

NETWORKWORLD

T R E N D W A T C H

SECURITY

SECURITY LEVEL 02



ERROR!!
PLEASE START AGAIN

How information protection, identity-centric access control, security event management and managed services are shaping new defenses

IRONPORT POWERS AND PROTECTS

YOUR NETWORK INFRASTRUCTURE WITH
WEB SECURITY, EMAIL SECURITY
AND SECURITY MANAGEMENT APPLIANCES



Web Security The IronPort S-Series™ is the industry's fastest Web security appliance – providing a network perimeter defense for the broadest range of spyware and Web-based malware.

Email Security The IronPort C-Series™ and IronPort X-Series™ email security appliances are in production at eight of the ten largest ISPs and more than 20 percent of the world's largest enterprises. These industry-leading systems have a demonstrated record of unparalleled performance and reliability.

Security Management The IronPort M-Series™ security management appliances centralize and consolidate important policy and runtime data, providing administrators and end-users with a single interface for managing their application-specific security systems.

Through a global salesforce and reseller network, IronPort, now part of Cisco, offers a "Try Before You Buy" program. IronPort has thousands of customers around the world who realized after a short trial that this is the most advanced security technology available today. To receive a fully-functional IronPort appliance to test in your network, free for 30 days, call 650-989-6530 or visit us on the Web at www.ironport.com/try.



www.ironport.com

IronPort is now
part of Cisco.



Preventing the Spread of Web-based Malware.



TRY BEFORE YOU BUY PROGRAM

Through a global salesforce and reseller network, IronPort, now part of Cisco, offers a "Try Before You Buy" program. IronPort has thousands of customers around the world who realized after a short trial that this is the most advanced security technology available today. To receive a fully-functional IronPort appliance to test in your network, free for 30 days, call 650-989-6530 or visit us on the Web at www.ironport.com/try.



www.ironport.com

To date, the most successful malware worms use a new blended attack where malware is hosted on a website instead of inside an email message. Separate anti-spam and Web traffic monitoring systems aren't as effective at stemming the spread of such malware. For greater effectiveness, IT departments should consider solutions that can detect malicious patterns and holistically share results between the following functions:

Spam filtering. The Storm worm sent out email with different attachment types – some of which (such as PDFs) were initially difficult for anti-spam programs to identify as spam – in different campaigns over 2007. However, Storm seems to have settled on spam that includes a short message and website link, rather than an attachment, as most effective in 2008. The anti-spam solution should block email that includes suspicious domain names and URLs as well as email with suspicious attachments.

Web reputation assessment. An anti-malware system that uses Web reputation to identify and block connections to suspicious websites, and checks every object a browser needs in order to load a webpage correctly, is crucial. As this new kind of malware may compromise trusted, legitimate websites to insert a malicious payload, an accurate Web reputation system should not merely depend on past reports of malware or the domain itself. The most effective system proactively assesses threat indicators from any URL, IP address or Web server on the Internet.

In addition, ostensible spyware scanner and fraudulent protection websites (which appear to thwart such malicious attacks, but instead deliver malware) are deceiving even sophisticated Web users with legitimate-looking language and counterfeit "endorsements" from recognized software rating companies. Systems that perform object-based checking of information and verify the source of the data, instead of relying on URL categorization, can more effectively block downloads from these sites.

Port and communications activity monitoring. A system that detects patterns and flags unexpected levels of activity on any unusual ports (such as Port 53 or 25) or using atypical communications protocols can be an excellent warning indicator.

Keeping anti-virus and anti-malware products updated. Given the speed and frequency with which Storm and its successors morph into new variants, comprehensive, reliable and very frequently (or automatically) updated anti-virus and anti-malware products are essential.

Finally, IT departments may help reduce infections by regularly reminding computer users on their network about how these new kinds of malware use social engineering and what types of email, blog comments and websites may try to infect their computers with malware payloads.

IronPort is now
part of Cisco.





Security from inside out

The perimeter is a known entity; what's going on inside the perimeter is what's frightening readers, our recent survey of security trends finds

“IT has pretty much figured out how to secure the perimeter.” So says Paul VanAmerongen, manager of information security services at MultiCare Health System in Tacoma, Wash. He’s not alone.

VanAmerongen, a member of [Network World’s Technology Opinion Panel](#), is one of 483 readers who participated in a [July survey](#) on security trends conducted for us by Research Concepts. He’s among the 61% of respondents who said they were confident or extremely confident in their organizations’ perimeter defenses. Another is Douglas Davis, IS coordinator for Monical Pizza, a Midwest restaurant chain in Bradley, Ill. He rates his confidence level at 99.95% — “about the maximum you can be,” he says.



This is not to suggest that these IT executives believe their enterprise’s perimeter provides rock-solid defenses or doesn’t require their attention. “Of course you’re constantly monitoring and making sure your patches and everything else on the perimeter are up to date. . . . It’s a constant battle out there,” VanAmerongen says.

For the most part, however, enterprises understand perimeter technologies and the types of attacks they might suffer. As VanAmerongen says, “The perimeter battle is not as ambiguous as what an internal user now can do.”

And that’s the crux of [enterprise security](#) today. What’s going on inside the perimeter can be far more confounding than what’s going on outside it.

“We’re now questioning what our internal people — the people who are allowed to be on our system — are doing. We also have to think about what other people in our buildings, maybe even patients, are doing. Questions come into play like, ‘Can we be attacked through any internal systems? What kind of damage can they do? What happens if somebody walks in with a USB stick and plugs into one of our computers? What happens with wireless?’” VanAmerongen says.

Concerns such as these have given rise to two IT security trends: the focus on controlling access to information, and the shift in mindset from guarding the network to protecting the information.

In our recent survey, for example, 63% of respondents said they consider network access control (NAC) important or extremely important to their organization’s security. Almost one-third reported having completed NAC deployments, and nearly another third said they are deploying NAC or will be within the next 12 months.

Dimitri Yioulos, CIO at First 1 Financial, a subprime auto finance company in Norwell, Mass., is among the 22% of respondents who haven’t committed yet but are considering NAC. “When you have the word ‘financial’ in your company name, you might as well have a big target on the side of your building. We already have a network that gives users the least privilege necessary, and our business applications log everything a user does, but we are exploring NAC too,” he says.

Like many other survey respondents, Yioulos recognizes NAC as but one element in a company’s strategy for controlling whose eyeballs land on which data. Forty-five percent of the readers surveyed said they either disagree or strongly disagree that NAC addresses all their organization’s access-control issues. That’s more than twice the percentage of respondents who said they agree or strongly agree that NAC is essentially the be-all and end-all of access control.

At Monical’s, NAC is the final step. “That’s the door with the key,” Davis says. “I believe in security through limited access: You don’t build a door and put a lock on it; you just build a wall. Then you don’t have to worry whether the NAC client has the right key. Having all the keys in the world isn’t going to help you walk through a wall,” he says.

At MultiCare, educating users about the critical nature of data is as important as determining how to protect the data with technology, VanAmerongen says. That’s a great starting point, today’s leading security strategists say. Information protection begins with knowing which data is valuable, then finding where it is located and protecting it. Inside, we explore the various ways enterprises are handling the challenges of doing that.

— Beth Schultz, special projects editor



INSIDE:

4
Information AND network protection: Finding the right mix

8
Access control: The evolving tool set

12
Security event management: Finding the proverbial needle

15
Managed security services: Outsourcing threat management

ONLINE:

Trend Watch Extra

Get all the results from our recent security concerns reader survey.

[View slideshow](#)

Editor: Beth Schultz

Art director: Brian Gaidry

Copy editors: Carol Zarrow, Ryan Francis



Information AND network protection: Finding the right mix

How to secure critical and regulated data when network defenses aren't enough

BY DEB RADCLIFF

For years, with organizations increasingly opening their networks and data centers to external business partners and mobile employees, experts have been claiming that the perimeter is dead. At the very least, perimeters are riddled with enough holes that restricted data from the creamy center is leaking from endpoints and pouring out of databases and file-shares.

The industry, of course, is still stinging from the most notorious example of this — the TJX Companies case. An ongoing Secret Service investigation resulted in last August's [indictments](#) of a ring of 11 attackers that also had been in the transaction-processing systems of six other brand-name retailers — some of them hidden since 2004. As a result, the criminals compromised nearly 45 million credit and debit accounts.

The porous perimeter needs protection from more than the bad guys attempting to make a buck off stolen credit-card numbers: It needs protection from the gung-ho employee who, while trying to get some extra work done at home, inadvertently sends restricted material across the Web.

"A typical organization has lots of connections through its firewall — customers, Web services, suppliers, outsourcers," says Steven Bellovin, professor of computer science at Columbia University and co-creator of the Usenet online-discussion system. "We haven't been protecting this data effectively enough. And I'm asking the community, 'What should we do differently?'"

Bellovin raises the notion of security at the center to protect against attacks getting to critical data in databases and file-shares. This idea is similar in many ways to [The Open Group's Jericho Forum](#), which advocates assigning priorities to data, focusing on the most critical areas, and applying secure communications and encryption around these classified resources.

Neither Bellovin nor the Jericho Forum is suggesting organizations do away with their edge security. The perimeter, which serves an invaluable role in filtering the "noise" of network-based attacks, can be tuned to serve more data-centric functions. Nor are they claiming to simplify the processes of information protection. If anything, their approaches mean creating more layers, complexities and choices to be made around best-of-breed and point-product integrations.

"The problem is we don't look at data holistically. Consequently, data breaches are all over the news," says Jeff Boles, director of validation services at server and storage consultancy Taneja Group. "The way to get there is to look at a resource being accessed in context of the relationship between who the user is, what the user nor-



"Our challenge now is tightening [user – access] permissions."

STARLA RIVERS,
technology security architect,
Sharp HealthCare

MARTIN TRAILER

mally does, and the nature of the data.”

A holistic approach to critical data protection would suggest integrated options for IT pros trying to cross the chasms between data that is structured and unstructured, at rest, in use, and in motion. Unfortunately, the jobs of prioritizing, encrypting, monitoring and controlling the access to and use of sensitive data are anything but integrated. As a result, organizations are taking a variety of approaches to protect their data from flowing out of their organizations, including [data loss prevention](#) (DLP), access controls and encryption.

Goopy center

To get started, organizations need to know which data needs protection, and how to locate it — the cornerstone of the Bellovin and Jericho models.

Too many organizations, however, don't know what and where that data is, says Derek Brink, vice president and research fellow at Aberdeen Group. In an Aberdeen survey of 120 IT security professionals released in May, 50% of the best-in-class respondents had discovered and classified their critical information.

“You don't want to spend the same money protecting e-mail to the family about Sunday's barbecue as you do [protecting] your financial data,” Brink says. “You only want to protect the resources that matter. But classifying those resources is the real challenge.”

San Diego's Sharp HealthCare, with 16,000 employees at seven hospitals and two medical groups, is one enterprise well on the way. It uses a variety of manual and automated processes to understand and manage its critical data, says Starla Rivers, technical security architect.

Sharp uses Symantec's [Vontu Data Loss Prevention](#) product suite to discover critical unstructured data, such as health identification-card and Social Security numbers. Vontu does this by fingerprinting that data in a few key databases in which Health Insurance Portability and Accountability Act-specified, financial and other regulated data is processed. Then it looks for instances of that data outside the database on file-shares and endpoints. ([Compare DLP products.](#))

In keeping with the Bellovin and Jericho theories, DLP tools are best used when they monitor for the least number of data types necessary, say DLP vendors. So, Vontu doesn't need to tag every type of data in a critical database for its initial scan. People generally tag the top five or six data types requiring protection. Like Sharp, most organizations start by classifying and protecting their regulated customer and reputational data, according to Aberdeen survey findings.

Vontu discovers sensitive data on network file-shares, tracks data movement at the endpoints and enforces group policy around that data. Sharp needed a second product, however: Varonis Systems' [Varonis Data Advantage](#), for governance and auditing. ([Compare Network](#)

[Auditing and Compliance products.](#))

“Group A may have 120 people, and I want to assist the department's data owner in determining the appropriateness of the individual, not just the group, with access to the folders containing sensitive data. That means determining who is accessing the folder, how often, and whether or not he should have those privileges,” Rivers notes. “Our challenge now is tightening these permissions. Right now we're using Varonis to assist us in that.”

Once the Vontu agent determines that a folder contains sensitive data, Rivers provides the file list to the managers accountable for that data. In turn, these managers are responsible for determining whether the folders and the files contain the minimal amount of information necessary to conduct the business function. They are expected to think in terms of records, fields, people and time, she says.

Rivers also uses the Varonis and Vontu tools to analyze regulatory rules for retention and other processes for which a single blanket policy is difficult to write. “We have so many regulations to follow here, and there is no one data-retention rule that I can write a policy to,” she says. “Some departments shouldn't be storing sensitive data at all, whereas other departments may need to keep the data for 10 years.”

The IT group and business unit managers can learn from the analysis provided by the Vontu and Varonis tools, Rivers says. Meantime, user education comes through e-mail and the pop-up alerts Vontu delivers when policies are violated. As a result, employee-use violations have decreased by 70% since the system was implemented in 2007. And Sharp's staff members have even used the system to educate partners sending inbound information of a sensitive nature.

Taneja's Boles refers to data protection models like Sharp's as context-based data controls. A lot of companies play in the classification space, he says, naming Abrevity, Kazeon Systems, Mimosa Systems and StoredIQ. It takes finesse by user organizations, however, to get to this next level of context-based controls through benchmarking data-use and monitoring outbound data flows.

Web and endpoints

Network-based DLP devices fit Bellovin's model of placing security closer to the database. So too do [database application firewalls](#), such as those from Guardian and Imperva, for hardening, discovery, classification, monitoring and auditing.

Bellovin has reason to worry about protecting the database, particularly when it comes to its relationship with the Web server, says Richard Rees, security solutions director at SunGard Availability Services, a provider of information availability and business continuity services. “When we do penetration testing on clients' Web servers, we don't care about the server except as an avenue back to the data on the database,” Rees says. “We find all types of vulnerabilities that can be exploited to do this — SQL

SYMANTEC IS

COMPREHENSIVE SECURITY FROM LAPTOPS TO DESKTOPS
TO SERVERS.

ENDPOINT PROTECTION.

Confidence in a connected world.



injections, cross-site scripting attacks and so on.”

Bellovin has a fix in mind. He proposes a Web SQL language called “NewSpeak,” in which no verb can be ordered to do something insecure.

“No command can say, ‘Give me the credit card number.’ This is not something the Web server needs to be able to do. Instead, it should say, ‘Here’s the total amount. Send this transaction to billing;’” Bellovin explains. “There shouldn’t be verbs to dump the database or read the credit card.”

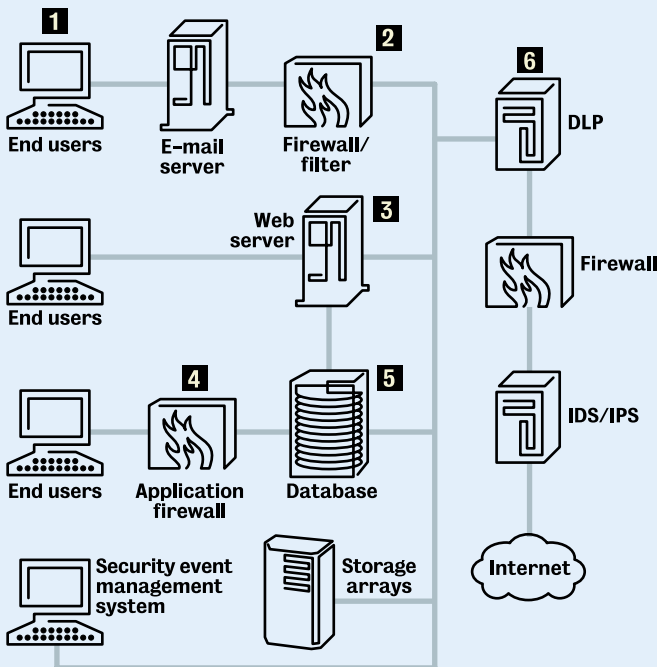
By rewriting commands, developers would be hardening the Web appli-

cations. This, however, requires teaching developers to think in language that not only can’t be tricked but also is understood explicitly by the database — something that’s not likely to happen overnight, analysts say.

Bellovin also suggests taking the authentication role from the Web server and in so doing, removing the credentials to every account in the database. Instead, he recommends user-level authentication. This probably would be managed through a federated-identity model, such as is used by companies like [TriCipher](#), which provides Web authentication

Securing the network and the information

Beyond the firewalls and intrusion detection/prevention systems (IDS/IPS) standing guard at the enterprise perimeter, today’s data-centric security means putting protections closer to the database and endpoints where critical, protected data is housed and processed.



1 At the desktop:

- Endpoint security and patch management
- DLP-enforced policies on leakage via USB devices, e-mail and instant messaging
- E-mail protections against inbound phishing and malware
- Access controls

2 On the network

- Behavior monitoring
- Data reading (full decryption/inspection)
- Inter-departmental firewalling

3 At the Web server

- Close extra ports
- Run only necessary services (no authentication)
- Scan and patch
- Firewall

4 At the database gateway

- Monitoring/firewall/access control device
- Advanced access controls (users can only access the data they need)
- Fine-grained resource allocation
- Departmental management for employee access and account termination
- Monitoring (most don’t use native monitoring because of performance)

5 In the database

- Native auditing tools and access controls

6 At the perimeter

- IDS/IPS and firewalls tuned to watch inbound traffic
- DLP tuned to watch outbound traffic (data typing, data reading full decryption/inspection, pattern recognition)



SYMANTEC IS

BRINGING INNOVATION BACK TO DATA PROTECTION.

NEXT GENERATION DATA PROTECTION.

Confidence in a connected world.



for e-business applications. ([Compare Identity Management products.](#)) Meanwhile, the Jericho Forum argues that access should be controlled by the security attributes of the data itself. This could be facilitated through encryption, with rights being temporary, limited to that session.

“What I’m proposing is authentication accompanying every SQL command from the user, through the Web server to the database,” Bellovin explains. “The database server won’t respond to any request for user records if the request doesn’t have a password. Even if I hack the Web server, I can’t get into your account because I can’t find your password. It’s known only to you and the database.”

Imperva and other database-protection products could support such an architecture as long as they combined protection mechanisms — heuristic, correlative or signature — says David O’Berry, IS director at the South Carolina Department of Probation in Columbia. They also would have to be based on a simple valid/invalid request-response-transmission/transaction system that could be checked at every leg of the transmission.

“What Steve [Bellovin] is talking about is really concentric layers,” SunGard’s Rees says. “We can’t do away with firewalls and [intrusion-detection systems] at the perimeter because they do a great job of protecting networks. They don’t do a good job of protecting applications.”

Besides monitoring their database and network for classified data, organizations need to protect against data leaking out at the endpoint.

To this end, endpoint-protection companies have been integrating DLP into their product suites, often through acquisition. Besides Symantec, which closed its Vontu acquisition last December, endpoint-DLP deals include Trend Micro’s October 2007 [acquisition](#) of Provillea and McAfee’s [recent purchase](#) of Reconnex. Now these companies’ DLP portfolios include gateway-monitoring devices, as well as endpoint agents that feed data into a reporting console.

DLP companies also are expanding their portfolios with encryption — another layer of data protection necessary under new security models. Sophos, for example, recently acquired [Utimaco](#), a German data-security company, and McAfee [bought](#) SafeBoot last fall and made data encryption centrally manageable. Using such tools, organizations can uphold policy on the endpoint, for example, “encrypt when downloading to a USB device.”

“The endpoint really must evolve to be the flexible, resilient hard

perimeter, or the skin on the network,” says South Carolina’s O’Berry, who’s evaluating McAfee’s [Reconnex iGuard](#) in tandem with his deployment of McAfee’s endpoint DLP agents, and using Safeboot for endpoint encryption. “The endpoint is what the criminals are most aiming for because they’re making a lot of money off hacked, remotely controlled computers, keyloggers and phishing attacks against end users.”

O’Berry’s probation department supports more than 750 mobile, convertible tablet users, along with connections to other law-enforcement and social services agencies. “Those tablets log in from various nontraditional locations, including home networks, to insecure, open wireless networks wherever they’re available.”

Another enterprise, Signal Financial Credit Union, reports having stopped 98% of its data leakage problem using DLP at the gateway and endpoints. The company uses [Code Green Networks’](#) Content Inspection appliance at network egress points to inspect and enforce protections on outbound e-mail traffic, create tickets, and manage rules and roles, says Steve Jones, CTO at the Kensington, Md., organization.

To expand DLP capability on the network, Jones uses Blue Coat Systems’ ProxySG appliance to proxy other outbound flows, including SSL traffic that it decrypts with an optional SSL decryption card. Outbound data transfers often hide in the commonly used SSL protocol.

“The DLP device is monitoring everything going out, looking for account information, card numbers and several other data types that we’ve deemed critical,” says Jones, who also uses Code Green agents on his endpoints to prevent leakage through USB ports and wireless connections.

Ultimately, security of critical data will occur at flow and use points across the enterprise and beyond, O’Berry says. This, he adds, essentially means layering additional protections at the database, the endpoint, the network and Web.

Bellovin has the bottom line: “We need to think about the problem in a different way because what we’re doing [with perimeter protections] isn’t working. What we need is a more data-centric architecture with strong protections around the important data because security holes in the perimeter are inevitable.”

Radcliff is a freelance writer covering computer crime. She can be reached at deb@radcliff.com.



SYMANTEC IS

FROM ANTIVIRUS TO VIRTUALIZATION TO DATA CENTER MANAGEMENT, SYMANTEC IS HARD AT WORK IN OVER 99% OF THE FORTUNE 500®. FOR AN INSIDE LOOK AT WHAT SECURITY MEANS TODAY, VISIT US AT SYMANTEC.COM/EVERYWHERE

EVERYWHERE.

Access control: The evolving tool set

Enterprises struggle to find the sweet spot — in cost, complexity and capability — as they adopt user-centric security

BY JOANNE CUMMINGS

Smart enterprise IT executives know that who you are and what you're doing mean a whole lot more than which device or network port you're using.

Craig Richard, IT director for NaviMedix, a Cambridge, Mass., company that manages electronic communications among health insurers and physicians, gets it. "You may have a port with access to parts of the network that should be protected. But someone could easily plug a device into that port and have that same level of access, even if they weren't authorized to have it. Access needs to tie directly to the user," he says.

Mobility has forced the issue. In the past, ports and IP addresses were reasonable proxies for identities, says Andreas Antonopoulos, a partner at Nemertes Research and *Network World* "Security Risk and Reward" columnist. "I [once] had a Solaris workstation that weighed 300 pounds and was connected to the network by an Ethernet coaxial cable as thick as my thumb. My mobility was rather limited, and my IP address literally did not change once in three years. So, there was a very direct association between IP address and user," he says.

That has all changed because the types of devices people use and the ways they connect to the network are so varied. "The IP address of my BlackBerry changes every few hours, and the IP address on my laptop changes depending on if I'm using Wi-Fi, 3G, a LAN, a VPN or whatever," Antonopoulos says. "The IP address has become very transient. You might have a dozen users using the same IP address during the period of one day."

That transience is a nightmare for network security teams, especially when they investigate incidents or demonstrate compliance. In either case, being able to link an IP address in a log to a specific user is highly desirable if not outright necessary.

"If you're lucky, you have a DHCP server that keeps good logs of who got which IP address when," Antonopoulos says. "And if you're really lucky, that DHCP server is properly time-synchronized to an atomic clock or [network time protocol] source so those logs can be correlated. And if you're even luckier, all of your other logs sync to the same source. Then you can say that this IP address accessing this application at this second was issued to this user, on this media access control-addressed machine. It's not easy," he says. (See "SIEM: Finding the proverbial needle," page 12.)

"Access needs to tie directly to the user."

CRAIG RICHARD,
IT director,
NaviMedix

NETWORK SECURITY THREATS ARE CONSTANTLY INCREASING...

HOW WELL IS YOUR NETWORK PROTECTED?

The most effective way to protect your business is to secure your endpoints and control access, preventing problems before they arise. Our comprehensive pre- and post-admission control solution takes you beyond visibility capabilities to deliver proactive security, preventing the misuse of resources and limiting potential liabilities.

Alcatel-Lucent User-Centric Network Security Solutions

AUTHENTICATION



Control who gets access to your network: White-listed exceptions and blacklisted rogues and customized access for employees, remote VPN users, contractors and visitors.

HOST INTEGRITY CHECK



Ensure end-point compliance with policy: Up-to-date and active antivirus, compliant operating system with critical patches.

ROLE-BASED ACCESS



Profile controlled access to different areas of your network: Role-based access to enterprise resources and information.

ANOMALY DETECTION



Detect and prevent attacks: Signature-based and inspection, live security dashboards for authentication failures, policy incidents and awareness.

QUARANTINE & REMEDIATION



Identify and isolate security policy violators: Customizable quarantine enforcement on the network edge, and automated remediation and restoration to network when clean.

MONITORING AND COMPLIANCE



Meet compliance requirements: User aware security management, network monitoring, incident capture, extensive logging of network access and activity, and reporting.

Learn more online: www.alcatel-lucent.com/enterprise/networksecurity



Getting there

Fortunately, security tools are evolving beyond the simple IP address and IP port focus, and increasingly are becoming more user-centric, working their way slowly up the Open Systems Interconnection stack. Network-access control (NAC) is the primary transportation for this move. Depending on the vendor, NAC handles everything from Layer 2 endpoint security to access control, ID management and behavior-based monitoring at Layer 7 — which all rely on a user's identity and role in the organization. Most of the marketing thunder surrounds such big-name tools as Microsoft's Network Access Protection and Cisco's Network Admission Control; many other NAC flavors offer their own slants on solving the problem. ([Compare NAC products.](#))

Enterprise interest is plentiful. In a recent [Network World survey](#), 63% of 483 reader respondents said they consider NAC either an important or extremely important piece of their enterprise security plans. Forty-eight percent of respondents have deployed NAC products, while another 11% expect to do so within the next 12 months.

NaviMedix is in the former category. For user-centric security, it uses [Bradford Networks' NAC Director](#), a policy-based appliance. NAC Director works with a company's LAN switches to manage individuals' identities by associating them not only with IP and MAC addresses, but also the individuals' roles in the company and the applications they are authorized to use.

Because NAC Director focuses on identity, it eliminates the problem of insecure ports. "When everything is tied to a user account and identity, it's far easier to secure," NaviMedix's Richards says. "No valid user account, no access. And that means zero possibility for unauthorized users to get to the protected parts of the network."

In addition, NAC Director integrates with Microsoft's Active Directory service, which NaviMedix uses. This integration lets the firm base application access on Active Directory group membership using virtual LANs. "With the VLANs, only certain individuals and departments can get to certain parts of the network," Richards says. "Together, NAC and Active Directory grant authorized individuals access to their data wherever they are in the company. Their VLANs follow them, so they get what they're supposed to get based on who they are. And they get proper access, no matter where they login or what device they use."

The forklift route

NaviMedix chose Bradford's NAC appliance because it didn't require network changes. Richards could make the out-of-band appliance work with the company's existing Cisco switches, none of which were the latest and greatest.

While clearly not necessary, network overhauls do provide a simpler entry into user-centric security. Such was the case at Ferrum College in Virginia, which recently implemented Juniper Networks' new [EX 4200 and EX 3200](#) LAN switches together with its [Unified Access Control](#) flavor of NAC. Ferrum primarily needed the new network for better stability and support for an online-learning management system and upcoming move to VoIP, but user-focused security was a consideration, too. ([Compare Access Switch products.](#))

"Rather than basing security on machines, we wanted to base it on people," says Christine Stinson, CIO at the college, which has 1,400 students and 300 faculty and staff. "We wanted groups to access certain resources, while locking out others, and we wanted to be able to track all that," she says.

Ferrum uses VLANs to segment the network, keeping guests and students separate from such business functions as admissions and the registrar's office. Managing users and their access levels is relatively easy, Stinson says. "Once you have one VLAN set up, you can copy the settings, modify what you need to modify and basically create a new VLAN," she says. "And it's easy to move users from VLAN to VLAN. Once the groups are defined, we simply say this user is in this group, or this user is in these two groups. That's not a problem at all," she adds.

The NAC implementation ensures that the school balances the needs for open Internet access and strict data security.

"Academic freedom is a very strong part of our history and tradition here," Stinson says. "But we also have pressure from federal and state laws regarding privacy and security. We need to provide students and

User-centric security begs for process overhaul

Such is the wisdom gained in one college's deployment

At Ferrum College, a moderately small school in Virginia, a Juniper Networks-based [network access control](#) deployment makes sure that access to sensitive data is based on who the users are, not where they are or which devices they're using. The new user focus on security, however, required an overhaul in people and processes as well, says Ferrum's CIO Christine Stinson.



Before the Juniper network, Ferrum used what Stinson calls family-style computing. "We were a small campus, and everyone knew everyone. So, if you needed access to something, you would go over to the computer-services desk and say, 'Hey Tim, I need access to this,' and Tim knew you and would give you access," she says.

That changed as the campus grew, and Stinson began the move to user-focused security. She assigned ownership to all the data stores on campus, removing access from IT's purview. "I tell everyone that your data is like a horse," she says. "We're the stable. We keep your data, we feed it, we clean up the mess after it. But you determine who rides it." ([Compare Network Access Control products.](#))

Now, when requests come in for access to particular databases or files, the data's owner has to sign off on giving that access, as does the CIO. "I review everything, sign off on it, and only then does administrative computing grant the access," Stinson says.

Perhaps more importantly, the college also instituted a formal process for reviewing access. "Every six months, we review all of the access that's been given," Stinson says. "If there's not a need for the person to have access, we make sure we close it out. All of these processes needed to be in place first. Otherwise, the network segmentation wouldn't have made any difference in our security posture."

Stinson made sure she had buy-in from each data owner and user by making them all play a part in building the processes. "One thing I've learned is that if I simply announce a change, there will be a lot of resistance to it," she says. "So instead, I identified all the people who created databases and met with them as a group. I explained what the new privacy and security requirements were that were imposed on us legally. Then we developed consensus on what an ideal process for managing data access would be."

"Once the data owners bought into the process, it was very simple to say to the rest of the community, if you want access to their data, here's the process," Stinson says. "All that needed to be in place before we ever looked at rolling out a tool."

faculty with access but we have to be very concerned with the safety and protection of student, faculty and employee data. NAC helps us strike that balance."

The downside of NAC

Of course, Ferrum's greenfield, Layer 2-7 deployment — of a single vendor's LAN switches, NAC appliance, policy server and firewalls — is

See [Access control](#), page 17



SIEM: Finding the proverbial needle

We're getting closer to the day when making sense of and taking action on disparate security events gets quick and easy

BY SANDRA GITTLEN

Matt Roedell, vice president of infrastructure and information security at TruMark Financial Credit Union in Trevoze, Pa., has a big dream for his layered security network: One day, his antivirus protection, firewall, intrusion-detection system and other security tools will use integrated, intelligent [security-information and event-management](#) techniques to stop fraudulent transactions.

An early adopter and big believer in SIEM (also called security event management or security information management), Roedell believes the technology will reach its full potential only when it's integrated into application and network security tools. Today SIEM comes in the form of stand-alone tools that collect, correlate and analyze event logs across a security infrastructure. ([Compare SIEM products.](#))

Roedell's wish is on its way to being granted, says Kelly Kavanagh, research analyst at Gartner. SIEM providers are making creative strides, moving from mere log collection to intelligent analysis, he says. As an example, he points to SIEM's newest use case: application-layer monitoring for fraud detection or internal threat management. Companies are putting SIEM alongside their traditional security tools to collect and analyze application-level events or transaction logs for the purpose of discovering transaction combinations that are indicators of fraud or misuse, he says.

Roedell calls SIEM, which has more than 20 competing vendors, one of the fastest-growing security markets, having a growth rate of more than 50% in 2006 and 30% in 2007, when estimated revenue topped \$800 million. Large enterprise companies, such as CA, Cisco, EMC (its RSA security division), IBM, Novell and Symantec, have SIEM products, as do a host of smaller companies. These include ArcSight, High Tower Software, Intellitactics, LogRhythm, netForensics, Prism Microsystems, Q1 Labs, SenSage and TriGeo.

The first indications of the full integration that Roedell wants are starting to show up, too, Kavanagh says. Such companies as CA, IBM and Novell have started to bundle or integrate SIEM with other pieces of their portfolios, including identity-based access management; systems management; and IT governance, risk and compliance management offerings.

"I can prove to auditors that [the SIM appliance is monitoring] just about anything with an IP address."

MATT ROEDELL,
vice president of infrastructure
and information security,
TruMark Financial Credit Union

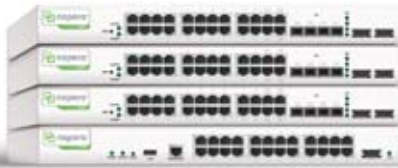
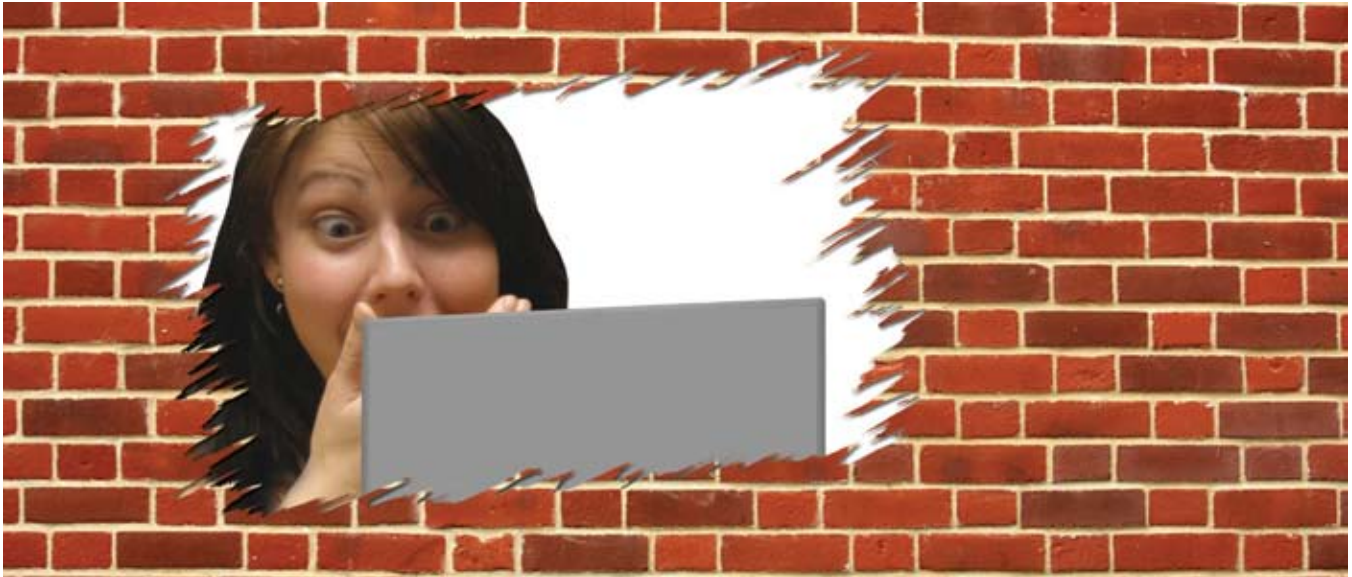
Agents on the loose

Roedell uses TriGeo's [TriGeo Security Information Manager](#) (SIM) appliance to determine the severity of threats to his company's security infrastructure. The agent-based TriGeo SIM correlates events, such as alerts about TCP port scans on the firewall or intrusion-detection system (IDS) anomalies, and sends a ticket to IT or mitigates the problem based on preset thresholds. For instance, it can end PC processes, shut down switch ports, add access lists to routers or make firewall configuration changes — actions that otherwise would require someone to log on to each device and manually update it.

Using the SIM appliance to keep such close tabs on his security network not only has made vulnerability management much easier but also has improved compliance initiatives, Roedell says. "I can prove to auditors that [the SIM appliance is monitoring] just about anything with an IP

B. PROUD

Your employees just blew up your firewall!



The Napera N24 is an appliance and integrated Web-based management service that makes sure only authorized users and secure computers access your systems.

It is the only practical network access control solution built for the small and medium enterprise. In just ten minutes, you can deploy Napera and start taking back control of your network!



Find out if your network is at risk by taking the Napera Network Test, and you could **win a free iPod nano!**

www.napera.com/products_test.php

In today's mobile computing world, laptops move in and out of your network and your users walk right around your firewall, bringing unknown threats with them.

A virus, Trojan horse, or hacker is like dynamite to your business, with just one attack costing hundreds of thousands of dollars in lost revenues, productivity and corporate reputation.

Napera plugs those holes in your firewall by:

- Making sure computers are updated and patched before access
- Quarantining unhealthy devices
- Enforcing identity
- Providing real-time visibility and reporting

address," he says.

Compliance, nevertheless, is only one factor leading to enterprises' increased awareness and adoption of SIEM tools, Gartner's Kavanagh says. Their interest also can be attributed to the technology's maturity, the decrease in its deployment and management complexity, and the availability of affordable, easy-to-deploy SIEM appliances.

Although SIEM tools have improved since earlier versions, they still can be too complicated, cautions Ted Ritter, research analyst at Nemertes Research. This is especially the case for large enterprises: "The complexity of the SIEM implementation goes up dramatically with the size and complexity of the infrastructure," he says. In a 2007 "Security and Information Protection" benchmark study, Nemertes found that 64% of 54 participants at 49 companies collected logs, but only 25% had implemented SIEM. "They said the main reason they hadn't is that it's still too complex and difficult to configure to catch the things they want to catch," he says.

Millions and billions of events

When SIEM is done well, however, threat management becomes so much easier, says Denis Hein, senior information security engineer at Wells Fargo Bank in Chandler, Ariz. He describes security management before he deployed SIEM: "We had processes in place, but they weren't enough to handle the tens of millions of events we receive daily. Four or five people were logging into separate security tools looking at information in different ways. There was no common view or correlation," he says.

In addition, Hein was frustrated with each vendor's threat taxonomy, he says. "What one firewall vendor might call critical, an IDS vendor might ignore. Although we had all these tools and were monitoring a lot more, we were still missing things," he says.

Now Hein uses [ArcSight's SIEM](#) platform to develop and apply his own logic for identifying, prioritizing and mitigating threats. "The tool has better information, so it is generating better information on threats. [That] means we can take better action," he says.

Team members can tailor their own views of the data, Hein adds. "Although we all have access to the same information, it enables us to be far more focused. For instance, one person looks only at events and information pertaining to credit-card processing, while another can focus on a virus issue, all from within the same console," he says.

Like Hein, Arlan McMillan, global head of information security operations at ABN AMRO, a Chicago financial services giant with 110,000 employees, has tapped into advanced SIEM features. "You have to get out of the narrow focus of threat vectors and get into the range of behavioral analysis. Let your point solutions worry about Trojans and viruses. [SIEM] tools take you to the next step," he says.

For example, McMillan uses the [collection and correlation features](#) of his Intellitactics Security Manager appliance to identify patterns that indicate what he calls "low and slow" attacks. "Viruses and worms like 'I Love You' and Slammer are really easy to see. What we need to get are the more sophisticated attacks," he says.

All of ABN AMRO's security endpoint data — more than a billion events a month — passes through the centralized appliance. In turn, it correlates the data and filters out such faulty information as IDS false-positives, which can be as high as 80%, and mistaken firewall patterns, McMillan says. "We then present a 'washed' version of the data to a human analyst for further investigation. If we were to give him the raw data, there would be zero expectation for consistency, reliability or repeatable processes. And if you don't have these three things, you can't set rules or check the validity of your systems," he says.

Behavioral analysis is just the beginning of what SIEM tools will be able to do in the near future, says Julio Casal, CEO of AlienVault, a support and certification provider and contributor to an open source version of SIEM. The Open Source Security Information Management project is working on advanced versions of SIEM tools in conjunction with universities.

"This market is growing so fast," Casal says. "Soon these tools will use artificial intelligence, neural networks and fuzzy logic to spot potential problems with the network based on changes, and carry out quick remediation."

Gittlen, a freelance technology editor in the greater Boston area, can be reached at sgittlen@verizon.net.

Four tips for SIEM success

1. Start with a baseline understanding of your security events.

"You have to do a risk assessment before choosing a tool to know what you need. Look at every event in your environment, ask if it's normal and then what the threshold is within a certain time frame," says Matt Roedell, vice president of infrastructure and information security at TruMark Financial Credit Union in Trevose, Pa. In addition, be sure you understand your alert and mitigation strategies, he says. Skipping this step will render your security information and event management (SIEM) product useless, he adds. ([Compare SIEM products.](#))



2. Don't bite off more than you can chew.

The "start slowly" advice for IT deployments definitely [applies to SIEM](#), says Denis Hein, senior information security engineer for Wells Fargo Bank in Chandler, Ariz. "First, bring the product in-house and test it. How it looks on paper can be quite different than how it runs in your environment," he says. Next, tackle perimeter security, he advises: "Stay conservative to make sure it holds up as you scale and add in more endpoints."



3. Establish a system for dealing with alerts.

"If you don't already have processes in place for dealing with logs, then SIEM will not improve your security posture," says Kelly Kavanagh, principal research analyst at Gartner. Unless you have a plan in place before deployment, you're sure to waste your SIEM investment, he adds.



4. Make sure executives are onboard.

"Properly define your mandate and have your executives endorse it," says Arlan McMillan, global head of information security operations at ABN AMRO, a Chicago financial services giant. "IT teams will have to cross internal organizational borders to secure logs that might be sensitive or confidential, so you need all your governance issues clearly laid out before you start deployment."



— Sandra Gittlen





Managed security services: Outsourcing threat management

As prices fall, managed security services entice enterprises looking to offload the tedious work of monitoring security systems

BY DAWN BUSHHAUS

In 2001, Incyte Corp. found itself in a quandary: The company — known at the time as Incyte Genomics — centered on selling subscriptions of its genomic-database encyclopedia to the biotech and pharmaceutical industries. As information about the human genome increasingly became part of the public domain, Incyte realized it soon could be left without its flagship product, says Roger Hoilman, vice president of IT at the Wilmington, Del.-based company. That meant Incyte had to find a way to reinvent itself.

Incyte has since refocused its efforts on drug discovery, and transitioned into a pharmaceutical company. Restructuring IT was a big part of that effort. The company went from having 900 total employees and an IT staff of 275 people, to having 200 total employees and 10 IT professionals, Hoilman says.

“There’s no way my staff can run everything 24/7/365, because we don’t have the time, and we don’t work in shifts. My strategy for keeping my head count down is to have a few people on staff who can wear many hats, and to co-manage or outsource anything I consider busy work,” Hoilman says. Among those tasks constituting busy work, he adds, was the continual monitoring of firewalls and intrusion-detection and -prevention (IDS/IPS) systems.

Cost and Complexity

Now Incyte works with managed security-services provider (MSSP) [SecureWorks](#) (formerly LURHQ) to manage its firewalls and IDS/IPS appliances — for less than it would cost the company to do the work on its own. Hoilman would need three people to monitor the company’s firewall around the clock, he says he figures. At about \$90,000 a year plus benefits for a single certified security engineer, he would have to spend more than a quarter-million dollars for firewall and [IDS/IPS](#) protection — and that figure doesn’t include the cost of hardware and software. “SecureWorks costs me a little more than half the salary of a security engineer,” he says.

Offloading busy-work and saving money also lured Boiling Springs Savings Bank in Rutherford, N.J., to the outsourcing model. The bank, a \$1.2-billion thrift with 16 locations in New Jersey, turned to [Perimeter eSecurity](#) in 2003 for managed IDS/IPS services and has since added several other services including e-mail and Web hosting.

“Security is always a catch-up game,” says Ken Emerson, senior vice president and director of strategic planning

“There’s no way my staff can run everything 24/7/365.”

ROGER HOILMAN,
vice president of IT,
Incyte Corp.



B. PROUD

Is YOUR data leaking?



SafeGuard Enterprise 5.3
NOW RELEASED!

Data encryption protects your company's critical data if it ends up in the wrong hands. Data leakage prevention solutions save you from unintentional or malicious data threats from within your organization.

Working together, **SafeGuard® Enterprise** and **SafeGuard® LeakProof™** secure all your data—at rest, in motion, and in use.

Data Encryption

+ Data Leakage Prevention

Data Security 360° by Utimaco



Utimaco Safeware Inc.
10 Lincoln Road
Foxboro, MA 02035
Phone: +1 (508) 543-1008
sales.us@utimaco.com
www.utimaco.us

© 2008 Utimaco Safeware AG. All rights reserved. SafeGuard Enterprise is a registered trademark of Utimaco Safeware AG. LeakProof is a trademark of Trend Micro Incorporated.



at Boiling Springs. "Training for security personnel must constantly be kept current; and for an organization my size, that's a very expensive proposition. An MSSP can leverage the investment in personnel and education across many users," he says.

Indeed, the complexity and expense of providing network security has led many enterprises, especially small-to-midsize companies, to seek out MSSP partners. In a recent survey of the Network World Technology Opinion Panel about security trends, 62% of 483 respondents indicated they were using a managed security service. On average, these readers said they were meeting 30% of their organizations' security needs with a managed service. Two-thirds of respondents said they expected their use of managed security services to increase over the next two or three years.

Options galore

Their options are plentiful. [Managed security services](#) are available from such established global carriers as AT&T, BT and Verizon Business, as well as from such smaller, specialty providers as Perimeter eSecurity and SecureWorks. "The market is being driven by a desire for a better-documented, process-driven security-monitoring program, and in many cases by compliance concerns," says Kelly Kavanagh, principal research analyst at Gartner.

Falling prices are fueling enterprise uptake, too, Kavanagh says. "Between 2002 and 2006, prices fell significantly, and since 2006 there has been a slow erosion of pricing," he says.

Today, pricing varies with some providers offering services à la carte

and others bundling them in packages. A firewall service offered in the cloud — which means the firewall resides inside the network and can be partitioned for more than one user — might cost a few hundred dollars a month, while a package of several customer-premises-equipment-based services that are not shared can cost \$5,000 to \$7,000 a month.

For such companies as American Nuclear Insurers (ANI), a joint-underwriting association that provides liability insurance for nuclear facilities in the United States, the latter option makes sense — but not the former. "We would draw the line at putting our data out in the cloud or trying to run applications in that mode. That would be much harder to justify," says Daniel Antion, vice president of IS at ANI, in Glastonbury, Conn.

ANI has been using AT&T's managed security services since 2006, when prices fell enough to warrant Antion's attention. "Historically when we looked into [Web and e-mail filtering] services, we simply couldn't afford them," he says. After attending an AT&T seminar on managed security services two years ago, "I was very surprised when I discovered the old 'faster, better, cheaper' scenario applied to its services," he adds.

ANI now uses AT&T's Web filtering and e-mail filtering and archiving services. Antion would consider outsourcing other infrastructure services, such as VPN and firewall, if the price were right, he says.

Bushaus is a freelance writer in the Chicago area. She can be reached at dbushaus@mindspring.com.



Access control, cont'd from page 10

atypical. For most enterprises, such a forklift upgrade is neither financially nor logistically feasible — and that makes full user-centric security hard to do.

"NAC works as advertised only if you have a single-vendor network or applications suite," Nemertes' Antonopoulos says. "Or even better, a single vendor that covers both. The problem is that everybody has Cisco and Microsoft, and until those two figure out how to work together seamlessly from Layer 1 to 7 — plus include other products, like HP and 3Com switches, Nortel VoIP systems, Oracle and SAP applications, and IBM WebSphere — [their NAC approaches] won't be useful, especially for large companies," he says.

[Standardization](#) could help, but Cisco and Microsoft are trying to advance standards to their own ends — Microsoft from the application side via the Trusted Computing Group (TCG) it champions, and Cisco from the network side via the IETF's Network Endpoint Assessment group it spearheads. "Enterprises are stuck in the middle, waiting to see what happens," Antonopoulos says.

Companies' directory infrastructure often is a stumbling block, too. Rather than simply tying the NAC implementation to a single Active Directory, as NaviMedix was able to do, many large enterprises are stuck trying to integrate several directories. "Every single organization above a certain size runs into this problem," Antonopoulos says. "They may have a legacy directory for Unix and one for Windows environments, but then they acquire Bank of Podunk, which uses a different one, so they'll try and integrate that. But before they're done, they've acquired yet another company," he says.

Managing user-centric policies and access-control lists is no picnic, either. "There is an operational complexity that can get in the way," says Joel Snyder, senior partner at Opus One and a [Network World security product tester](#). "Once you say you want to decide what access everyone has, based on who they are, you're committing to management of a security policy across all users, so every single user needs to be pigeonholed. For some companies, that's just too difficult," he says.

Enterprise IT executives also are forewarned not to get caught up in the vendor focus on endpoint security, with its patch- and antivirus-checking. A true user-centric approach means being able to monitor user behavior after network and application access are granted and authorized.

"A guest contractor plugs into the conference room, and the NAC solution says, 'OK, you're using the IDs I gave you and you have the latest software updates. Go ahead and be on my network.' That contractor can then sit back and launch a zero-day attack," says Richard [Stiennon](#), security expert and Network World security blogger. "You need post-admission controls in place — a way to identify when someone is spreading a worm and block that person's access — or you don't have true user-focused security," he says.

For now, post-admission control is a feature of smaller, single-vendor networks. This should change, however, as NAC companies begin adopting and integrating the Interface to Metadata Access Point (IF-MAP) post-admission-control [standard issued](#) by the TCG in May.

Process, not technology, is key

Even with these roadblocks, large companies can move closer to user-focused security by concentrating on processes, especially those having to do with identity life-cycle management, analysts say. They also can look to well-worn strategies, such as integrating disparate directories and implementing stronger user-authentication tools.

"Having strategic initiatives around identity management and directories, then working to integrate directories rapidly as your company changes can be much more effective approaches to identity-centric security than things like NAC," Nemertes' Antonopoulos says.

Security expert Stiennon agrees. "I would argue there isn't such a thing as full-blown NAC, and you probably shouldn't even attempt it," he says. "If you have dollars to spend on full-blown NAC, you should spend them instead on some good physical-token-based access-control system. It will get you to the same place, but cost a lot less."

Cummings, a freelance writer in North Andover, Mass., can be reached at jocummings@comcast.net.