layer on to fix our security woes, especially given how much we're overlooking the simple stuff.

When it comes to deciding where a breach detection system may be appropriate to deploy (and likely used in conjunction with an IPS or NGFW), I suggest:

1. In complex IT environments, namely large enterprise business and government agencies; and
2. Small and medium-sized environments where little to no security technologies are in place to detect such security incidents.

In the end, the enterprise that blocks all attacks is not the one that wins because that's an impossible feat. Instead, the enterprise that wins is the one that has a technical and operational environment that facilitates the prompt response to security breaches to help minimize the impact to the organization,

Next article

In this e-guide

Using intrusion detection systems for incident prevention, improving ROI

Bill Hayes

Intrusion detection and prevention system offerings are effective at stopping many of today's attacks, both at the network perimeter and on internal network segments. These extra sets of eyes lead to a reduction in data loss and related collateral damage to the organization, both in money and in reputation.

However, the effectiveness of this new light in dark places only works if there is sufficient manpower and training. For organizations that lack those resources, managed security services can provide trained analysts able to recognize network-based attacks. Organizations should realize that intrusion detection and prevention system (IDS/IPS) training at some level is required to be able to interpret and act on reported events.

The business benefits of using IDS/IPS technologies fall in several categories, such as identifying the number and type of security incidents; preventing security events from becoming security incidents; protecting vulnerable assets; improving the ability to identify network devices, their operating systems and software; and using acquired information to meet various regulatory requirements.

Let's explore each category in depth.

In this e-guide

Identifying security incidents

While the logs from a firewall show you the IP addresses and ports used between two hosts, IDS/IPS technologies not only show those, but also can be tuned to specific content in network packets. For instance, they can identify compromised endpoint devices as they report to botnet controllers and can identify distributed denial-of-service attacks. Modern IDS/IPS sensors can help you quantify the number and types of attacks your organization is facing and thus help it alter existing security controls or employ new ones, address host and network device configuration problems and identify software bugs. The metrics gained can be used in ongoing risk assessments.

Security incident prevention

IDS/IPS technology can both report on security incidents and prevent them from occurring by disrupting communication between attackers and targets. Modern sensors are able to take the data provided in network packets and examine it within the context of the supported protocol. For instance, HTTP protocol attacks such as cross-site scripting can be detected and blocked, as can SQL injection attacks. Additionally, IDS/IPS sensors can look for anomalous behavior -- such as unexpected outbound traffic -- and block it.

In this e-guide

Protecting vulnerable assets

IDS/IPS vendors have touted the ability of their products to be "virtual patches" for known software vulnerabilities. This allows organizations to block attacks until software can be patched without disrupting business processes and the attendant costs in replacing systems and software until patches can be fielded. The ability to identify patch levels also can be used for automated vulnerability assessments and gauging patch deployments.

Identifying network devices and hosts

IDS/IPS sensors can be used passively to detect the presence of network devices and hosts. Based on the data within the network packets, they can in real time -- and with a good degree of certainty -- identify operating systems and services offered by a host or network device. This helps eliminate a good deal of manual work in determining how many systems are available and their current configurations. In addition to helping automate hardware inventories, IDS/IPS sensors can be used to identify rogue devices, such as unauthorized hosts, rogue wireless access points and hot spots.

In this e-guide

Leveraging information gained to meet regulatory requirements

Since IDS/IPS technologies give an organization greater insight into its network and connected resources, you can more easily meet regulatory mandates. For instance, PCI DSS 1.1.6 "documentation and business justification for use of all services, protocols, and ports allowed" can be researched using reports gleaned from IDS/IPS logs.

Improve ROI

Some improved efficiencies and attendant lower labor costs have been identified above. In addition, an organization, using its latest risk assessment, can also determine how much of a return on investment (ROI) IDS/IPS may provide if that system reduces or eliminates either (a) a denial or degradation of Internet service and/or internal network service (including the associated business ramifications of network, application or service downtime), or (b) a security breach involving the direct loss of sensitive customer data or intellectual property.

Next article

In this e-guide

Seven criteria for purchasing a wireless intrusion prevention system

George Hulme, Business and technology writer

When organizations get serious about protecting their wireless networks, selecting the right wireless intrusion prevention system (WIPS) isn't a decision that comes out of thin air. There is a lot to consider when buying a WIPS, such as whether the WIPS functionality built into the organization's access points (APs) provides enough wireless security, or if -- as is often the case -- those abilities just aren't comprehensive enough. Taking the time to select the right dedicated WIPS for the job pays off significantly in risk reduction and improved manageability.

When starting to investigate a WIPS purchase, it is important to become familiar with the evaluation criteria for comparing and contrasting WIPS products; everything from cost to how the devices will be managed need to be taken under careful consideration. The more an organization knows about what it is looking for in a WIPS, the more likely it will be to pick a wireless security system that meets its particular needs and wireless environment.

In this e-guide

WIPS criteria #1: Device management

It's hard, if not impossible, to secure what an organization can't manage. So it is very important to carefully look at how well the WIPs software enables the management of sensors, maps the wireless network and AP locations, and makes it easy to send out updates, modify policies or limit access (or even segment portions) of a network under attack. Good management software should also make it easy to set granular policies.

Not only does adequate device management make it straightforward to set, change and monitor policies, it also helps to strengthen security through making swift and necessary adjustments to policies when necessary, as well as helps to keep ongoing operational costs low. Unfortunately, this is an area many businesses overlook, and they end up lacking the ability to centrally manage their access points.

Don't become one of those organizations. Centralized management ensures security and infrastructure teams know where authorized APs exist, and can quickly spot when systems are under attack, or when rogue APs arise.

WIPS criteria #2: Attack discovery

Any time an enterprise establishes barriers or builds walls, someone is going to try -- and will all too often succeed in -- circumventing them. This could be as non-threatening as a user installing a rogue AP for unfettered Internet

In this e-guide

access in the office, to malicious denial-of-service (DoS) attacks launched at network availability. It's also important that organizations know what classes of attacks any prospective WIPS product purports to defend against.

These include, for example, in addition to the ability to spot and block attack types such as spoofing, rogue connections and the aforementioned DoS attacks, as well as the detection of encryption cracking tools and so on.

WIPS criteria #3: Policy compliance

In addition to security risks, it's also important that regulatory compliance risks associated with APs and wireless networks be managed by WIPS. Typically, these controls are an extension of security efforts, but the more granularly the WIPS can report on the settings and configurations of the enterprise Aps -- as well as the access control policies in place -- the better. An example would be reporting on what administrators have access to which APs and which users have access to the wireless network.

WIPS criteria #4: Forensics data

Like all of security devices, WIPS amass a trove of data that will need to be analyzed. This data includes, but isn't limited to, access logs, times of access and who accessed the wireless network.

In this e-guide

Carefully evaluate how the WIPS management software helps extract insight from all this data. How are reports displayed, are they customizable? What analysis tools are made available?

WIPS criteria #5: Attack defense

Just as is the case with traditional prevention and detection systems, there are many instances when a WIPS is run in "monitor" mode (as an attack detection and alerting device, rather than blocking attacks in-line). How well devices identify attacks and issue alerts needs to be investigated when evaluating WIPS products. Examples would be few false positives (issuing alerts for attacks that are not actually occurring) or false negatives (missing attacks altogether).

However, since we are discussing the procuring of WIPS devices, if a WIPS can actually proactively block attacks without disrupting legitimate traffic, all the better. This makes the ability to tune the prevention aspect of WIPS essential.

For example, if a worm starts scanning an organization's network, a wireless intrusion prevention system could allow for the disconnection of infected endpoints. Or, if a subnet is infected, a WIPS could segment it from the core network until malware infections or compromised systems can be cleaned. Be sure to test these capabilities on non-production networks for all WIPSes being considered.

In this e-guide

WIPS criteria #6: Performance

On large and -- especially -- mission-critical networks, scalability and high availability matter. Make sure the WIPS high-availability capabilities meet the needs of the enterprise. For example, as the business grows, organizations will want to easily grow its WIPS defenses; or, in the event of a device failure, it will want to smoothly failover to a redundant network equipped with a redundant WIPS device so its wireless systems are always protected. Relatedly, be sure to ask WIPS vendors how failovers and loss of network access are managed.

WIPS criteria #7: Price

Commonly, dedicated WIPS products are purchased as a server or appliance. In addition, WIPS deployments include wireless network sensors, installation services and maintenance.

Costs for these can vary wildly, with the server/WIPS appliances running $5,000 or more, and the price of sensors changing all the time. So be sure to call all WIPS vendors under consideration to get their current pricing levels. And, of course, the more servers and sensors purchased, the more likely it will be that volume discounts will apply.

In this e-guide

If it's determined that intrusion detection system/intrusion prevention system capabilities built-in to the AP will do, expect to pay an annual subscription to turn the WIPS functionality in each AP.

To calculate the cost of WIPS deployment, estimate the number of servers and sensors the organization will need (it varies, but the rule of thumb is often cited as a ratio of four or five APs to every WIPS sensor), the cost of the installation and the cost of maintenance.

Tips for researching WIPS

The very first step to researching WIPS is to determine what features and capabilities are most important to the organization: security, cost, manageability, preferred vendor(s) and so on. Then rate each WIPS product under consideration per each criteria outlined in this article.

To begin WIPS research, visit the leading vendors' websites, read analyst reports and -- most important -- reach out to peers to see what products they are deploying. Ask peers about WIPS costs, their ease of use, ability to get data from the logs, support and performance, as well as the other criteria that are important to the organization. Keep careful notes.

Another great resource is community forums, where an organization can reach out to others who have recently faced the same WIPS purchase decision. Ask for suggestions on how to best negotiate with specific vendors, how reliable their products are and how responsive support tends to be, for example.

In this e-guide

Testing a proposed endpoint security product

Experts suggest evaluating a wireless intrusion prevention system on an organization's shortlist on a test network, or a small subnet. Run the WIPS in monitor rather than block mode and study how it performs in the organization's environment.

Don't be afraid to ask vendors for pilot equipment. This will provide firsthand experience on how the WIPS is deployed, managed and run. If on a test network the organization controls, go ahead and try to run a number of the types of attacks it is concerned about against the system to see how the WIPS performs.

If test equipment isn't available for some reason, interview customers who are using the WIPS. If possible, try to find these customers without input from the WIPS vendor (customers that are fed by the WIPS provider are likely to be the best customers). Either way, however, whether you find the customers on your own or through the assistance of the WIPS vendor, customer input can still be a viable resource when answering questions about the product and support.

Research is a must when choosing a WIPS

The decision on what wireless intrusion prevention system to purchase will not come right away, or overnight. But if an organization does its research

In this e-guide

and follows the criteria laid out in this feature, then it will be able to narrow down the list of choices to only those WIPSes that best meet its established needs.

The next article in this series will detail how to map the purchase criteria described in this feature to specific use cases and scenarios and the best likely WIPS product from a select group, which includes the top WIPS vendors on the market today.

Next article

In this e-guide

Find network anomalies and you'll ax advanced malware

Peter Sullivan

As most security pros are well aware, malware is code, a program or software inserted into a computer or network system to compromise a target's data, applications and operating system, or otherwise disrupt operations of the victim. Whenever there's a new data breach, account compromise or denial-of-service attack, malware is usually the weapon used.

Recently, talk about malware has started to center on a new breed -- so-called *advanced* malware. What makes malware advanced, you ask? There's no one answer, but the industry has come to broadly define it as malware with new and sophisticated capabilities that distinguishes if from thousands of new-yet-ordinary malware that appears daily on the Internet. These advanced capabilities include: an ability to hide from detection for long periods (through encryption, for example); an ability to target an individual or small group, often by compromising previously unknown flaws (also known as zero days); and an ability to attack a number of vulnerabilities by combining a multitude of techniques.

Today's enterprises struggle to defend themselves against advanced malware. As research shows, some organizations haven't yet realized their security focus must extend well beyond their network perimeters; those that

In this e-guide

have attempted to do this often struggle to get the funding they need for the technology and trained staff that an effective advanced malware defense requires. And even if an organization has virtually every possible defense in place, it can still be compromised, because the evasion techniques advanced malware employs are notoriously difficult to identify and stop.

Thus it's no surprise that enterprises are doing such a poor job in detecting intrusions. In several of the recent large retail network attacks in the United States, the network owners never discovered the intrusions, but rather were informed by third parties, including law enforcement and -- in one case -- a security blogger. Unfortunately, by the time a third party notices that tens of thousands of credit cards from a given retailer are being sold on the underground market, the opportunity to quickly detect and stop the intrusion has been lost.

Protection strategies

What about the use of common technical controls at the border? Why aren't they working to detect advanced malware? Let's look at two common technical security products: the firewall and intrusion detection/prevention systems.

Firewalls

A firewall is a default-deny control device. Similar to a router, a firewall forms a boundary between networks. As a control device, a firewall can "decide" to either allow or deny traffic through the boundary. The firewall makes its

decision based upon rules that an administrator has applied. *Default-deny* means that in the absence of a rule that permits network traffic, the traffic is denied and not allowed to cross the boundary.

It can be difficult to know what traffic should be permitted across the boundary. A clearly written firewall security policy can help. In the absence of a firewall security policy (and in the spirit of causing the fewest problems for users) firewall rule sets can be very permissive. Sometimes firewall rule sets don't progress beyond the original default configuration the manufacturer ships with the product.

Intrusion Detection and Intrusion Prevention systems

An intrusion detection system (IDS) is a passive monitor that observes network traffic and attempts to search for malicious activity by matching traffic with a set of rules or signatures; it works much like an antivirus system. If a match is discovered, an alert is sent to an administrator and a security console. The problem is that there will be no recognition of malicious traffic, and therefore no alert, unless:

- Malicious traffic is publicly known;
- A signature has been developed for that malware; and
- Signatures for that malware have been installed.

Beyond these conditions, there is the problem of a security team not responding to alerts in a timely fashion -- or not responding to them at all.

In this e-guide

An intrusion prevention device (IPS) is *default-allow* control device. If an IPS matches traffic with a signature in its database, then it can stop the traffic, much like a firewall can. Many IPS systems are installed on firewalls.

An IPS system has exactly the same problems that an IDS has with signatures, making both the IDS and IPS security solution ineffective against advanced malware.

What's needed now

Because IDS and IPS cannot adequately protect against advanced malware, security pros must change their focus and do more than just try to detect and deny malware at the border. They must acquire and deploy tools that examine the interior of the network as well as the perimeter, tools that possess the ability to detect network anomalies.

Next section

In this e-guide

Section 4: Wireless

Wireless network security

Achieving the best network security you can also means making sure Wi-Fi networks are locked tight against potential intruders. Here's what you need to know about how to make Wi-Fi secure, as well as some of the attack vectors your network is up against.

In this e-guide

As WLANs grow, so does need for secure wireless networks

The trusty Ethernet wall jack has seen better days. Although hard-wired connections offer better speeds and greater reliability than wireless networks, users increasingly favor Wi-Fi as the connectivity medium of choice.

Access point (AP) shipments were up 14% in the third quarter of 2014 compared to the previous year, reported Infonetics Research. Meanwhile, wireless devices are expected to account for 61% of IP traffic by 2018 -- according to Cisco's "2014 Visual Networking Index" -- while wired devices will make up 39% of traffic. As recently as 2013, wired devices still accounted for the majority of traffic at 56%.

The preference for wireless isn't just a matter of convenience. Mobile devices are playing a greater role in how enterprise users get their work done, and devices like Apple's iPhones and iPads don't even have an Ethernet port. For enterprise networking pros, this increased reliance on corporate Wi-Fi means a secure wireless network is no longer optional.

In light of today's sophisticated threats, however, securing a wireless LAN (WLAN) requires more effort than simply password-protecting your service set identifier (SSID). A secure wireless network uses the latest form of encryption -- Wi-Fi Protected Access 2 (WPA2) -- along with other best practices. These include using 802.1X for stronger authentication, restricting

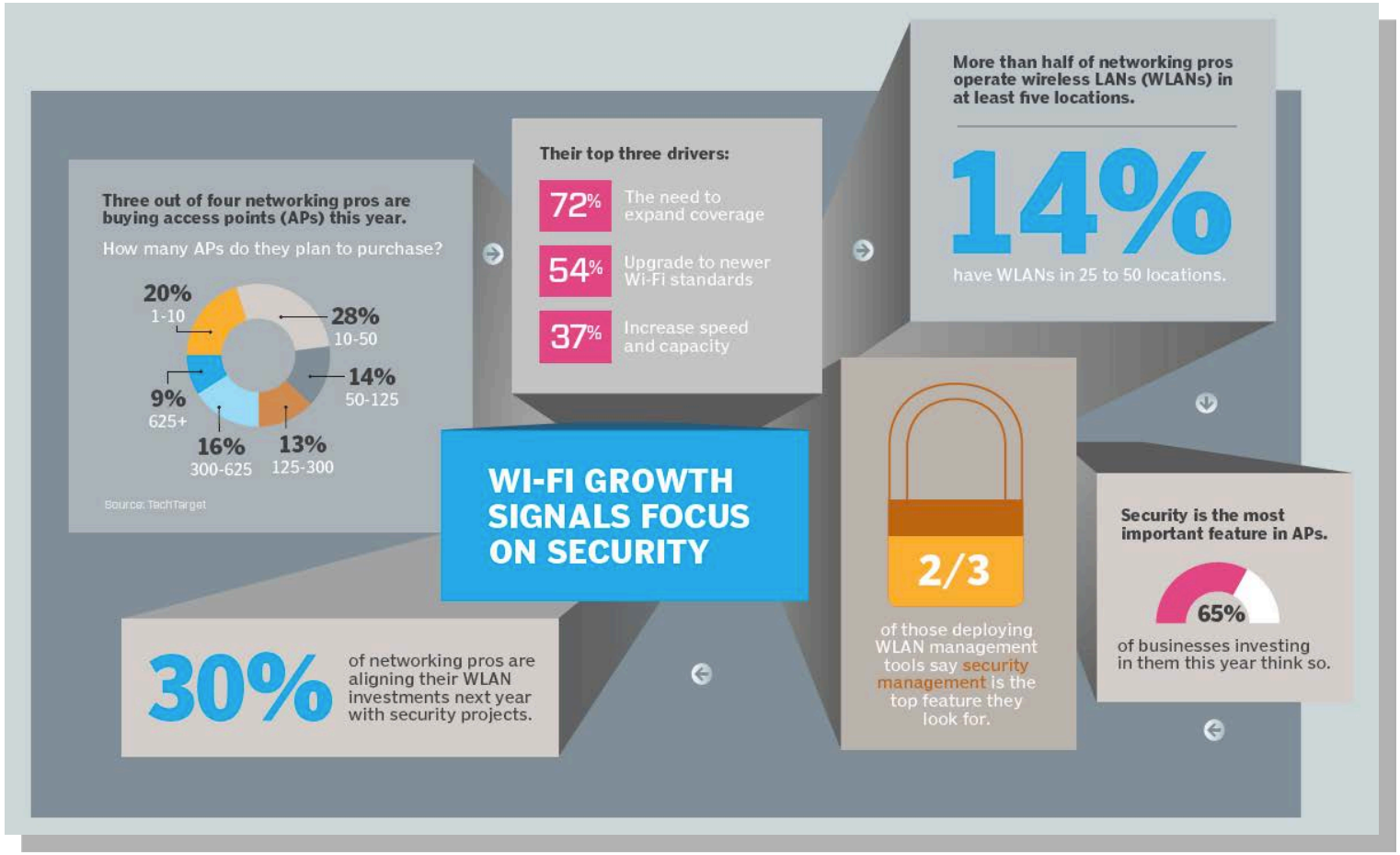
In this e-guide

guest networks to separate virtual LANs (VLANs) with harsher policies, scanning for rogue APs, and using strong passwords on APs and changing them every three months.

In the following pair of infographics, first learn how enterprise WLANs are growing in size and importance, consequently driving the need for more secure wireless networks. Then, find out how vulnerable wireless networks really are, plus what happens when WLAN security is ignored.

(Next page.)

In this e-guide

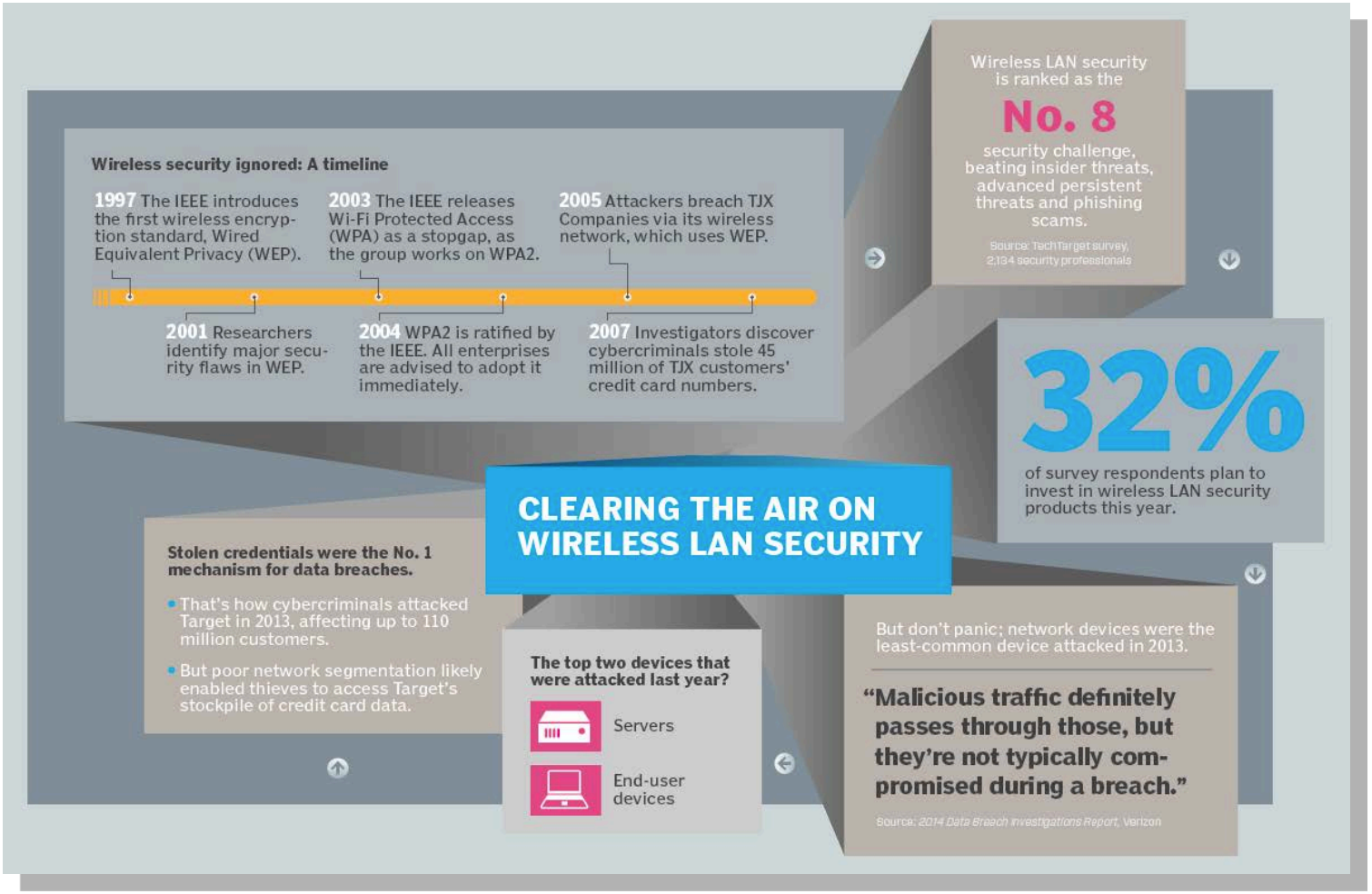


In this e-guide

In this second infographic, we dive into the role wireless security played in the notorious series of hacks on TJX Companies in 2007 that resulted in cybercriminals making off with 45 million debit and credit card numbers. And while network devices like switches and routers themselves are now rarely the direct targets of attack, according to Verizon's "2014 Data Breach Investigations Report," poorly secured networks continue to be a vulnerability that hackers don't hesitate to exploit.

(Next page.)

In this e-guide



Next article

In this e-guide

How to bake security into your Wi-Fi deployment

Lisa Phifer, Owner, Core Competence

Wi-Fi started its long, steady climb 15 years ago, spring-boarding from home to office, eventually displacing Ethernet as the preferred enterprise network access method in many organizations.

Today, enterprise Wi-Fi deployments are being further fueled by 802.11ac, which represented 18% of the 176 million access points (APs) sold in 2014. Wi-Fi not only transforms how workers connect, but also how communications are secured. Wi-Fi security is no longer an add-on; it must become an integral part of security policy enforcement. In this tip, we examine how organizations can embrace this network security transformation.

Beyond the basics

Years ago, security for a Wi-Fi deployment meant link-layer encryption: First came Wired Equivalent Privacy (WEP); next was Wi-Fi Protected Access (WPA) and Temporal Key Integrity Protocol, or TKIP. Then came Wi-Fi Protected Access 2 and Advanced Encryption Standard (WPA2/AES). However, WPA2, combined with Pre Shared Keys (PSKs) or 802.1X access control, has been supported by every Wi-Fi *certified* product for nearly a

In this e-guide

decade. Similarly, keeping wireless intruders at bay may have started with Wi-Fi sniffers and manual site surveys, but fully automated wireless intrusion detection and prevention (WIDS/WIPS) has become a staple, found in every enterprise-class wireless LAN (WLAN) product today.

While these technologies remain largely unique to wireless, they are now simply a foundation upon which to build. For example, 802.1X lays the groundwork to control LAN access, both wireless and wired. WIPS containment can often be triggered to block a suspected attacker at the point of network attachment, both wireless or wired. Increasingly, security policy is not about *how* a device is connected, but rather *who* is connected, *what* they are doing and *where* they are.

Wi-Fi deployments and policy enforcement

According to Ozer Dondurmacioglu, senior director of product and solutions marketing for Aruba Networks Inc., in Sunnyvale, Calif., many large organizations seek ways to create and then enforce a single security policy that does it all.

"When my doctor is in the cafeteria, he may need access to the Internet -- and nothing more. When he's in his office, he may get access to patient data as well. When he's working from other locations that are high-risk, he may be required to take extra precautions," said Dondurmacioglu. "There should be a way to encapsulate all of this in a single policy, and then translate that paper policy using tools for enforcement."

In this e-guide

Enterprises have many tools at their disposal to help them enforce this kind of unified security policy, including identity management services, network and application firewalls, mobile device and application managers, secure wired switch ports and APs, location-based services, guest access services and more. However, realizing this single policy vision is best viewed as a phased process which begins with a target policy, taps available tools to enforce essentials, and then layers on new tools to further enhance policy granularity, threat resistance, and user productivity.

For starters, identity management can drive security policies, tying access rights and requirements not to devices or network attachment points, but to individuals and roles; in the scenario mentioned above, the physician could be granted levels of access that vary throughout the workday, based on policy-driven criteria.

Second, firewalls, switches and APs can monitor and implement those access rights. Broad network segmentation can be applied through VLANs and SSIDs, enforced by switches and APs. Network traffic can also easily be filtered by those edge devices -- for example, determining whether that doctor has access to the Internet or to patient data. However, given the complexity of today's mobile applications and associated risks, application firewalls can be useful to assert more granular policies that reduce risk, deter malware and plug data leaks.

Third, policies may factor in device type, ownership and trust by harnessing mobile device and application managers. For example, the doctor may carry a smartphone and tablet, using both throughout his workday. The same policy may apply different access rights to a fully managed tablet and a

bring-your-own smartphone, or may require that a secure container be installed on each device as a condition of access to patient data.

In addition, policies are starting to take advantage of location-based services, using techniques such as geo-fencing to restrict access to specified venues and authorized areas within them. Location-based services are now expanding, using new equipment like Apple's iBeacons to improve accuracy (especially indoors), either separately or through integration with network infrastructure. In our example, the doctor's tablet may recognize where it is -- either inside the hospital or at a café -- and vary its behavior accordingly, despite being connected via Wi-Fi in both locations.

Finally, guest access services are playing an increasingly important role in security policy enforcement -- not just for visitors, but also for employees using bring-your-own and other devices. Specifically, network infrastructure can be used to manually or automatically redirect new devices to enrollment portals, where workers can register devices, agree to terms of service, receive device certificates and be provisioned for secure Wi-Fi access. Once connected to a secure network, additional steps may be taken to enable secure mobility, such deploying a secure container or application on our doctor's now-authorized and authenticated mobile device.

Building today to scale for tomorrow

Some of the network technologies that enable a flexible mobile security policy as described above have been around for years; others are relatively new. All of them represent opportunities to harness the network to enforce

In this e-guide

security policy in a manner that recognizes the risks inherent in a Wi-Fi deployment but also addresses them within a holistic framework that is focused on users and enables their computing needs. As wireless grows more pervasive, enterprises should embrace this kind of approach to enable and enforce secure mobility everywhere.

Next article

In this e-guide

Faster wireless means wireless security policies need an update

David B. Jacobs

It's been almost a year since the IEEE 802.11ac specification has been ratified and although wireless speeds have greatly increased, the security standards underpinning gigabit wireless have yet to change. Indeed, the same WPA2 encryption protocol supported in 802.11g and 802.11n remains in force. The introduction of the new standard, combined with the increasing use and capabilities of mobile devices, should prompt network managers to review their networks' wireless security policies.

Let's first review the capabilities of IEEE 802.11ac. Wireless LAN (WLAN) systems supporting this standard can deliver data rates in excess of 1 Gbps due to these advances over the earlier 802.11n standard. To that end, 802.11ac:

- Increases the maximum radio channel width from the earlier standard's 40 MHz to 80 MHz or an optional 160 MHz. Doubling the channel width doubles the maximum data rate.
- Introduces an improved modulation technique that increases the amount of data that can be placed in a packet. More data per packet increases the data rate.
- Supports multiple-input, multiple-output (MIMO) to transmit and receive multiple data streams simultaneously in the same radio

In this e-guide

channel. IEEE 802.11ac doubles 802.11n's four streams to a single device. The new standard can transmit up to eight streams with a maximum of four to a single device; four each to two different devices; or a single stream to eight devices. Each additional stream to a device increases the total data rate to that device.

- Fully supports beamforming, a technique that allows an access point (AP) to focus its transmission energy in a particular direction via multiple omnidirectional antennas. Focusing the signal increases its strength, improving performance for devices at a distance from the AP. The IEEE 802.11n standard included beamforming but differences in implementation among equipment vendors reduced its usefulness. The new standard defines implementation, facilitating operation among multiple vendor products.

Time to review security as mobile devices proliferate

For some enterprises, the introduction of IEEE 802.11ac required no significant changes in their wireless security policies. These enterprises have already recognized that many of their employees rely on mobile devices and have already updated their policies. Many others have made some updates to address issues such as employee-owned devices, but have not undertaken a top-to-bottom policy review.

That said, it's important that all enterprises deploying IEEE 802.11ac -- those that have updated security as well as those that haven't-- determine whether

In this e-guide

their current WLAN is operating in the 5 GHz band. The 802.11n specification operated in either the 2.4 GHz or 5 GHz bands. IEEE 802.11ac operates only in the 5 GHz band. If the new standard's introduction reflects an enterprise's first use of the 5 GHz band, they will need to update scanning equipment and other procedures to detect rogue APs and other intrusion attempts operating in the higher band.

No single set of mobile security policies will apply to every enterprise. Some must adhere to very specific sets of regulations such as payment card industry compliance or the Health Insurance Portability and Accountability Act; others protect different types of sensitive data, such as corporate financial records or product plans and designs. Some have mobile employees who seldom visit a corporate office; and in others, employees work primarily in the office but log in from home. Each requires a security policy designed for the nature of its business.

Security assumptions must be updated as networks transform

When mobile devices first appeared, they were often considered to be adjuncts to the wired network. This was fine for reading email while out of the office or for taking notes in a meeting, but most work went on at employee desks and was connected via the wired network.

An all-wireless network changes fundamental security assumptions. Data access through the wired network was often determined by employee login

In this e-guide

credentials and Ethernet port-based virtual LAN (VLAN) membership. Port-based VLAN access is no longer effective in a wireless network. Access instead must be based on the identity and role of the end user, but other considerations may apply.

Device type may also be a critical factor. Many employees have multiple mobile devices and may be limited to reading email from their personal phones, but only be able to access critical information when using an enterprise-owned and configured laptop.

Additionally, location can dictate access. Security software can use various means, such as GPS data or network traceroute, to determine employee location. Data available when an employee is home can be off-limits when in a coffee shop. Detailed financial information may become unavailable as an employee walks out of the office area and into the company cafeteria.

BYOD policies should be re-evaluated with the deployment of IEEE 802.11ac and the understanding that the wireless network has become primary. New devices are released every few months with constantly increasing capabilities. Policies created a few years ago may not account for the new environment.

IEEE 802.11ac greatly increases wireless network capacity but simply represents the latest step in wireless technology's evolution. Additional standards will undoubtedly be developed with additional capabilities. The bottom line: Network security managers must regularly review wireless security policies to address evolving technologies and recognize how

business practices have adapted to take advantage of new technological capabilities.

Next article

In this e-guide

In this e-guide

What's the best way to provide Wi-Fi guest network security?

Kevin Beaver

I read a survey that purports most organizations fail to provide proper guest network security. What are some of the best methods to provide adequate Wi-Fi security for guest users?

These are interesting survey findings indeed. However, I'm never too surprised seeing such studies when they're sponsored by product vendors. I perform many internal network security assessments each year and see fairly robust guest wireless configurations handled by systems from Meraki (Cisco), Aruba Networks and the like. Many businesses I've seen ensure guest network security by physically segmenting them away from the internal LAN and often routing them through a dedicated Internet connection.

The main problem I see with this approach is that the same security controls present inside the corporate network (i.e., Web filtering, enterprise firewall, monitoring/alerting) are often not protecting the wireless environment in the same ways. So, whose responsibility is it to ensure the wireless network is safe? It depends on your approach to risk. Are you evaluating risk in terms of your users or in terms of your own internal network? Most IT shops are concerned about the latter.

In this e-guide

Outside of using an enterprise-grade wireless intrusion prevention system, keeping it patched and tested, and tying that environment into your proactive monitoring or security information and event monitoring system, I'm not convinced there's a simple way to protect everyone from each other, especially since you don't have control over the endpoints.

The issue is, once you start locking down guest wireless, you'll get complaints and can experience various problems that can tie up help desk and related IT resources. In the end, your business needs to decide whether it makes sense to spend time, money and effort attempting to secure something that may not be truly securable.

Next article

In this e-guide

Wireless access point security: Defending against Chameleon malware

Nick Lewis

Can you please tell me more about the Chameleon malware, including how to detect it and how to keep Wi-Fi access points safe from it?

Researchers from the University of Liverpool developed a new proof-of-concept malware called *Chameleon* to demonstrate malware that spreads via wireless access points (WAPs). Chameleon reportedly spreads over the air by attacking insecurely configured WAPs. Once an access point is compromised, Chameleon captures unencrypted network traffic to gather usernames and passwords and scans other wireless networks for insecure configurations.

Chameleon was designed to highlight some of the vulnerabilities of wireless networks in high-density cities where biological viruses spread faster because of their close proximity to other vulnerable hosts. The basic functionality of the Chameleon malware could be extended in a modular way to add other functionality or exploits, such as other modern malware features.

Chameleon exploits some of the same insecure configurations as Firesheep, and many of the same protections against Firesheep can work against Chameleon. Using an encrypted wireless network and an encrypted IP

In this e-guide

network connection will protect users against Chameleon. Securely configuring wireless access points will also help boost an enterprise's wireless network safety. Additionally, scanning and removing insecure wireless access points will prevent these types of attacks.

Most enterprises are at minimal risk of being hit by the Chameleon malware or something like it, due to the fact that they largely have deployed wireless networks using encryption. Nevertheless, a new version of Chameleon could be released with support for attacking encrypted networks or against common enterprise wireless access point products, putting seemingly safe enterprises at higher risk.

The standard advice -- improving wireless access point security by not allowing enterprise employees to use insecure wireless networks -- will prove to hold true in this scenario.

Next article

In this e-guide

Wi-Fi router security: Assessing the vulnerability of backdoor attacks

Kevin Beaver

I read that certain Wi-Fi routers can potentially contain backdoors that make them vulnerable to remote attacks. Are there any reliable ways to know if our gear is vulnerable?

There's been quite a bit of new research in this area recently that points to wireless routers containing backdoors. Apparently equipment from Netgear to D-Link to the seemingly unthinkable Cisco are all vulnerable to these basic backdoor attacks.

So how do you know if your system is vulnerable? You can do your own testing with vulnerability scanners (network/OS such as Nexpose or QualysGuard, and Web such as Netsparker or NTOSpider) to check for susceptibility on your router(s). You could also connect a network analyzer such as OmniPeek or CommView for Wi-Fi to your wireless routers and monitor for odd behavior such as disallowed protocols and workstations generating an enormous amount of traffic.

If you're technical enough, you could also do your own packet poking and prodding like researchers do. The real question becomes: Where are these routers located in your enterprise? If they're directly accessible over the Internet, then why? If you have a reasonable guest wireless configuration

and have such routers connected to a dedicated DSL or similar connection that's completely disconnected from your business network, then it may not be an issue at all. However, if you've placed these routers behind your firewall, you could be opening your entire network up to people outside your four walls. Only you will know.

As far as finding out whether your systems are vulnerable, you could reach out to vendors directly, look at the links above or do your own Internet searches specific to your router model numbers to see if there's a known problem and/or solution. However, I'm not convinced that manufacturers are not complicit in these backdoors. I hope they're not and that they're as trusting (ignorant?) about all of this as the general public is.

Next article

In this e-guide

Getting more PRO+ exclusive content

This e-guide is made available to you, our member, through PRO+ Offers – a collection of free publications, training and special opportunities specifically gathered from our partners and across our network of sites.

PRO+ Offers is a free benefit only available to members of the TechTarget network of sites.

Take full advantage of your membership by visiting http://pro.techtarget.com/ProLP/

Images; Fotalia