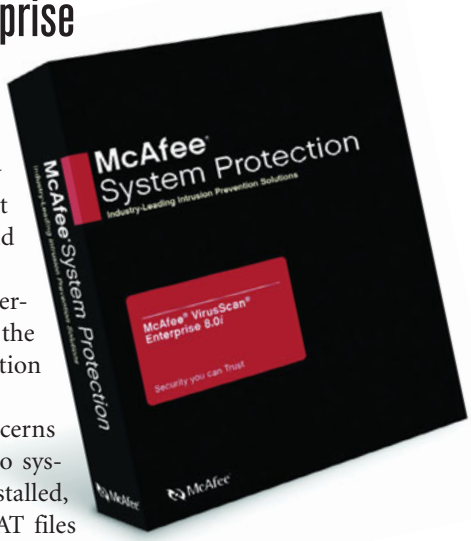
Your Picks for Best Products

Illustration by JEFF MANGIAT

GOLD | McAfee VirusScan Enterprise and AntiSpyware Enterprise

McAfee • www.mcafee.com • Price: VirusScan, $31.90/user; AntiSpyware, $12.90/user



With Microsoft getting in the antimalware game—behind free antivirus and antispyware in Vista and its Forefront Client Security business software—standalone antimalware vendors have had to adjust their strategies and improve centralized management, spyware and rootkit protection.

Readers deemed McAfee VirusScan Enterprise and AntiSpyware Enterprise ahead of the pack, praising the speed of signature updates to the product as well as its ability to detect, block and remove malware. Administration and configuration also scored well with readers.

McAfee AntiSpyware Enterprise satisfies concerns over administration by pushing its protection onto systems where McAfee's VirusScan Enterprise is installed, providing both defenses with the same engine, DAT files and management interface.

VirusScan Enterprise, like many antimalware products, moves beyond a strictly signature-based design. McAfee's tool also uses heuristics and genetic detection to provide protection from malicious code.

Another feature of the antimalware combination is its access protection rules, where customers can define how a system is used. "With [these] rules, we can lock down folders, files and processes," says Ed Metcalf, senior product marketing manger for McAfee. Metcalf suggests a user could configure VirusScan, for example, to block the execution of any non-Windows executables, close ports or prevent the alteration of any file extensions.

Users are also able to customize the update process for remote systems, and tailor updates to physical locations and connection speeds.

In addition to the management capabilities, readers praised McAfee VirusScan Enterprise and AntiSpyware Enterprise's reliability and ease of use. McAfee's focus on integration and management put it over the top. Both VirusScan and AntiSpyware Enterprise are essential parts of McAfee's Total Protection product, released a year ago. ›

HOST IPS EARNING ITS PLACE ON DESKTOPS

Once a marginal technology, host-based IPS (HIPS) is gaining traction in the market as organizations increase attention on endpoint security. In addition to behavior-based detection of unknown attacks, HIPS typically offers application and access controls. McAfee Host Intrusion Prevention and Cisco Security Agent drew particularly strong positive response in the Readers' Choice survey.

TIE

SILVER | Websense Enterprise

Websense • www.websense.com • Price: $19/seat, 1,000 users

Reporting and alerting features, as well as service and support, earned Websense Enterprise high marks and a share of the silver medal. The tool allows organizations to establish flexible Internet use policies and control Web access. The Web filtering tool categorizes sites, scanning the Internet for malicious code or potential attacks.

Websense Enterprise's policy interface enables users to organize their employees into groups and provision access accordingly. Policies can be set based on users/groups defined in Microsoft Windows Active Directory, Sun Java System Directory Server and Novell eDirectory accessed via LDAP, RADIUS and Citrix environments. ›

SILVER | Trend Micro AntiVirus, AntiSpyware

Trend Micro • www.trendmicro.com • Price: $39.95/user

Trend Micro's AntiVirus and AntiSpyware earned a share of the silver medal with high scores for its reporting and alert capabilities, as well as for its signature update features.

Trend Micro AntiVirus and AntiSpyware do real-time monitoring, automatically checking email attachments for known and unknown attacks, and issue alerts when an abnormality is detected. Scans can also be scheduled or customized. Trend Micro has trimmed false positives, the company says. It also offers deleted file recovery features, which can help users recover any quarantined files that may have been cleared out accidentally. ›


Jack Seuss

Keeping pace...for now

Security managers rely on layers of defense against malicious code.

Nobody knows more about the insidiousness of malware than a university security officer. On a college campus, CIOs like Jack Seuss are often faced with the challenge of securing thousands of computers. "There's really no single solution that's a silver bullet," says the vice president of IT at the University of Maryland. Malware defense requires a multitude of approaches.

Seuss has used a host intrusion prevention system that covers most campus desktops. He also automates patch updates on the majority of Windows machines, and has enabled campus-wide distribution of antivirus and antispyware software. Part of that layered-defense strategy includes user awareness.

While victory certainly cannot be declared, many security officers feel like they've done a decent job keeping up with malware—so far.

"[Last] fall was the smoothest in the six years I have been at Northeastern," says Glenn Hill, the university's director of information security. He says credit belongs to students and administrators who are actively protecting their computers and avoiding malware more than ever.

John Hornbuckle, network manager for the Taylor County school district in Florida, hasn't had an outbreak in some time, but he isn't celebrating yet. "Just because we're relatively safe today doesn't mean we will be tomorrow," he says.

With the stealthy nature of malware, a major problem involves actually finding the bad stuff. "A piece of malware may have a characteristic of this or that," says Jim Moore, an information security officer at Rochester Institute of Technology. "If it's a variant, is it a variant of malware A or malware B? Or did someone get the bright idea to take pieces of one and pieces of the other?"

Another sticking point with antimalware technologies is their signature-based design. "To defeat these products, all a malware author has to do is get his product distributed more quickly than updated signatures can be distributed," says Hornbuckle.

With the geometric expansion of virus variants, many are looking for more behavior-blocking technologies that monitor system and application behavior that runs contrary to policy, rather than matching characteristics with a known virus signature.

According to a recent Yankee Group report, vendors such as Prevx, Sana Security, Third Brigade and Determina specialize in this type of technology, competing with larger vendors like IBM Internet Security Systems, Symantec, Cisco and McAfee.

"I need a tool that baselines process and data flows, and detects aberrations," says Moore. "There are different ways of doing that, from heuristics to no-execute bit architectures."

As malware writers and antivirus vendors continuously try to outsmart the other, information security officers do the best they can with what's available. "We're holding even," says Seuss.

Billy Hurley is assistant editor of SearchSecurity.com. Send comments on this article to feedback@infosecuritymag.com.

MARKET OVERVIEW

GUIDANCE

Investments in signature-based products remain vital, but companies need to start looking at whitelisting and behavior-blocking technologies to repel unknown attacks.

MOVING TARGETS

Through a variety of approaches, antimalware and Web filtering products protect an infrastructure from malicious code.

Size	Corporate market in 2006: $2.6 billion Antispyware: $440 million Host intrusion prevention, behavior blocking: $85 million*
Maturity	Established
Leaders	McAfee, Symantec, Trend Micro
Contenders	CA, ESET, F-Secure, Kaspersky Lab, Panda, Sophos
Innovation	Innovators are focusing less on signature-based technology and more on heuristics, behavior blocking, herd intelligence and whitelisting. Also, vendors are looking to create more integrated antimalware suites.
Disruptions	Heuristics is hot, but false positives are a problem. Whitelisting, another alternative, requires a thorough classification of files. Defining "good" application behavior is a challenge.

*Yankee Group

GOLD | IBM WebSphere DataPower XML Security Gateway XS40

IBM • www.ibm.com • Price: $65,000

They say you never get fired for buying IBM. *Information Security* readers are in line with that thinking when it comes to securing applications running in a service-oriented architecture or Web services applications.

They made IBM's WebSphere DataPower XML Security Gateway XS40 their top choice in the application security category.

Further validating the hype over service-oriented architecture (SOA) and the standards-based XML applications around it, readers said the XS40 appliance did better than counterparts at detecting, reporting and preventing known and unknown attacks. It also scored well in integration with other security tools for remediation and reporting, and ease of installation, configuration and administration.

IBM, in 2005, acquired DataPower and its trio of products, which also includes an XML accelerator and an integration appliance. As with any SOA or Web services product, standardization is critical. In addition to the WS-* family of standards, the DataPower appliances support a new breed, including XACML, which is a standard for uniformly expressing fine-grained authentication and authorization rules. This is key with SOA applications, whose machine-to-machine interactions must properly exchange credentials to ensure a secure transaction. XACML enables companies to move authorization rules from one enforcement point to another.

"CISOs are looking at SOA in two ways—one, if the security piece isn't done right, this is a huge liability, exposing the back end to new threats and unauthorized access," says Eugene Kuznetsov, founder of DataPower. "The other part is, if you do this right, your security and compliance improve at the same time."

The DataPower appliance acts as an XML proxy that can parse and validate XML schema, encrypt XML message flows and verify digital signatures. Enterprises can use it as an enforcement point for XML and Web services interactions, providing not only encryption, but firewall filtering and digital signatures.

Some of the country's leading banks have deployed the appliance to process mortgage applications using XML or Web services, validating messages and making calls to authentication systems. It's also present in the Department of Defense for internal security between different tiers of applications and filtering messages between classified networks and applications.

"Customers are increasingly recognizing that to make applications scalable to make the business agile, you can't have security architecture teams go into every application, audit and modify it to make sure it's secure," Kuznetsov says. "There is a trend of figuring how to move security to hardware or other tiers, abstracted out of applications." ›

SILVER | SPI Dynamics WebInspect

SPI Dynamics • www.spidynamics.com • Price: $25,000

SPI Dynamics' WebInspect scans Web applications for vulnerabilities introduced during development; it's a tool that can help security managers eliminate the disconnect between coders and the security office. In according it the silver medal, readers said installation, configuration and administration of WebInspect was a breeze, potentially making it attractive to developers looking for tools they can use during coding. SPI Dynamics says it has re-architected WebInspect 7 to assess the security of Web 2.0 applications built on AJAX, JavaScript, Flash and other dynamic development languages and methods. The vendor says the re-build took three years. ›

BRONZE | Citrix Application Firewall

Citrix Systems • www.citrix.com • Price: $45,000

Citrix's Application Firewall models application behavior, then applies policy against the baseline; any application straying from the baseline is treated as malicious and blocked. In earning the bronze medal, the product scored well on preventing known attacks and vulnerabilities, as well as detecting and reporting them. It also scored consistently well in support and installation, and most respondents in this category said they were satisfied with their investment ROI. Citrix touts the product's ability to learn application behavior and generate policy recommendations. Citrix says it can be deployed as a standalone firewall or in tandem with the Citrix NetScaler Application Delivery Systems. ›


Steve Zimmerman

Necessary integration: security and development

Application security woes must be addressed in development.

Security managers are quickly adjusting to the fact that the woes plaguing today's dynamic Web applications cannot be repaired with a regularly scheduled deployment of patches from the Pacific Northwest.

The root of these problems lies in a place of integrated development environments (IDEs) and where features and functionality take precedence over security. The cure: integrating security tools and best practices into development lifecycles.

Steve Zimmerman, a former CISO for a top 10 financial institution, recalls many a pen test and vulnerability scan on homegrown Internet-facing apps delivering disturbing—but fixable—results.

"What we found is that we had excellent programmers, but a lot of them dealt with rolling out internal applications, where there's no need for the same level of security as those facing the Net," Zimmerman says. "We were finding too many errors that should have been corrected in the development lifecycle."

Zimmerman realized it was imperative to integrate security into development, something contrary to the nature of a coder. Initially, it was a bumpy road. Projects hit hurdles that extended release dates. Quickly security became a hindrance rather than an enabler.

The trick, Zimmerman says, was to approach development teams from a partnership perspective. Rather than issue mandates about their practices, Zimmerman's teams provided guidance about current threats and tools to bring security checks to the coders' efforts.

"We try to help during the process, rather than go through it at the end and fix problems," Zimmerman says. "We're not here to tell you how to create naming conventions or variables, we're here to give advice on what we see in security on the Net. We provided them with a white paper and security solutions."

Web applications are rapidly becoming a hacker's playground—most e-commerce apps connect to databases holding customer data, making them rich targets. Programming flaws like input validation errors and buffer overflows are as old as the first coding textbooks, yet those bugs often yield hackers the greatest bounty.

Couple those traditional problems with the new breed of dynamic applications powered by JavaScript and AJAX, and security managers often find themselves further behind. "Instead of static HTML, you're having more dynamic pages built. As that happens, you open yourself for holes because these things are rendered in real time," Zimmerman says. "This coding must be analyzed quicker, efficiently and the results more accurate."

Scanners have come a long way. Zimmerman, whose bank ran SPI Dynamics' WebInspect on its Web applications, says false positives have been dramatically reduced.

"When these products first hit the market, we were seeing 50 percent of returns being false positives. With the latest, we're seeing just a handful," Zimmerman says. "We were cutting pen tests down by 50 percent because we didn't have to go through as many issues as before."

Michael S. Mimoso is editor of Information Security. *Send comments on this article to feedback@infosecuritymag.com.*

MARKET OVERVIEW

GUIDANCE

Must-have technology; applications are generally a gateway to databases, and in an age of regulatory mandates, every vulnerability must be addressed.

DYNAMIC CAPABILITIES FOR A DYNAMIC MARKET

Application security scanners evaluate source code for vulnerabilities, ideally during development.

Size	$143 million in 2007 (IDC)
Maturity	Nascent
Leaders	IBM, SPI Dynamics, Watchfire
Contenders	Fortify, Ounce Labs, Klocwork, WhiteHat Security, Beyond Security
Innovation	Dynamic application scanning capabilities are imperative to counter threats caused by AJAX and JavaScript.
Disruptions	Vendors have a formidable market niche, and it may only be a matter of time before development platform vendors like BEA, Sun, Oracle and others start looking for acquisition targets.

GOLD | RSA SecurID

RSA Security • www.rsa.com • Price: $2,995 for an annual subscription

For Andy Pruitt, chief technology officer for Backstop Solutions Group, an on-demand platform for hedge funds, RSA was the only vendor that worked with the firm's particular integration needs. "They took the space seriously," says Pruitt. "[Other vendors] didn't get it. The integration level we needed was deep because we had to be able to control the administration."

Web-based services, compliance and the continual onslaught of data breaches are fueling the market for stronger authentication. As a vendor with more than 20 years experience, it came as no surprise that RSA Security and its SecurID came out on top.

The reasons it edged out its competitors: ease of use, integration and compatibility, according to readers who use the product.

When Backstop Solutions Group started to look at authentication products last July, it brought in a number of vendors. Initial meetings went well, but when Backstop started to get more specific about its needs, "that's when things started to fall apart," says Pruitt. Backstop's development environment was JBoss, "and when you are Java-based there is no comparison [between RSA and other vendors]," Pruitt says.

While Pruitt was willing to make the authentication investment because his users are high net-worth customers, traditionally cost has been a barrier to the market's widespread growth, industry watchers say.

Toffer Winslow, vice president of product management and product marketing for RSA, disagrees. While RSA SecurID tokens appear higher priced, he admits, "when you evaluate total cost of ownership and the amount of integration, we are much better [priced] than the competition," he says. Because of a rigorous certification process, RSA has been working with 300 of the top applications. "We know they work with SecurID," Winslow says.

In fact more than three quarters of readers surveyed said they were pleased with the ROI and felt they were getting their money's worth from SecurID.

And RSA has continued to innovate beyond tokens to secure other types of devices and applications. At RSA Conference 2006, the company unveiled the SecurID Toolbar Token and RSA SecurID SID900 Transaction Signing Token to secure online transactions through digital signatures. The company, now a division of EMC, also recently announced partnerships with Research in Motion, SanDisk and Motorola, among others, to use its technology to secure BlackBerries, cell phones and USB flash drives.

"The goal is to get RSA credentials everywhere," says Winslow. ›

SILVER | VeriSign PKI

VeriSign • www.verisign.com • Price: $19.95 per certificate

VeriSign took silver with its range of PKI services. The company edged out the competition due to its top scores in the ease-of-use and response categories, where more than 70 percent of readers rated it highly. During the past year the company has expanded its reach with the acquisitions of GeoTrust, an SSL certificate supplier, and SnapCentric, a provider of online fraud detection solutions that help companies comply with FFIEC regulations. VeriSign also announced its Extended Validation (EV) SSL certificates that support Microsoft's IE 7 and Vista and incorporate technology that enables Windows XP clients using IE 7 to display the same green address bar for Web site authentication as Vista clients. ›

BRONZE | ActivIdentity Smart Cards

ActivIdentity • www.actividentity.com • Price: $15-$83.25

ActivIdentity, formerly known as ActivCard, took the bronze. Readers were pleased with the scalability of its products and end user ease of use. ActivIdentity offers solutions including physical/photo ID, logical access using SSO to incorporate resources, secure remote access, and digital signature and encryption of email and documents. Within the past six months, the company has broadened its solutions for the Sun, Novell and Microsoft platforms. It recently bolstered its health care suite with SecureLogin Kiosk and announced that its Mini Token OE and ActivIdentity Authentication SDK support the HMAC One-Time password algorithm developed by OATH. ›

Token support isn't enough

Hidden costs can derail strong authentication rollouts.

Implementing strong authentication is about planning, education and simply accounting for the foibles of human nature.

One of the most common stumbling blocks is user acceptance and the resulting support costs to roll out such an implementation.

"It simply makes authentication harder," says Peter Gregory, a senior security specialist at a company that provides on-demand business services. "There are more pieces on the critical path for a user who needs to access systems.

"There are difficulties simply because people can't find the token, they lose the token, they accidentally drop the token in water, etc. All of this translates into support costs," says Gregory.

As a result, security managers should have a detailed, mapped-out plan, according to users who have gone through this process.

"Support personnel including help desk and desktop services must be ready to field calls from users who are confused," says Ron Woerner, information risk manager at ConAgra Foods.

Gregory agrees, and adds that companies need to account for all the hidden costs. The cost of implementation—getting people trained, provisioned and supporting them—probably exceeds the cost of the token itself.

Depending on the size of the organization and type of authentication used, training can be cumbersome.

Training and rollout can be especially difficult when large organizations try to do it en masse. "It's usually an all-or-nothing deal," explains Woerner. "In large organizations, it requires a lot of coordination to ensure there are no gaps."

Furthermore, with today's highly distributed workforce, logistical rollouts aren't simple. You can't walk down the hall and hand out tokens. It makes it more time consuming, Gregory says.

And while the second factor provides additional security, it is not foolproof. "For fobs or number generators, there is still a worry that the second factor does not necessarily ensure that it is really the user in question. I can steal a fob and with some other social engineering I can log in to the system," says Ernie Hayden, CISO of the Port of Seattle.

For that reason, biometric devices are more secure, but also come with their own headaches, Hayden says.

A headache to avoid is a biometric implementation that doesn't integrate with Active Directory or the GINA (Graphical Identification and Authentication) for Windows systems—the primary systems used for user authentication. "You need to be absolutely sure that all aspects of privacy are addressed in the specification, procurement and implementation," says Hayden.

Strong authentication "isn't a panacea but it does close one of the avenues of weakness," says Gregory.

Kelley Damore is editorial director of Information Security.
Send comments on this article to feedback@infosecuritymag.com.

MARKET OVERVIEW

GUIDANCE

Stay put—depending on your needs and applications, you may want to wait and see what innovation takes hold in 2007.

WHO ARE YOU?

Hardware or software technology, or service, for determining whether someone or something is, in fact, who or what it is declared to be. This includes PKI, RADIUS, biometric products, and soft and hard tokens.

Size	$1.1 billion for 2007. Includes traditional token market and advanced authentication market; does not include services and smart cards. (IDC)
Maturity	Established
Leaders	RSA Security, VeriSign, Aladdin Knowledge Systems, ActivIdentity, Entrust, Gemalto, SafeNet, Secure Computing, VASCO, Juniper Networks, Arcot Systems
Contenders	Bharosa, Corillian, Imprivata, Utimaco, Verid
Innovation	New regulations such as FFIEC portend more cost-effective innovative offerings in the consumer authentication marketplace.
Disruptions	Technology can be expensive. Customers don't want to pay extra and are not inclined to carry a token or smart card. Market won't take off until the fraud incurred outweighs the technology costs.

GOLD | Symantec Database Security

Symantec • www.symantec.com • Price: Appliance, $10,000; software, $5,000 per CPU for Windows, $10,000 for Unix

Symantec has been quick to assert itself in the growing database security market, with a new auditing and monitoring product that resonates with its customers, earning a Readers' Choice gold medal.

Respondents gave Symantec Database Security high marks where it counts, overwhelmingly rating it excellent or good in protecting their data. Almost as important, they gave it high marks for ease of installation, configuration and administration, a major factor as organizations struggle to integrate new security tools without additional management resources. The product passively sniffs traffic and stores audit data offline, causing zero impact on database performance or availability.

"There's no overhead on production servers—that's a key for us," says Ayad Shammout, lead technical database administrator for CareGroup Healthcare System, which manages four Boston-area hospitals. "And we don't want to deploy agents. They're a headache to manage."

Users also like the product's scalability and its minimal impact on existing infrastructure.

Symantec Database Security sniffs database traffic, detecting anomalous behavior from insiders or external sources, which may be malicious or simply authorized personnel failing to follow procedure. It does this by running in learning mode to build a profile of normal behaviors, allowing managers to distinguish between unauthorized and acceptable activity.

The product continuously monitors database activity, firing off alerts and enabling security managers to quickly investigate and mitigate issues. Organizations can use it in a variety of ways: to protect confidential data, detect fraud activity, monitor and confirm change management procedures and prepare comprehensive reports for auditors.

While the IT/security giant has been drawing attention for a wave of acquisitions, Database Security is a homegrown product, developed by Symantec's Advanced Research Group, which is "like a small startup within Symantec looking for new opportunities in emerging markets," says Gautam Vij, senior product manager, Symantec Database Security. Symantec has spent close to four years in development, he says.

Although Database Security was initially rolled out as an appliance, Symantec, consistent with its new strategy, will continue to develop and market it as software, working with OEMs. ›

SILVER | AppDetective

Application Security • www.appsecinc.com • Price: $900 annually per database

It's a safe bet your critical databases are vulnerable to attack, and AppDetective, one of a handful of specialized vulnerability scanners on the market, performs its job so well that readers voted it silver medalist in the database security category. AppDetective, available as a standalone product or as part of the DbProtect suite with AppRadar, a database monitoring tool, scored high among readers for its integration and compatibility with existing infrastructure, an important point for vulnerability scanners, which are often seen as intrusive, even disruptive. Readers also liked AppDetective's reporting and alerting capabilities. The network-based scanner simulates attacks, performing penetration testing to discover vulnerabilities and misconfigurations. It can also perform security audits, determining vulnerability to internal misuse. ›

BRONZE | SecureSphere Database Security Gateway

Imperva • www.imperva.com • Price: Starts at $45,000

This database monitoring, auditing and protection appliance drew strong approval from its customers, rating very well across the board to earn the bronze. SecureSphere scored well in every criteria: granularity of access controls and integration with existing infrastructure, scalability and management, data protection, customer support and alerting and reporting. Respondents said they're getting their money's worth. SecureSphere assesses databases by profiling normal behavior in learning mode, and detects anomalous behavior based on that, as well as built-in and custom policies. It offers an enforcement capability, giving organizations the option to automatically block select unauthorized activities. In addition, its integrated IPS protects against attacks on known vulnerabilities in database platforms and operating systems. ›

The heart of the business

Databases contain the lifeblood of your business; preventing data breaches and satisfying demanding auditors can be a resource-draining exercise in frustration without the right tools.

Security is at the core of all operations when you're in the business of producing enriched uranium for commercial power plants, but as a publicly traded company, USEC faces the same challenges as other corporations satisfying SOX requirements for strong controls over its financial databases.

"We had to monitor access to privileged accounts, primarily for financial systems," says David Vordick, USEC's CIO. "We had to be sure of our internal controls for privileged users, primarily DBAs, to be sure they weren't misusing that right.

"Our SOX audit has gone well," says Vordick, who has been using Guardium's SQL Guard database monitoring and auditing tools for about 18 months. "The technology was a key part. The solution is identified in our internal controls, and we had no problems."

Regulatory pressure is driving many corporations to deploy database security tools, and they are keenly aware that an embarrassing breach of sensitive nonpublic information can severely damage their business.

"We have key databases with phone records, personal information and credit card numbers used by call centers," says Christopher Knauer, vice president of information security for Vonage, which recently deployed RippleTech's Informant database monitoring product. Notably, information security falls under the legal department at the VoIP phone service provider. "At lower levels, access is very restricted, but we have concern at higher levels of access—we want to know exactly what they are doing."

Database security is not for the faint of heart. Even with the best processes and policies in place, organizations are hard-pressed to wade through mountains of logs or crawl through databases without the right tools to verify security controls and expose vulnerabilities, access violations and fraud.

"Our system has 35 schools, large and small. At small schools, the DBA may also be the programmer and the Web master," says Scott Woodison, IT audit manager for the board of regents for the University System of Georgia. Using Application Security's AppDetective database vulnerability assessment tool helps Woodison to act as a roving pen tester throughout the system.

"We had a huge logging problem, devoting an FTE to manually review gigabytes of daily logs and produce reports," says the security manager for a mid-market financial institution. "Auditors were not impressed with manual auditing of 20 to 30 databases and less than thrilled with the accuracy of the human brain to parse through millions of lines from logs."

The financial institution bought Imperva's SecureSphere tools to help bring the process under control. ▸

Neil Roiter is senior technology editor for Information Security. *Send comments on this article to feedback@infosecuritymag.com.*

MARKET OVERVIEW

GUIDANCE

Regulatory compliance, particularly Sarbanes-Oxley for demonstrating and reporting controls on financial databases, are compelling organizations to deploy automated database monitoring tools.

KEEPING WATCH

Database security products protect and monitor assets stored in a database from unauthorized access from malicious outsiders or trusted insiders. Products not only secure access to a database, but can encrypt its content.

Size	Estimates from less than $100 million to $300 million-plus
Maturity	Developing
Leaders	Application Security, Guardium, Imperva, Lumigent, Tizor
Contenders	Embarcadero, Ingrian Networks, IPLocks, Symantec, Vormetric
Innovation	Continued improvement in native database security
Disruptions	Carefully evaluate products' impact on database performance and availability before deploying.

GOLD | Symantec Network Access Control

Symantec • www.symantec.com • Price: $18,000

Network access control for several years has been the most overhyped product category in the security industry, inheriting the title from previous champion PKI. Although vendors have promoted their wares as the next big thing, few have actually delivered any working products. Among those that have brought a system to market is Symantec, winner of the gold medal for endpoint security with its Network Access Control offering.

Symantec Network Access Control, like most similar offerings, uses a server-and-agent architecture in which an agent is installed on each endpoint on the network and administrators handle policy creation and enforcement from a central console. When a protected device connects to the network, the agent performs a series of integrity checks on it to determine whether it complies with corporate policy.

Readers gave the product high marks for its enforcement options, ability to integrate with the existing infrastructure, as well as its logging and reporting capabilities.

Administrators can design policies that require certain patch levels, antivirus signature versions and personal firewall settings before access is granted. Symantec Network Access Control also ships with some canned policy templates. If a device is found to be noncompliant, the system can bring the machine into compliance by applying required patches or other protections before allowing it full access to the corporate network.

Symantec's product also has the ability to enforce policy on machines even when they're not connected to the network. And when an unknown device attempts to connect to the network via an SSL VPN, Web application or wireless switch, the system can install an on-demand agent to ensure the machine is within the accepted policy. It also includes support for 802.1x authentication over wired and wireless networks, as well as DHCP for LANs and wireless LANs. Interestingly, Symantec also has included support for Cisco's Network Admission Control agent.

The Symantec system gives customers the flexibility to use either a software and hardware approach or go with software only. The hybrid option requires the Symantec Sygate Policy Manager software and the Symantec Enforcer appliance, a 1U rack-mountable box that runs on a hardened version of Red Hat Linux ES 3.›

SILVER | Cisco NAC

Cisco Systems • www.cisco.com • Price: $6,000-$40,000

Cisco Systems recently changed gears on its Network Admission Control platform and began focusing its efforts on the NAC Appliance, formerly known as Cisco Clean Access. The company had been touting a more complex NAC system, which required expensive upgrades to routers and switches, but the cost and complexity of the system was an obstacle for many enterprises. The shift to the NAC Appliance has paid off, as Cisco pulled down the silver medal in the endpoint security category.

The appliance uses the network infrastructure to enforce security policy, authenticate and authorize users and evaluate and remediate wired and wireless devices before they are allowed full access to the network. The NAC Appliance not only has the ability to recognize devices, but also can identify individual users and their respective roles in the company, allowing it to make informed decisions on resource access.›

BRONZE | McAfee Policy Enforcer

McAfee • www.mcafee.com • Price: $30 per host

Antivirus and intrusion prevention powerhouse McAfee garnered the bronze medal for its Policy Enforcer product. Policy Enforcer boasts all the features of other NAC systems, but is a software-based system and not an appliance. It's designed to be installed at various points across a network and integrates with the company's ePolicy Orchestrator management console for policy enforcement and effective control.

Policy Enforcer can discover managed and unmanaged devices on a network, and perform automated remediation in order to bring managed machines up to approved levels. McAfee also decided to include support for all major NAC enforcement frameworks in Policy Enforcer—Cisco NAC, Microsoft NAP (Network Access Protection) and the Trusted Computing Group's TNC (Trusted Network Connect). This gives administrators the flexibility to use whatever scheme they like best, without needing to replace agents or hardware.›

A NAC for access control

Network access control technology is fine for evaluating system health, but IT wants to extend those capabilities to users, not just machines.

NAC and other endpoint security technologies have garnered a lot of press and attention in the last year, and much of that attention has focused on the products' ability to check the security posture of machines attempting to connect to the network. Vendors have touted the ability to admit or deny users based on the relative health of their machines as the key to keeping their networks clean.

However, some users say that while the health check capability is all well and good, the true value of network access control lies in its ability to limit network access for specific users, and not just their machines. Deployed at strategic points inside a network, and not simply at the network edge, NAC systems can function as gatekeepers and prevent unauthorized users from accessing network segments or resources they're not meant to see.

"What I was looking for was an admission control system that could automatically assign users to a VLAN based on the user, not the machine," says George Owoc, director of business administration at EADS Astrium North America, a manufacturer of satellites and other space systems. EADS Astrium uses a NAC appliance from Lockdown Networks. "We have a lot of contracts that are controlled by the State Department because of export issues and a lot of classified material," Owoc says. "We also have a lot of interns and students and we had to make sure that we didn't have any unauthorized access."

This access-control role in the past has been played with varying levels of success by inward-facing firewalls and simple password protection on sensitive servers. In some cases, classified or otherwise restricted material is placed on a separate network, but this approach can hamper the ability of legitimate users to access files. So NAC systems have begun taking over that function in some large, distributed enterprises like EADS Astrium with clear needs to segment their user populations.

"I needed a way to isolate visitors and others by their access to data," Owoc says. "And I didn't want something with a client, because the administrators of those visitors' machines have locked them down as much as they can, and probably have them set to deny any software that's pushed down to them."

The forthcoming NAC-NAP offerings from Cisco Systems and Microsoft will be uniquely well positioned to perform this access-control function as well. Cisco's position as the provider of networking infrastructure for many enterprises, and Microsoft's equally dominant position in the server realm, give them the ability to determine who can access what resources and when. ›

Dennis Fisher is executive editor of TechTarget's Security Media Group. Send comments on this article to feedback@infosecuritymag.com.

MARKET OVERVIEW

GUIDANCE

Organizations should ensure NAC products support 802.1x, VLAN capability and the Cisco NAC agent, rapidly becoming the industry standard. Enterprises should avoid niche vendors; many will soon disappear as the market consolidates.

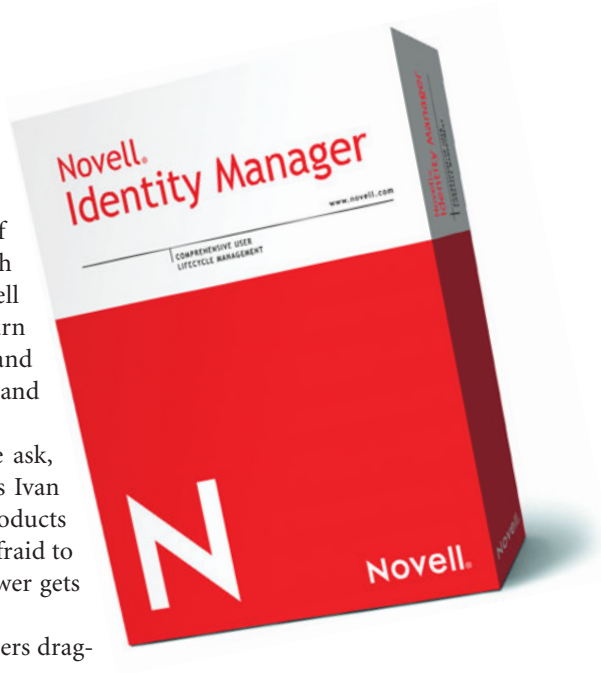
RIPE FOR THE PICKING

Network access control products are designed to perform a health check on PCs as they connect to a network and ensure they have the proper patch levels, antivirus signatures and other security measures.

Size	$340 million in 2007 (Internet Research Group)
Maturity	Nascent
Leaders	Cisco Systems, Vernier, Symantec
Contenders	Microsoft, McAfee, Lockdown Networks, Juniper Networks
Innovation	The next step will be a move away from third-party, appliance-based offerings and toward integrated solutions, such as Microsoft's NAP and offerings from Enterasys and others.
Disruptions	Many enterprises are delaying plans to deploy NAC until Microsoft and Cisco fully flesh out their respective offerings and partnership. SMBs are making the bulk of the purchases today, but if Microsoft and/or Cisco fail to produce a high-quality NAC solution, enterprises may turn to the smaller vendors.

GOLD | Novell Identity Manager

Novell • www.novell.com • Price: Server, $75,000; Per user, $25



Novell says it has invested plenty to simplify the usability of its Novell Identity Manager product. Readers responded with a bevy of high ratings to earn Novell the gold medal. Novell Identity Manager earned high marks for scalability, return on investment, integration and compatibility, extensibility and breadth of platforms, applications and domains supported, and vendor service and support.

"We spoke with end users and managers and we'd hear people ask, 'How much consulting will I need to get it up and running?'" says Ivan Hurtt, product and marketing manager for security and identity products at Novell. "We had a lot of people who liked the product but were afraid to use it. If people don't know how to use the technology, all that power gets wasted."

Novell Identity Manager offers graphically based tools that let users drag-and-drop and create "what-if" scenarios.

"You can test it for a shorter period of time with a higher level of certainty, and then roll it out more aggressively," says Hurtt.

If users come to an Error 404 page, Novell Identity Manager creates a workflow request to the owner of the content rather than posting the usual dead end. On the other side, the owner can see the requester's attributes, decide if he or she deserves access to the content, and receives a report to show auditors.

Once all connectors, roles and policies are in place, Novell Identity Manager, with one click, can create a 250-page PDF file for auditors that includes workflows, access rights and style sheets that are innate to the system. Any changes made to the end user's network are instantly recorded in the file.

Continuum Health Partners in New York City installed Novell Identity Manager 13 months ago for messaging and file and print services. It already has added 21,000 identities, and is building drivers to the organization's downstream systems that will allow for provisioning and automatic attribute sharing of information like phone numbers in the GroupWise directory. "It's worked out really well for us and our HR people like it too," says Ken Lobenstein, CTO of Continuum.

Organizational buy-in is key because HIPAA requirements make access management a company-wide issue. Lobenstein got Novell Identity Manager running in six months so other departments could see quick results.

SILVER | RSA ClearTrust

RSA Security • www.rsasecurity.com • Price: $26 per user

RSA ClearTrust—now known as Access Manager—enables single sign-on for customers, partners and suppliers, combining Web access management with role-based provisioning. Readers gave RSA ClearTrust high marks for extensibility across platforms, applications and domains, as well as for ease of use and end-user transparency. RSA touts the product's ability to integrate within a heterogeneous environment of Web and application servers with native support for directory servers and databases. Users also have self-service features for account creation, group assignments, profile updates and password resets.

BRONZE | Oracle Identity Management

Oracle • www.oracle.com • Price: $80 per user

Oracle Identity Management has a full suite of identity management capabilities, including single sign-on and Web access control, provisioning, federation, directory services, strong authentication and development toolkits. Readers rated Oracle Identity Management highly for its return on investment and scalability. Oracle says the software runs on top of your existing directory, or with Oracle's virtual directory, which also enables an enterprise to combine directories and make them look like a single entity. One area readers say Oracle Identity Management could use work is extensibility and breadth of platforms and domains it supports.

The politics of IAM

Security managers need time to implement identity management, while business units want immediate results.

When it comes to getting the most of your identity and access management system, IT directors must first ask: How quickly do you need to score a victory with your colleagues?

"A decision needs to be made about the political nature of your organization, and whether you need to look for quick wins" with your IAM product, says Ken Lobenstein, chief technology officer and chief security officer with Continuum Health Partners in New York City.

Lobenstein believes it takes two to three years for organizations to best implement and utilize identity and access management. Of course, other departments in your organization might not want to wait 24 months to see the fruits of the IT department's latest endeavor. That's especially true with IAM, with regulatory pressures requiring IAM capabilities.

Lobenstein understood he needed a quick victory when the hospital network he works for bought Novell Identity Manager one year ago. Within six months he had the Novell device managing the identities of 400 new residents across three databases. With more than 21,000 users, that may not sound like a big victory. But his co-workers were pleased, and that initial triumph kept enthusiasm alive for the ongoing implementation.

Looking for the quick victory "makes it harder and it takes more time for the business people in my office up front because they have to talk more about the installation in the first year," says Lobenstein.

However, Lobenstein's quick victory was not without setbacks. "The pain was that we didn't have business rules fully developed as we implemented it, so we had to rebuild our drivers two or three times because they didn't quite work," he says.

To avoid such problems, companies need to figure out what they want out of their IAM product before buying one. "Start small and don't try doing every single application," says Karl Jackson, an IT software engineer at Brigham Young University in Provo, Utah.

Jackson has used CA eTrust Identity and Access Management Suite for five years to manage the university's administrative computing needs. He started primarily with provisioning but branched out with the product as new challenges arose. "It's grown in terms of integration as I've grown more comfortable with it," he says. "Components like access control and SiteMinder [Web single sign-on] and eTrust Administrator [provisioning, password management] are integrated. The trick is taking what I've got and leveraging that integration."

Dave Young, program director of Web services with Geisinger Health System in Danville, Pa., spent nearly a year defining how he wanted to implement identity and access management before he shopped for a vendor. "You can't just take the product out of the box," says Young, who chose RSA Security's RSA ClearTrust. "You need policies behind the product."

Young, for example, needed a device that created different password requirements for various user groups. RSA ClearTrust lets employee passwords expire every six months, but patient passwords never expire.

Ira Apfel is a freelance writer based in Washington, D.C. Send comments on this article to feedback@infosecuritymag.com.

MARKET OVERVIEW

GUIDANCE

Must-have technology; compliance and auditing mandates make identity management indispensable.

IAM IN DEMAND

Identity and access management helps users log on to networks, check credentials, manage passwords and provision access to assets and systems.

Size	$3 billion (2005, IDC)
Maturity	Mature
Leaders	IBM, Sun, HP, Oracle, Novell, RSA
Contenders	Bridgestream, M-Tech
Innovation	Digital identity, biometrics, smart cards
Disruptions	Unified digital identity could dramatically change the field.

GOLD | TippingPoint Intrusion Prevention System

TippingPoint • www.tippingpoint.com • Price: $4,995-$169,995

One of the most critical components of any IT security program is the ability to detect or prevent network intrusions before the attacker is able to do real damage. Asked which IDS/IPS system best meets the challenge, readers gave the highest marks to TippingPoint's Intrusion Prevention System (IPS).

The TippingPoint IPS is an inline device that gives packets a thorough inspection to determine if they're malicious. This instantaneous protection is the most effective means of preventing attacks from reaching their targets, says Neal Hartsell, TippingPoint's vice president of marketing. TippingPoint is a division of 3Com.

"Customers are looking for an inline device that actively takes malicious traffic out of their network—plain and simple," he says. "Customers come to us and say they want the traffic removed in a transparent way that doesn't affect network infrastructure or user connectivity."

> "Customers are looking for an inline device that actively takes malicious traffic out of their network—plain and simple."
>
> –NEAL HARTSELL, VP of marketing, TippingPoint

According to the vendor's Web site, TippingPoint IPS provides application, performance and infrastructure protection at gigabit speeds through total packet inspection. Application protection capabilities provide fast, accurate, reliable protection from internal and external attacks. The product is designed to protect VoIP infrastructure, routers, switches, DNS and other critical infrastructure from targeted attacks and traffic anomalies.

The system is built upon TippingPoint's Threat Suppression Engine (TSE)—a hardware-based intrusion prevention platform consisting of state-of-the-art network processor technology and TippingPoint's custom ASICs. The TSE architecture utilizes a 20-Gbps backplane and high-performance network processors to perform total packet flow inspection at Layers 2-7. Parallel processing ensures that packet flows continue to move through the IPS with a latency of less than 84 microseconds, independent of the number of filters applied.

SILVER | Symantec Network Security 7100 Series

Symantec • www.symantec.com • Price: $11,300

The silver medal is readers' sendoff for the Symantec Network Security 7100 Series intrusion prevention appliances. Symantec announced last year it was getting out of the appliance business; through a partnership with Juniper, Symantec will provide IPS signatures for Juniper UTM boxes.

The appliance, powered by Symantec's Intrusion Mitigation Unified Network Engine (IMUNE), combines protocol anomaly, signature, statistical and vulnerability attack interception techniques to keep known and unknown attacks from spreading throughout networks. Symantec says the appliance requires no network reconfiguration and supports aggregate network bandwidth from 50 Mbps to 2 Gbps to meet deployment needs at branch offices, distribution sites and the network core.

BRONZE | Juniper Networks IDP

Juniper Networks • www.juniper.net • Price: $9,000-$60,000

Juniper Networks' Intrusion Detection and Prevention (IDP) is an inline appliance, and readers praised its low rate of false positives. Juniper says its IDP targets vulnerabilities, not attacks, in warding off zero-day attacks and known worm, Trojan and spyware attacks.

The device also provides information on rogue servers and applications that may have been unknowingly added to the network. Administrators can have the Juniper Networks IDP enforce application usage policies or check if the resource usage meets desired application policies. A centralized, rule-based management approach offers granular control over the system's behavior with access to extensive auditing and logging, and fully customizable reporting.

The Juniper Networks IDP product line includes Juniper Networks IDP 50, 200, 600 and 1100 for small to large enterprises.


Dave Bixler

The trouble within

IT pros have two big headaches when it comes to intrusion defense—getting support from upper management and getting users to clean up their computing habits.

Ask IT professionals which intrusion defense challenges keep them awake at night and few will mention the performance of their IDS or IPS devices or the tenacity of remote hackers.

Sure, for some users, headaches abound when it comes to their IDS devices giving off false positives and needing too much configuring. Dave Bixler, CISO for Siemens Business Services, says it was too much trouble tuning his IDS and babysitting it 24/7 to ensure it was properly monitoring everything. So he outsourced those tasks to a MSSP.

"We cured our pain points by passing the buck," Bixler jokes. "We decided to do this because of our earlier experiences with IDS/IPS, the expertise required to adequately tune it and the need for 24/7 monitoring, plus the added overhead of proving to auditors that we responded to every alert made."

For most IT security pros, however, the biggest obstacles to an adequate intrusion defense don't come from imperfections in their IDS or IPS. They come from executives who don't always understand the need for security investment or employees whose computing habits make it easier for the bad guys to steal sensitive data.

Of 307 IT professionals who took a SearchSecurity.com survey on intrusion defense early last year, 50 percent cited a lack of upper management support as a problem, while 71 percent cited cash constraints. Jon Payne, vice president of IT at Wild Oats Markets, and other IT professionals have found that top brass can be won over by explaining how certain investments and policies could boost regulatory compliance efforts and prevent a headline-grabbing security breach.

Dealing with the rest of the workforce is another matter. They may leave USB keys with sensitive data in hotel rooms and airplanes, lose laptops, or open malicious attachments.

To deal with that problem, Bixler and other IT professionals rely on user education programs and an array of security devices—everything from IDS and IPS to antivirus software and firewalls, content-scanning filters and vulnerability management tools. That way, if an intruder punches through one end of the network, he can be stopped by devices and procedures deployed in other parts of the network.

City of North Vancouver IT manager Craig Hunter agrees user education is important. But he says the average employee will never become an infosecurity expert. That's why good security technology is important.

"The best you can do is embed security into systems so the users don't see it," he says. His philosophy: "Make it easier for users to do it right than to do it wrong."

Bill Brenner is senior news writer of SearchSecurity.com. Send comments on this article to feedback@infosecuritymag.com.

MARKET OVERVIEW

GUIDANCE

Figure out security goals before buying an IDS/IPS device. Remember that intrusion defense involves a wider array of technology such as antivirus software, vulnerability management tools and firewalls.

DETECTING AND PREVENTING SUSPICIOUS ACTIVITY

IDS technology monitors the network, detects suspicious activity and alerts the user. IPS technology is designed to prevent suspicious activity.

Size	$1.6 billion (Infonetics Research)
Maturity	Established; widely used, especially among larger enterprises
Leaders	Internet Security Systems (a division of IBM), Sourcefire, TippingPoint (a division of 3Com), McAfee, Juniper, Cisco
Contenders	Lucid Security, Reflex Security
Innovation	Stagnant; perhaps most noteworthy is Sourcefire's RNA technology, which brings network context to intrusion alerts.
Disruptions	Tuning the devices and setting the right policies can be tricky. False positives are often a problem.

GOLD | Postini Perimeter Manager

Postini • www.postini.com • Price: $15 to $20 per user

Postini Perimeter Manager's gold medal in the messaging category is a victory for security sold in an on-demand model.

The product safeguards enterprises from malicious email and instant messages without the need for software installations, hardware deployments or on-site configuration. Readers lauded the product's uptime, noting that outages were kept to a minimum. The on-demand model results in cost savings, and it's headache free, says Sundar Raghavan, Postini vice president of solutions marketing.

"You can manage policies in one central location in a Web browser with a check of a box," Raghavan says. "Once a link is established with our customers, we track all email and IM messages in real time and they're archived in our world-class data centers."

The company started in 1999 and quickly gained momentum around its on-demand model for secure email, archiving and spam-blocking features. Perimeter Manager blocks spam, viruses and phishing attacks. The platform provides filtering, multiple redundant layers of threat protection, and administrative controls to manage messages and enforce policy.

Archiving also helps companies meet more stringent federal discovery rules around electronic data, Raghavan says. The new rules, which went into effect Dec. 1, require companies to keep track of email, instant messages, BlackBerry messages and other electronic data that could become relevant to a federal court case.

Postini's archiving system gives employees a personal archive, which provides access to email and IM chat searching. Searching also extends to file attachments that may have been exchanged, Raghavan says.

More Postini customers are also choosing to add Perimeter Manager instant messaging security features to their lineup. The IM extension stops IM-borne worms, viruses and spim from reaching the network. Administrators can also set IM access policies, control outbound IM file transfers, filter conversations for inappropriate or sensitive content, and archive instant message sessions for searching and retrieval. The software uses integrated filters from Symantec to filter spam and spim and block malicious URLs. Perimeter Manager is also automatically updated every minute, without interaction from IT staff. In addition to IM, Raghavan sees VoIP and video conferencing security to be in Postini's future product set. ›

SILVER | Microsoft Antigen

Microsoft • www.microsoft.com • Price: $10.50 per user

When Microsoft acquired Sybari Software in 2005, security pros wondered whether it would lead to the demise of Sybari and its flagship Antigen email security product. Microsoft, however, hasn't tinkered much with it because of strong interoperability with Microsoft Exchange. Antigen, which finished second in the messaging category, has been rebranded and wrapped into Microsoft's Forefront line of security products. The software uses a layered, multiple scan engine approach and is integrated with Microsoft Exchange, SharePoint and Live Communications Server. Antigen provides server-level antivirus, antispam and content-filtering features. The software protects Exchange 2000 Server, Exchange Server 2003, SharePoint Portal Server 2003 and Windows SharePoint Services 2.0. ›

BRONZE | IronPort C series, X1000

IronPort Systems • www.ironport.com • Price: $3,000

IronPort says its Reputation Filters, a key component of its C series and X1000 email security appliances, block 80 percent of spam at the connection level. The antispam scanning feature also blocks unwanted messages by reviewing the context of a message, including its construction method and the reputation of the sender. It also has a built-in URL scanning feature that investigates URLs within a message body to assess trustworthiness. Like most of its competitors, IronPort software is automatically updated to eliminate manual tuning and maintenance. Administrators can also configure the software to set user- and group-specific policies. End users can access spam digests to check and manage messages flagged as spam.

Cisco Systems, which acquired IronPort in January, says IronPort will be a separate business unit, and its features eventually integrated into Cisco's network security platform strategy. ›

Taking aim at IM security

Securing IM takes on many forms, from investments in enterprise-class IM clients, to outright prohibition of IM use.

Security pros are grappling with ways to make sure critical corporate data doesn't slip beyond the company firewall through the growing use of instant messaging (IM) clients in the workplace.

Regulatory pressure to archive messages is also forcing enterprises to extend their messaging security investments—limited today to inbound and outbound email—to IM. Some firms are deploying enterprise-class IM clients, others have initiated strict controls and policies to warn employees of unauthorized use, and others are outright banning IM clients.

"We've done our best to educate people in terms of appropriate use of IM clients, but everybody uses their commercial IM product and they use it all over the place," says Chris Ranch, director of network architecture at Affinity Internet. This year the Web and e-commerce vendor plans to introduce its 275 employees to an enterprise messaging system that encrypts and stores IM conversations on company servers.

"IM security is absolutely critical," Ranch says. "We want to gain control without pulling the plug on everybody."

Security pros are looking for products that detect and block spam over IM (spim) as well as phishing attempts, viruses and spyware in messaging traffic. Archiving chat conversations and the ability to build comprehensive reports with messaging data also are needs. Experts say many companies are turning to enterprise-class IM clients with fully integrated security features.

Jeff Carnahan, a messaging solutions architect at a Midwestern bank, says his company has been in control of its instant messaging security since it deployed IBM Lotus Sametime software in 1999. It started with 4,000 employees using IM, but now the bank's 50,000 employees have access to the IM client strictly for internal communications, he says. It also deployed archival and storage software from FaceTime Communications.

"There's definitely some concern about chat sessions, but the benefit of internal instant communications has been more of an advantage than a disadvantage," Carnahan says.

Disintegrating employee productivity forced Chad Richards, IT director at Riverton, Utah-based Stampin' Up!, a seller of wood-mounted rubber stamps and accessories, to pull the plug on IM use. After reviewing company chat IM logs, Richards says that one of 10 messages were legitimate work-related chats.

"While I see a lot of potential benefits, distractions and difficulties in managing IM far outweigh the benefits," Richards says. "It took a constant policing effort, and it had a negative impact throughout the company."

Robert Westervelt is news editor of SearchSecurity.com. Send comments on this article to feedback@infosecuritymag.com.

MARKET OVERVIEW

GUIDANCE

Growing regulatory pressure makes ongoing investments in messaging security products a must. IM must be addressed, either with enterprise-class clients, or banning IM altogether.

CAREFUL COMMUNICATION

Messaging security products monitor email, IM and voice over IP traffic for malicious code, and filter content for policy violations. Some offer archiving features to satisfy regulators.

Size	$1.1 billion in 2007
Maturity	Established
Leaders	Symantec, McAfee, Microsoft
Contenders	Trend Micro, IronPort (Cisco), Secure Computing, Postini, Message Labs, Proofpoint, FaceTime
Innovation	Technology will improve to better address instant messaging security, VoIP and video conferencing security.
Disruptions	Heavy consolidation is resulting in small best-of-breed vendors getting gobbled up by large messaging infrastructure vendors.

GOLD | Cisco PIX Security Appliance Series

Cisco Systems • www.cisco.com • Price: $40,000

Cisco has been in business for more than 20 years and is emerging as a security powerhouse to be reckoned with, especially as security merges more with network operations in the enterprise.

"Cisco has been benefiting from recent market changes," says Jon Oltsik, a senior analyst with market research firm Enterprise Strategy Group. "The networking group is having a larger say in the purchase of security products, and that has translated into more success with its security products."

There may not be better evidence of Cisco's emergence than readers giving its PIX appliance series the gold medal in the network firewall category, a narrow victory over standby Check Point's FireWall-1.

High marks from readers were concentrated on the most important duty firewalls perform: keeping hackers outside corporate networks. Readers noted Cisco PIX's ability to block intrusions, attacks and unauthorized network traffic, in addition to its application-layer/protocol/HTTP controls. Also, Cisco scored well for its service and support; logging, monitoring and reporting; integration with other network defense/management tools; central management; and ROI. Readers weren't as complimentary with the product's ease of installation, configuration and administration.

Cisco's PIX Security Appliances integrate a range of firewall services and feature stateful inspection that tracks network communications and prevents unauthorized network access. The product includes attack protection features such as TCP stream reassembly, traffic normalization, DNSGuard, FloodGuard, FragGuard, MailGuard, IPVerify and TCP intercept. The Cisco line also wards off DoS attacks, fragmented breaches, replay advances and malformed packet forays. The system provides real-time alerts to administrators, so companies can immediately take steps to oust intruders.

Recently security has been moving away from being viewed solely as a network issue and inching higher up the protocol stack; it is often viewed now as an application level problem. Cisco's PIX products deliver application layer security via intelligent, application-aware inspection engines. These gather application and protocol knowledge and use it to make decisions about providing access and information to different users and applications. The device's security enforcement technologies include protocol anomaly detection, application and protocol state tracking, network address translation (NAT) services, and attack detection and mitigation techniques, such as application/protocol command filtering, content verification and URL deobfuscation.

Corporations have a wide variety of devices connected to their networks, and managing them can be problematic. Administrators can integrate Cisco PIX security appliances into switched network environments by taking advantage of native 802.1q-based VLAN support. Cisco IP phones automatically register with Cisco's CallManager software and download needed configuration information and software images.›

SILVER | Check Point FireWall-1

Check Point • www.checkpoint.com • Price: Starts at $3,000

Check Point FireWall-1 is a fixture inside the Fortune 100, and nearly all of the Fortune 500. Readers rated highly its ability to block intrusions, attacks and unauthorized network traffic. They also noted its central management functions in this category.

FireWall-1 provides access control, attack protection, application security, intrusion prevention, content security, authentication, quality of service, and network address translation functions. In addition, Check Point developed the Open Platform for Security (OPSEC) standard so other vendors' products can be integrated into the firewall, and extend its functionality.›

BRONZE | Microsoft ISA Server

Microsoft • www.microsoft.com • Price: $5,999 per processor

Microsoft ISA Server earned the bronze medal with high marks for installation, configuration and monitoring capabilities, as well as for its integration with other security and management applications. ISA Server is now part of Microsoft's Forefront Edge Security and Access Suite, along with the Intelligent Application Gateway introduced in February at the RSA Conference. Microsoft added a bevy of features to ISA Server 2006, including new support for Exchange 2007 for enhanced remote access; a new flood resiliency feature and remediation against flood and other DDoS attacks; and support for LDAP, allowing ISA to authenticate to Active Directory without being part of the domain.›


Lloyd Hession

Missed connections

Users plead with vendors to standardize information exchanges between disparate firewalls.

BT Radianz provides network and system outsourcing services to 200 financial institutions worldwide, meaning it works with a range of firewalls from different vendors at customer locations. This makes chief security officer Lloyd Hession's job difficult.

"Since there are no industry standards, exchanging information from one firewall to the next requires a great deal of work," Hession says.

If a company decides to connect different systems, it can be a daunting task indeed. The problem is that vendors define the way they collect security information and exchange it in their products so differently, integration has to be done on a case-by-case basis. Compounding the problem is the reality that there really are no simple export/import utilities available. In addition, vendors have not spent much time or put significant effort into developing tools to help users with the task.

The result is six months or more of work connecting two vendors' firewalls. Most companies do not have ample resources to do so.

The lack of standards is one reason why users tend to stay with the same firewall supplier. "Once a company puts a firewall in, they find it difficult to move away from it," says Eric Maiwald, senior analyst at the market research firm Burton Group. Unfortunately, problems arise even when users stick with one vendor. With the amount of reshuffling that has been taking place in the security industry, companies sometimes find themselves with incompatible products from the same supplier.

Another trend throwing light on the standards limitation is many enterprises are taking a more comprehensive look at their security needs. They are not focused solely on the functions provided by firewalls, which were designed to protect the perimeter of a company's network. "Studies have shown that internal security breaches are just as important—and often more destructive—as those occurring around the perimeter," says Spartaco Cicerchia, manager of network infrastructure at Janelia Farm Research Campus, a subsidiary of the Howard Hughes Medical Institute and a nonprofit medical research organization.

Consequently, firewalls have been evolving to support additional security functions, such as intrusion detection systems, spam filtering, and even virus protection. Eventually, all these functions could wind up in unified threat management (UTM) systems, which consolidate security functions into a single platform.

Despite the need for firewall data-collection and data-exchange standards, little progress has been made.

"Vendors are more interested in proprietary products and locking users into their systems than easing information exchange," says BT Radianz's Hession. Until such thinking stops, companies will continue to have trouble exchanging information among different firewalls.

Paul Korzeniowski is a freelance writer based in Sudbury, Mass. Send comments on this article to feedback@infosecuritymag.com.

MARKET OVERVIEW

GUIDANCE

Though mature, the firewall market is undergoing dramatic changes. Users have more deployment options, but have to put in more time to ensure they make the right deployment decisions.

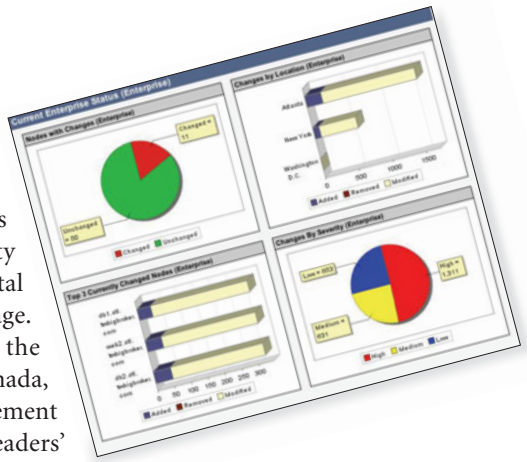
MATURE FIREWALLS REMAIN RELEVANT

Companies need to make sure they prevent outsiders from accessing corporate data. Firewalls are designed to turn back intruders before they tinker with enterprise data.

Size	The multibillion-dollar network firewall market has become difficult to track because firewall functionality is being integrated into a variety of devices—routers and switches, UTMs, and other discrete security products such as IDSes and spam filters.
Maturity	Established; these products have been in use for a decade and deployed in just about all corporations.
Leaders	Cisco, Check Point, Juniper
Contenders	Microsoft, Secure Computing, Fortinet, SonicWALL, WatchGuard
Innovation	Firewall design is changing from a centralized to a distributed system; improved performance and more granularity could result.
Disruptions	Integration and multiplicity are market watchwords. Vendors are trying to integrate firewall functionality into network devices. The standalone firewall market is under siege.

GOLD | Tripwire Enterprise

Tripwire • www.tripwire.com • Price: Not provided by Tripwire



Information security professionals have to deal with more than traditional Internet threats. More than ever, they're evaluating and managing risk from a business perspective, which means vulnerability management tools touted for risk management use just won't cut it. Security managers need tools that can keep tabs on incremental changes to the network that could cause irreparable damage.

That's part of what David Lewis, head of security at the Independent Electricity System Operator (IESO) in Ontario, Canada, was looking for in a tool to help with risk and policy management processes. His organization chose Tripwire Enterprise, the Readers' Choice gold medal winner for risk and policy management.

A longtime Tripwire customer, Lewis has used Enterprise at IESO for approximately seven months. He says it's easy to use, and enjoys that it's Web-enabled and provides tiered-access control.

While many enterprises mitigate risks once they are discovered, with Tripwire, security staff can act proactively and assess and correct problems. Tripwire monitors files, directories, registry settings, directory server objects and configuration files on file and directory servers and network devices, in real time.

Security managers will also appreciate Tripwire's "reconciliation techniques" that map to any organization's change policies. These techniques use multiple acceptance criteria, change categories and conditional change actions, making it easier for policymakers to ensure that an authorized person implemented a change and that the change occurred within a defined time period.

Its online dashboards and reports can also be customized for any environment to show status and history across an enterprise.

Lewis says one major draw of Enterprise is its ability to take the guesswork out of monitoring the system, a feature that will appeal to multitasking managers charged with investigating and mitigating enterprise risks. Readers gave Tripwire Enterprise high marks for its granular and flexible policy management definition capabilities, and for its ability to identify policy violations and understand security risks.

SILVER | Symantec Control Compliance Suite

Symantec • www.symantec.com • Price: $1,000 per server

Readers gave high scores to Symantec's Control Compliance Suite's granular and flexible policy management definition capabilities, for its ability to identify policy violations and for its integration capabilities with applications and devices.

The suite automates compliance measurement and displays pass/fail scores against regulations and frameworks, giving management an accurate reflection of how systems hold up to regulatory mandates. The product also offers guidance for addressing noncompliant servers and workstations when violations are detected. The suite is available on multiple platforms, enabling managers in heterogeneous environments to visually assess and mitigate complex compliance issues.

BRONZE | Altiris SecurityExpressions

Altiris • www.altiris.com • Price: $895 per server node

Altiris SecurityExpressions provides enterprises with a scalable agentless or agent-based configuration management solution that readers say is easy to use and offers strong trend reporting. It allows organizations to audit desktops, laptops and servers for compliance with security configuration policies. Systems can be audited on connection, as well as on schedules.

Readers touted its ability to identify policy violations, granular and flexible policy definition capabilities and solid return on investment. The product includes customizable policy files from organizations like NIST, CIS and SANS, and policy files for industry regulations such as SOX, FISMA and HIPAA. Altiris was recently acquired by Symantec.

Assessments, people problematic in managing risk

Security managers must stave off risk with comprehensive assessments.

"With big risks come big rewards" doesn't hold true for security managers, for whom big risks are a recipe for big failures. And, while risk factors differ between markets, the challenges and best practices for maintaining a risk management strategy are surprisingly similar.

"Risk management is an essential component to the information security officer; you can't secure things you don't know about," says Stan Gatewood, CISO at the University of Georgia.

Security managers say documenting risks is one of their greatest challenges.

"Risks aren't solely confined to technical operations; there are often compliance and other esoteric risks to consider," explains Ernie Hayden, CISO for the Port of Seattle.

Budget constraints are also commonly cited as pain points, especially for government-funded institutions, whose employees are often asked to do more with less.

People can be problematic, too. "Complacency is often a factor. Many believe in a 'if it ain't broke don't fix it' attitude, making it hard to move from a reactive to a proactive mindset," Gatewood says.

So what can be done to reduce the risk of data loss? For those who have the budget, use products that not only help manage risk but offer a good ROI.

Nick Garbidakis, CIO/CTO for the American Bible Society, uses Ecora Enterprise Auditor.

"Without this kind of system, someone has to go through every server and update manually. The system makes sure everything is updated and gives us reports. Before, we were reactive to issues. The reports show us who was in systems, what happened overnight. It enables us to be more proactive," he says.

Those who don't have the budget can start investigating policies and standards, like NIST 800-30, COSO and ISO 27001, to provide guidance for risk assessments.

Once a risk assessment has been conducted, CISOs should be able to classify risk types and define acceptable risk levels. The next step is education at every tier.

"I conduct seasonal brown-bag seminars that employees can voluntarily attend," says Hayden.

For upper management, provide quantifiable data and position yourself as an expert in the field, recommends Gatewood. "This means doing your homework, putting on the glasses, reading about risk management and how it applies to your sector."

Equally important, Hayden says, is to respect and trust senior management, regardless of what they do with the information gathered; they may know something you don't that may contribute to business failure.

Finally, keep abreast of security issues.

"Bad guys are getting sophisticated, and technical controls aren't as strong as they used to be. Therefore, we need to think through all risk factors," says Hayden.

Kristin Cipolletti is assistant editor of SearchSecurity.com. Send comments on this article to feedback@infosecuritymag.com.

MARKET OVERVIEW

GUIDANCE

Look for a standardized representation of policies, rules and guidelines that will fuel automated policy management.

WARDING OFF RISKY BUSINESS

Tools that automate the risk and policy management process, and help your organization assess threats as they apply to your market and compliance needs.

Size	Risk assessment: $70 million; Policy management: $200 million; Compliance management: $120 million (Forrester Research)
Maturity	Risk assessment: Adolescent; Policy management: Maturing; Compliance management: Maturing (Forrester Research)
Leaders	Risk assessment: Skybox; Policy management: Archer Technologies; Compliance management: IBM Tivoli Security Compliance Manager (Forrester Research)
Contenders	Risk assessment: Deloitte, VeriSign; Technical Policy management: ArcSight (SEM); CA eTrust (IAM); Compliance management: NetIQ (Forrester Research)
Innovation	Paramount are products that automate policy management, and map controls and compliance against operations.
Disruptions	Market acceptance is an issue.

GOLD | Cisco VPN 3000 Series Concentrator

Cisco Systems • www.cisco.com • Price: $2,995-$45,000

Cisco's VPN 3000 Series Concentrator continues to lead the secure remote access market, not only in the number of products shipped but also in customer satisfaction. "Cisco has become like IBM used to be in the computer industry—its products are viewed as the best choice because users know the company's future is rock solid," says Zeus Kerravala, vice president for enterprise computing and networking at the Yankee Group.

Cisco scored well with readers in four areas—authentication support; end user transparency and ease of use; investment ROI; and extensibility.

Authentication support has become an important issue in securing transactions, and warding off identity spoofing. "Cisco has been one of the companies leading movement to NAC (Network Access Control), which promises to make it easier for enterprises to authenticate remote users," says Pete Lindstrom, a senior analyst, Burton Group. NAC authenticates and checks on the health of systems as they attempt to connect to a corporate network.

One challenge for security administrators is deploying products that keep a company's data safe without hindering users' ability to function. The Cisco VPN 3000 Series Concentrator works with a variety of applications through its SSL VPN client.

In addition, the company has done a good job in making its system easy to deploy. Its integrated, Web-based management system provides an interface for configuring and monitoring remote users. For remote access and site-to-site VPNs, ease of deployment is critical because technical personnel are often not available to configure the secure connections at remote sites. Cisco's Easy VPN solution pushes security policies to remote VPN devices, helping ensure that up-to-date policies are in place before a connection is established.

Readers gave Cisco high marks for ROI. Since it is the leading networking company, Cisco can spread its operating costs over a large customer base and lower product pricing. The Concentrator platform does not add licensing costs for special features, such as a multidevice clustering that allows the remote access solution to scale as a business grows. Since both SSL and IPsec VPNs are available on one platform, customers can deploy parallel remote access infrastructures.

As the leading networking supplier, Cisco has garnered a stellar reputation for delivering products that meet customer needs. That success has migrated from its network equipment to its remote access security products. ›

SILVER | Citrix Access Gateway

Citrix • www.citrix.com • Price: $3,500-$50,000

Citrix Access Gateway simplifies and secures remote access to applications. The Access Gateway delivers the same desktop access experience users have within the network, removing the need for additional training. In addition, it automatically reconnects users to their applications and documents when they change locations or devices. Citrix also has an extensible product line—the Access Gateway provides secure access to Windows and UNIX applications, Web applications, Citrix Presentation Server-hosted applications, network file shares and telephony services using VoIP softphones. No application customization is required to use these features. ›

BRONZE | Check Point VPN-1

Check Point Software Technologies • www.checkpoint.com
Price: $3,000

Readers noted Check Point VPN-1's extensibility. VPN-1 works on Windows, Windows Mobile and Macintosh platforms. In addition, the client software supports dynamic and fixed IP addressing for dial-up, cable modem or DSL connections. This flexibility enables telecommuters and mobile workers to access their company networks via an Internet Service Provider, wireless hotspot or hotel Internet access connection. Authentication support was a second strong point.

VPN-1 also supports SmartDefense Services, which provides real-time updates and security configuration advisories. ›

IPsec-SSL debate still going strong

SSL VPNs continue to gain on the venerable IPsec connections.

Kevin Rice, global network architect at AT Kearney, a management consulting firm, understands the challenges of providing secure remote access. The bulk of the company's 3,500 employees spend their day working at customer sites and helping them address various technology challenges. "Almost all of our employees have laptops and access our corporate data daily from a variety of locations," he says.

To make sure the information is safe, Rice relies on two vendors' VPN products—Cisco's VPN 3000 Series Concentrator for IPsec connections and Check Point's VPN-1 for SSL VPN over the Web. "IPsec is still our most common connection, but a growing number of users work with SSL," Rice says.

Simpler administration is an appeal with these VPNs. "We have a small staff and are not able to spend a lot of time configuring and maintaining our security software," Rice says. Because they operate at the application level, SSL VPNs do not require as much customization and configuration on user machines and servers as IPsec solutions.

Flexibility is another SSL VPN strong point. Siemens Energy and Automation, which has 10,000 employees, delivers electrical, engineering and automation solutions to industrial, manufacturing and construction companies.

Three of every five employees need to access company data remotely. To support them, Siemens installed F5's FirePass Secure Remote Access SSL VPN because it lets the organization expose specific files or documents to users without granting them access to other corporate data.

"The granularity found with SSL VPNs appealed to us," says CISO Kathy Taylor.

Another initiative to simplify security tasks is getting mixed reviews. Network equipment vendors think that integrating VPNs into routers and switches would ease administration.

"Cisco has been talking about VPN router modules, and that feature appeals to me because it would lower the number of autonomous items that I would have to maintain," says AT Kearney's Rice.

Spartaco Cicerchia, manager of network infrastructure at Janelia Farm Research Campus, disagrees.

"Consolidating one set of security functions into a device designed with another purpose creates more problems than it solves," he says.

Janelia is a subsidiary of the Howard Hughes Medical Institute, and the campus enables 250 of the world's top medical researchers. Cicerchia needed to find a way to provide the researchers, who often work remotely, with secure access to the data center. He selected Juniper Networks' Secure Access VPN.

While users face numerous challenges in managing their VPNs, they believe progress is being made.

"The installation and maintenance of VPNs is simpler now than it was a few years ago," says Rice. "The products feature more automation, and the interfaces are more intuitive now than they were then."

Paul Korzeniowski is a freelance writer based in Sudbury, Mass. Send comments on this article to feedback@infosecuritymag.com.

MARKET OVERVIEW

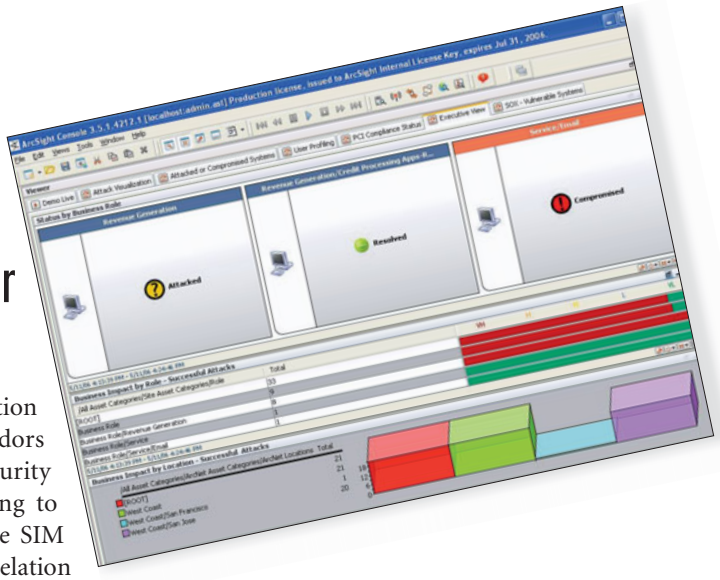
GUIDANCE

Users should not be too concerned about how vendors change product packaging, but instead focus on how the different options can be integrated into their security infrastructures.

READY FOR A CHANGE?

Companies need to provide employees, partners and customers with access to corporate data. VPNs ensure a secure connection between an end user node and a corporate computer.

Size	Because of different packaging options, market estimates range between $1 billion and $2 billion, with a 60/40 split between IPsec and SSL VPNs.
Maturity	Established; these products have been in use for a decade.
Leaders	Cisco, Check Point, Nortel Networks, Juniper
Contenders	Aventail, Caymas Systems, Citrix, F5, Microsoft
Innovation	Changes in authentication techniques, such as network access control (NAC), are creating confusion as security functions found in different products begin to overlap.
Disruptions	This market segment may be incorporated as a module in router and switch blades or more comprehensive security suites.



GOLD | ArcSight Enterprise Security Manager

ArcSight • www.arcsight.com • Price: $50,000

Organizations looking for a security information management (SIM) solution have a lot of vendors to choose from, but ArcSight Enterprise Security Manager stood out from the crowd, according to readers. The product won a gold medal in the SIM category, scoring high marks for its event correlation capabilities, effective management interface and compatibility with existing systems.

ArcSight ESM also scored well in its ability to map information to security policy or compliance regulations, and its granular and flexible policy definitions.

The biggest benefit of ArcSight ESM is its dashboard graphics for analysis of security events, says Tim Maletic, manager of information security at Priority Health, a Michigan-based health insurance company.

The product allows him to easily view events, drill down through various displays and pull data to research events.

In addition to using ArcSight ESM for incident detection and response, Priority Health uses the product to help with various compliance efforts. "It does a good job of recording what you do with the tool," Maletic says.

"I can use that data to back up my incident response policy and other policies we get audited on, and prove we're doing what we say we're doing," he adds.

Maletic says the list of devices ArcSight ESM supports is impressive. Priority Health uses the product to integrate data from IDSes, firewalls, Windows, UNIX and Linux servers, antivirus, and vulnerability assessment systems. The company also is writing customized agents for homegrown applications.

The fine-grained policies ArcSight ESM provides for user management can be a little daunting to set up, but provide valuable flexibility, he says.

Last year, ArcSight bolstered ESM with the release of its Compliance Insight Packages. The packages bundle rules and reports based on ISO 17799 and NIST 800-53 standards to help organizations meet regulatory requirements such as SOX, HIPAA, and the Payment Card Industry (PCI) Data Security Standard.

Also in 2006, ArcSight expanded beyond its core capabilities in security management with its acquisition of ENIRA Technologies, a supplier of technology for automating network management tasks. After the acquisition, ArcSight released Network Response Manager, which automates network responses in order to block worm outbreaks, hacker attacks or other security events, and Network Configuration Manager for automated network discovery and configuration management.

SILVER | NetIQ Security Manager

NetIQ • www.netiq.com • Price: Console, $2,500

Readers noted NetIQ Security Manager's management interface and compatibility with existing systems, earning it a silver medal.

The product helps organizations cope with compliance and the deluge of security events by consolidating and archiving log and event data. It provides a single system for event correlation, analysis, real-time intrusion protection, and reporting. NetIQ, acquired by Attachmate last year, released last fall NetIQ SM 5.6. It includes an enhanced UI with customized views of data from multiple sources, improved access control to support multiple roles during incident response, and reporting flexibility to allow for creation and viewing of reports based on audience and priority.

BRONZE | Check Point Eventia Suite

Check Point Software Technologies • www.checkpoint.com
Price: $25,000

Check Point Software Technologies' Eventia Suite won the bronze medal, scoring high marks from readers for its ability to map information to security policy or compliance regulations, and its event correlation capabilities.

Eventia also scored well in ROI—readers said they get their money's worth with the product. The Eventia Suite consists of the Eventia Analyzer for real-time security event correlation and Eventia Reporter for historical trend analysis. The suite helps organizations filter security events to zero-in on the ones that matter, respond in real time to incidents, and ease compliance efforts with centralized analysis and reporting.


Jim Granger

Tradeoffs to consider with SIMs

SIMs require plenty of up-front work understanding business processes and tuning agents, but the payoff is better security.

Security information management (SIM) systems can be a big help to an organization, but they have their downsides.

While SIMs can help meet audit requirements and improve incident response, they can be complex to deploy and difficult to manage. There may be agents that need tuning, false positives to sort out, and reports to run—all of which require resources. Some organizations have one or more engineers devoted full time to a SIM.

Jim Granger, technical director at the Navy Cyber Defense Operations Command, says SIMs are like any other technology in that they require an up-front investment of time and resources. And not just anyone can implement them; skilled technicians are needed.

"SIMs force you to understand what your business processes are and what your networks look like, but that in and of itself is a good thing," he says.

When first installed, SIMs can generate a lot of security events that don't need attention, but tuning the system for a specific environment helps resolve that problem, says Dave Daniels, network security engineer at PPD, a global contract research firm serving pharmaceutical and other organizations. The company installed a SIM from Q1 Labs that combines SIM with anomaly-based detection technology.

"The more it knows about your network the better," he says.

The payoff is streamlined security monitoring that makes it easier to track and analyze virus outbreaks, according to Daniels.

Security managers advise others to take the time to understand their needs before leaping into a SIM purchase.

"They really have to understand what their requirements are and map it to the products that they're after," says Dave Lewis, head of security at the Independent Electricity System Operator in Ontario, Canada.

"Don't worry about what vendor you're dealing with. Worry about what you actually need. …If you don't understand what you actually need, you're going to get a mess," Lewis says.

Likewise, Glenn Haar, IT resource manager at the Idaho Tax Commission, advises organizations to figure out what they want to accomplish before looking at specific SIM products. His firm studied its compliance and security needs before choosing High Tower Software's appliance.

"We didn't look at the product first. We talked about what our business goals were first," he says. "If you get your education from vendors, typically they educate you the way they want you to understand the world. Next thing you know, their product is the perfect fit."

Marcia Savage is features editor of Information Security *magazine. Send comments on this article to feedback@infosecuritymag.com.*

MARKET OVERVIEW

GUIDANCE

Must-have tool for organizations needing help with compliance demands and security management; stay-away for organizations without the resources to manage the technology.

RESOURCE DRAIN OR GAIN?

SIMs automate monitoring of firewall, IDS and other logs. SIMs aggregate, correlate and store data, providing visibility into network security, improving incident response and satisfying auditors.

Size	$284 million in revenue in 2005; projected to grow to $873 million in 2010 (IDC).
Maturity	Adolescent
Leaders	ArcSight, netForensics, Network Intelligence
Contenders	Cisco Systems, Symantec, Quest Software, Consul Risk Management (acquired by IBM)
Innovation	Technology focusing more on monitoring user access and provisioning activities for compliance purposes.
Disruptions	Can be complex to implement and manage. Market rapidly consolidating.

GOLD | Check Point VPN-1 UTM

Check Point Software Technologies • www.checkpoint.com • Price: Starts at $7,500

Readers gave Check Point's VPN-1 UTM, formerly known as Express CL, high marks for the depth of security it provides and its form factor. But there's plenty to be said for the company's stability as a security vendor.

VPN-1 UTM offers firewall, intrusion prevention, antivirus, antispyware, Web application firewall, and both IPsec and SSL VPN, within a single integrated platform. All these functions can be centrally controlled and updated in real time.

Geiger Brothers, the largest privately held promotional products company in the country, has used Check Point for more than eight years. "We have looked at other products and there are some cheaper solutions," says Rob Herman, IT operations manager with Geiger Brothers. "But Check Point is centrally managed so it cuts down on administration and overhead."

Geiger Brothers uses Check Point primarily to secure its 20 field offices across the country with its headquarters in Lewiston, Maine. "We really like Check Point because it's very secure and seamless to manage," says Herman. "It's also very stable. I've been here for five-and-a-half years and we've had very few problems with downtime."

Herman also notes that Check Point, while relatively small, sells to enterprise-sized companies. "They've got some big clients so obviously they're doing something right," he says.

Check Point's ease of use may have something to do with its target market of midsized offices and branches. "They have to conform to internal auditing requirements and they need options in terms of monitoring and reporting to management," says Dave Burton, director of product marketing with Check Point. "They want something that's easy to install and get up and going, and Check Point offers all of that."

Check Point also has a VPN-1 UTM Edge product specifically for companies with branch offices. "We've seen a trend toward appliances increasing in branch-sized offices," says Burton. "These branch offices don't have a security expert on-site and they want multiple security applications in one device. UTM Edge does just that."

Many UTM providers don't offer SSL and IPsec VPN as part of their solution; Check Point does. Although they come installed, users must purchase separate licenses to use them. ›

SILVER | Cisco ASA 5500 Series Adaptive Security Appliance

Cisco Systems • www.cisco.com • Price: $19,995

Readers were sold on Cisco's ASA 5500 UTM product, especially for its breadth of functions, such as firewall, IPS, VPN and antimalware. Service and support also rated well. "We like it because of its ability to recognize unusual behaviors," says Carl Goodman, IS manager with Premier Valley Bank in Fresno, Calif. "Other vendors just work with signature files. I liked that proactive approach." Goodman has used ASA 5500 for six months to secure his employer's internal network, and was high on Cisco support. "Cisco was the leader in new technologies, and because they're a large company they have a lot of staff if I have a question," he says. ›

BRONZE | SonicWALL PRO

SonicWALL • www.sonicwall.com • Price: $15,490

SonicWALL PRO's ability to provide deep-packet inspection of network traffic earned high marks from readers. They also noted its form factor and ROI, while indicating SonicWALL still has some work to do with installation, configuration and management of the platform. SonicWALL Pro includes enterprise-class networking, routing, firewall, secure wireless and IPsec VPN in one appliance. Melissa Young, information technologies manager with the Portland State University Bookstore, says SonicWALL PRO protected her employer's network from a virus that struck the Oregon university's network. "What I find useful about SonicWALL PRO is that it can take care of itself," says Young. "When I started here six years ago I had never set up a firewall before. For a novice to get it up and running for six years without any problems is great." ›

Clear network picture spares UTM headaches

Buyers beware: Defining your security requirements saves you time and money with your UTM vendor.

If your organization is shopping for a unified threat management appliance, users stress the importance of diagramming your network before sitting down with a vendor.

"We talked with our provider about what our network would look like and the implementation between [Juniper Networks'] SSG in our Internet space and the SSG in our local corporate network space; that was fully documented and agreed upon," says Matt Lauth of Six Disciplines, a corporate coaching service based in Findlay, Ohio. "Once that was agreed on we just followed the recipe. It made the implementation work very smoothly."

Lauth says if you don't define your security requirements with your solutions provider you end up spending too little in critical but overlooked areas, and spending too much on features that aren't necessary for your operation. "By documenting our network we were able to perform a balancing act," he says.

Midmarket and smaller firms with 100 users or fewer are wise to hire a solutions provider for a UTM installation, says Melissa Young, information technologies manager with the Portland (Ore.) State University Bookstore. "The first time I installed SonicWALL's UTM device, I wish I had hired a consultant," she says. "It was easy to operate but I wish I was more knowledgeable about it and a consultant could have helped me there."

> "The first time I installed SonicWALL's UTM device, I wish I had hired a consultant. It was easy to operate but I wish I was more knowledgeable about it and a consultant could have helped me there."
>
> –MELISSA YOUNG, information technologies manager, Portland (Ore.) State University Bookstore

Shopping for UTM devices isn't easy, even with a solutions provider, says Adam Hansen, manager of IT security with the Chicago-based law firm Sonnenschein Nath & Rosenthal.

"They'll do everything possible to try to confuse what you're getting," says Hansen, who eventually chose ISS's Proventia MFS UTM appliance. "One vendor was calling something antivirus when it really wasn't. Then, when you [talk with] references, you find they had to change things and upgrade things after they bought the product."

Hansen chose ISS in part because it agreed to his demand to put in writing all the products it was proposing for his needs, the function and performance of each product, and price quotes.

Once Hansen understood each ISS product, his decision was easy—and the product has worked great, he says. "With UTM you get a lot of vendors with good products but they don't have a good fit for your company," he says.

Ira Apfel is a freelance writer based in Washington, D.C. Send comments on this article to feedback@infosecuritymag.com.

MARKET OVERVIEW

GUIDANCE

Understand your present and future security needs so you don't buy unnecessary applications.

ONE-STOP SHOPPING

UTM integrates firewall, antivirus, content and spam filtering, and more in one platform, simplifying use and management.

Size	$660 million as of 2005 (IDC)
Maturity	Adolescent; consolidation and growth continue
Leaders	Juniper, Cisco, IBM, Fortinet
Contenders	SonicWALL, Cyberoam, Check Point
Innovation	VoIP, content scanning and integration with physical security
Disruptions	Maintaining processing performance is key.

GOLD | QualysGuard Enterprise

Qualys • www.qualys.com • Price: $2,995 for an annual subscription

Readers applauded vulnerability management gold medal winner QualysGuard Enterprise's ability to identify vulnerabilities quickly and accurately.

QualysGuard—which identifies potential network exploits and audits networks for compliance—also received high marks for being easy to install, configure and administer. Respondents praised QualysGuard Enterprise for the breadth of applications and devices with which it works; vendor service and support; and ROI, which most respondents rated "excellent" or "good."

Readers weren't as effusive about QualysGuard's ability to integrate with threat management systems, with many rating that feature "good" or "fair."

QualysGuard Enterprise 5.0, which was announced in February at RSA Conference 2007 and went into general release last month, boasts a revamped GUI; accelerated scanning through parallelization of scanner appliances; enhanced reporting features; and the ability to track scanning usage by business unit, according to company officials.

The new release "enables us to do things better and faster by utilizing an AJAX framework," says Amer Deeba, chief marketing officer at Qualys. He says the AJAX (Asynchronous JavaScript and XML) technology enables Web pages to be more responsive by exchanging small amounts of data with back-end servers, so that an entire Web page does not have to be reloaded each time a user makes a change. The technology is said to increase the speed with which the page renders, as well as its interactivity and usability.

CISOs inundated with information about the array of threats and potential threats want a product that can pare down the onslaught, Deeba says. "The new release filters out that overload of data and narrows it down to what is most important based on your role within the organization," he says. Rather than Qualys indicating "12 million problems, you only see what is relevant to you, based on your privileges."

While noting that Qualys management has been "thinking a lot" about the juncture between scanning for weaknesses and remediating them, Deeba says the company prefers "to remain a third-party auditor, where we can come in and audit you and give you full configuration and vulnerability information."

Qualys' other offerings include a product designed to measure PCI compliance, one aimed at security consultants, and several others. ›

SILVER | IBM Internet Scanner

IBM Internet Security Systems • www.iss.net • Price: $7,250 for the appliance

IBM Internet Scanner earned the silver medal on equal merit for its ability to find vulnerabilities, ease of use and reporting capabilities. Internet Scanner, which IBM acquired with its purchase of Internet Security Systems last year, offers unlimited asset identification to help CISOs keep an accurate inventory of their networks' electronic assets; an intelligent scanning feature that identifies the operating systems of target hosts and runs appropriate OS-specific checks against them; and a Common Policy Editor with 20 predefined policies that provides greater control over corporate scanning. ›

BRONZE | GFI LANguard NSS

GFI • www.gfi.com • Price: $495 (up to 32 IP addresses)

GFI LANguard Network Security Scanner (NSS), which identifies vulnerabilities and can also deploy necessary patches, won the gold medal in vulnerability management. The product scans a network IP by IP to provide information on missing security patches, open ports, service pack level of a machine, USB devices, and more. Companies can set GFI LANguard NSS to perform scheduled, customized scans and the product compares the results with previous scans and issues email alerts of new security holes. After a scan, it provides recommendations on remediation. Users can use the tool to deploy service packs and patches in operating systems and applications, as well as to install custom software. ›

VM a sound policy foundation

Vulnerability management tools help your organization build and enforce security policy.

A vulnerability management (VM) strategy offers not only the means to generate a security policy for your enterprise, but the technology to enforce it.

The myriad offerings under the VM umbrella—from scanners and patch-management tools to penetration-testing services and asset-management software—"provide the tools to build and maintain a security program or policy," says Dave Bixler, CISO for Siemens Business Services. In turn, the policy guides how and when such products are used.

Although products that occupy the VM space are becoming increasingly feature-rich, one tidy product addressing all of an organization's VM needs does not exist, in part because security managers don't want to cede control of fixes to automation.

"CISOs have been burned in the past when they put in [an automated solution] that blocked legitimate network traffic," says Khalid Kark, a senior analyst with Forrester Research.

Bixler, who launched an overhaul of his organization's security policy several years ago, says that at the time he not only wanted to keep his hand on remediation, but he wanted easy-to-use reporting to help him plan fixes. "It didn't matter what the tool was, as long as we could understand the reports," he says, noting that Siemens then deployed Internet Security Systems' scanner (now known as IBM Internet Scanner).

While Bixler characterizes the former ISS product as a "fantastic tool for addressing OS-related issues," the organization ultimately moved to products from Qualys, with PatchLink for some remediation. "It was starting to be obvious that the places attackers were attacking weren't necessarily the operating systems," he says. "They were going after Oracle, SQL—all our applications." Furthermore, Qualys' hierarchical permissions model let Bixler delegate responsibility for aspects of VM to different members of his team.

Joe Adams, IT director at Nuclear Fuels Corp., also is a fan of building a VM strategy around a well-delineated policy. NFC's policy dictates how StillSecure's VAM, integrated with Shavlik for patch management, is used.

Judicious application of technology is paramount, Adams says: "We don't treat all of our devices the same. We've got one process for our servers, another for our network backbone technology, and so on." Scans are conducted according to guidelines that determine when they occur, what vulnerabilities are being sought and how remediation should be handled.

These days, given the plethora of products in the VM space, security managers with one eye on the budget must guard against feature redundancy.

"I'm not interested in spending money on a remediation tool when I can remediate some things with my asset-management tool," says Bixler. Expect more products with more bang for the buck as the VM space progresses.

Amy Rogers Nazarov is a freelance writer based in Washington, D.C. Send comments on this article to feedback@infosecuritymag.com.

MARKET OVERVIEW

GUIDANCE

At least some VM wares are must-have. Organizations can't devise a thorough security policy without a hard look at weaknesses in applications, operating systems and devices.

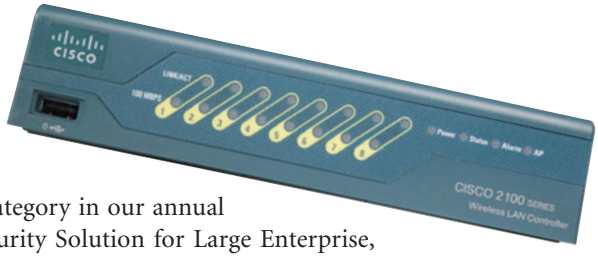
PLENTY TO CHOOSE FROM

Vulnerability management products encompass everything from patch management to configuration management to vulnerability assessment.

Size	Network vulnerability assessment: $225.5 million; host vulnerability assessment: $233.7 million; application vulnerability assessment: $143 million (IDC)
Maturity	Adolescent
Leaders	PatchLink, Shavlik Technologies, Microsoft, IBM Internet Security Systems, Qualys, McAfee, Symantec, NetIQ (Attachmate)
Contenders	St. Bernard, Hewlett-Packard, nCircle, eEye Digital Security, CA, IBM Internet Security Systems
Innovation	Vendors folding in more capabilities such as remediation
Disruptions	Be wary of automated solutions that may remediate common vulnerabilities but interfere with other network functions.

GOLD | Cisco Wireless LAN Security Solution for Large Enterprise

Cisco Systems • www.cisco.com • Price: Starts at $10,000



Cisco Systems is known as a networking giant because of its dominance in the enterprise networking equipment market. However, it may soon be known as the wireless security giant as well.

That's because it dominated the wireless security category in our annual reader survey, courtesy of its Cisco Wireless LAN Security Solution for Large Enterprise, formerly known as Wireless Security Suite. The name refers to a comprehensive set of wireless network security features in its wireless access points, switches, routers, appliances and client devices, which Cisco has combined in order to convince many of its longtime wired customers to relinquish their wireless security fears and implement over-the-air network infrastructures.

"The solution takes an integrated approach to delivering unified wired and wireless IPS/IDS, wireless device posture assessment and remediation, wireless host intrusion prevention and policy, and a comprehensive management framework for analysis and reporting," says Chris Kozup, manager of mobility solutions at Cisco. "The Cisco Wireless Security Solution is comprised of the Cisco Unified Wireless Network, the Cisco NAC Appliance, the Cisco ASA Firewall with IPS, the Cisco Security Agent and an integrated authentication framework using the Cisco Secure ACS RADIUS server and the Cisco Secure Services Client."

At the top of its feature list is support for the 802.11i WiFi security standard, which shored up weaknesses in earlier standards largely through the use of the stringent Advanced Encryption Standard (AES) or Temporal Key Integrity Protocol (TKIP) methods of wireless data encryption. Its 802.11i support also includes reliance on 802.1X-based mutual authentication and dynamic encryption key management, aiming to ease the administrative struggles that often come with static encryption keys.

As is often the case with Cisco gear, perhaps the product's most impressive feature is its integration with other Cisco technologies, such as its wireless mesh networking capabilities for securing access point-centric outdoor networks, integration with Cisco's Self-Defending Network threat mitigation offerings and the Network Admission Control endpoint security technologies.

Readers gave the product high marks for quality and ROI; Cisco support was also lauded.›

SILVER | Check Point VPN-1 Edge Wireless

Check Point • www.checkpoint.com • Price: Starts at $600

Check Point Software Technologies' VPN-1 Edge Wireless appliance is designed to extend wireless threat management capabilities to enterprise branch offices while being easy to manage. Readers gave it the silver medal.

When enabled with wireless security features, as is the case with its NGX model, the product supports a number of security protocols, such as 802.1X, IPsec over WLAN, RADIUS, WPA2/802.11i and WEP authentication, in addition to MAC address filtering. A recently added option can require users to authenticate to a RADIUS server, aiding proper identity and access management. Its integrated unified threat management (UTM), firewall, VPN, IPS and antivirus offer comprehensive protection for 802.11b and 802.11g wireless devices.›

BRONZE | AirDefense Enterprise

AirDefense • www.airdefense.net • Price: Starts at $7,995

Readers noted the AirDefense Enterprise wireless intrusion prevention and monitoring product's ability to detect intruders and mitigate attacks, as well as its access control capabilities, earning the product the bronze medal. The platform consists of distributed smart sensors and server appliances. Using many context-aware detection schemes, correlation and multidimensional detection engines, the product is able to detect attacks and anomalies originating from within or beyond the network with a low rate of false positives. It includes policy enforcement and compliance management features and analysis and reporting, plus it is centrally managed, supporting scalability across a large geographic area or a distributed implementation at numerous locations›

Policy, education combat rogue APs

A comprehensive wireless policy is likely to sway users from installing unauthorized access points, experts say.

Few environments lend themselves to objectionable over-the-air activity like a sprawling college campus. At the University of New Hampshire's campus in Durham, striking a balance between security and usability for faculty and staff who use its WiFi network each day at its peak is a difficult proposition.

Doug Green, network manager at UNH, says even though the network provides a VPN for user authentication and data encryption, it does provide some basic services without the VPN.

"Because we do not have ubiquitous WiFi deployment, users do connect rogue access points, and therefore lower the security standard we have established," Green says. "These users are then exposed to all manner of security problems, including eavesdropping—passwords can be grabbed—man-in-the-middle, hacking, etc."

It's not uncommon for Green and the networking team to discover unauthorized APs. Rather than coming down hard on the offenders, the team emphasizes education and a willingness to meet users' needs.

"We work with clients to understand their needs and develop a reasonable, legitimate service solution," Green says. "Often, users think they are saving money by using rogue equipment. Over time, many have come to understand that the service we provide is much more reliable."

That pragmatic approach, combining firm policy with practical methods for helping WiFi users meet their goals, is one that's achieving results for practitioners. Lisa Phifer, vice president with network security consultancy Core Competence, says the key goal of any network security strategy is typically to safeguard the wired network and its data, and WiFi introduces a number of different ways in which the network can be penetrated.

Phifer says establishing and maintaining a WiFi security policy is essential, but so is meeting the needs of employees so they aren't compelled to search for their own connectivity solutions outside that policy.

"Users will be less likely to rig their own unsafe wireless solutions," Phifer says, "and you can take steps to provide and enforce the use of secure wireless connections for all business activity."

David Fournier, senior information security analyst for a large New England grocery chain, is charged with securing a wireless network utilized by several thousand devices. When those clients range from wireless PCs to handheld scanning devices and transmit everything from mission-critical inventory data to day-to-day Web traffic, keeping business needs aligned with the wireless security policy isn't easy.

"It's a constant battle between availability and security," Fournier says. "It's about providing the availability and convenience of a wireless network, but in a secure manner."

Fournier says that in addition to an authentication system based on Cisco Systems' proprietary LEAP protocol, his company has a policy that relies on virtual LANs and SSIDs to segment guest wireless users.

Eric B. Parizo is site editor of SearchSecurity.com. Send comments on this article to feedback@infosecuritymag.com.

MARKET OVERVIEW

GUIDANCE

If your organization is looking to upgrade its WiFi security, now may be the time. Vendor competition is fierce, and experts say there aren't any major innovations on the horizon.

WIRELESS HAS ARRIVED

WiFi security technology enables workers to connect to the corporate network over the air without the fear of packet sniffing, rogue access points or any of the many WiFi threats.

Size	$50 million to $100 million annually for dedicated enterprise WiFi security products, but could be larger as infrastructure vendors often provide that functionality without breaking out the dollar figures.
Maturity	Established. Several generations of products and improved standards have created many top-notch offerings, but management and network integration means plenty of work ahead.
Leaders	Cisco Systems, Nortel Networks, Trapeze Networks, Aruba Networks
Contenders	AirDefense, Bluesocket, Meru Networks
Innovation	Consolidation and integration
Disruptions	Amid the emergence of WiFi-enabled PCs, handhelds and voice over WiFi, RF management is becoming a more vexing issue.

GOLD | CounterACT

ForeScout Technologies • www.forescout.com • Price: $4,995 to $48,995

In the film *Marathon Man*, Laurence Olivier repeatedly asks Dustin Hoffman, "Is it safe?" to proceed with his plans. Corporations ask the same question every time a user—especially a mobile user—logs in to the corporate network.

In the often confusing and still immature network access control market, ForeScout Technologies' CounterACT hits the sweet spot, providing flexible, policy-based security with minimal impact on infrastructure and users.

This is no mean feat, as corporations try to make sense of competing solutions—Cisco's NAC, Microsoft's NAP, Trusted Computing Group's standards-based Trusted Network Connect and a fistful of third-party products.

CounterACT is innovative technology that solves an important problem, from a company that earned credibility with its flagship product, ActiveScout, which brought a fresh and effective approach to network intrusion prevention.

That pedigree shows through in CounterACT, which provides a measure of intrusion prevention to its network access protection, using signature-less interrogation to detect and isolate self-propagating malware and worms, preventing mobile and remote devices and unmanaged computers from infecting the corporate network.

Managing the unmanaged is a key CounterACT advantage. Its agentless technology scans any device for appropriate access policy compliance, with responses ranging from keeping the device off the network to limited access and/or remediation. CounterACT boasts fine-grained inspection, matching agent-based technology—desktop firewall, antivirus definitions, patch levels and specific files and registry entries.

CounterACT is a nondisruptive technology. It works out-of-band, typically spanning off a distribution-layer switch or VPN concentrator, requiring no network infrastructure changes. Its FastPass feature allows users with uninfected devices to continue to log in and go to work even as scanning for policy compliance continues. Its Virtual Firewall can block a specific port or service and block user access to unauthorized or threatened resources, depending on scan results.

It performs vulnerability assessments on all connected network devices (and works with third-party VA scanners), building a complete network inventory and generating event reports. It's highly scalable, with one central manager controlling up to 50 CounterACT devices.

Information Security's product review from August 2006 says, "CounterACT provides a lot of bang for the buck. It's flexible and easy to use, providing intrusion detection/prevention and network access controls."

ForeScout's road map is focused on user- as well as device-based control. In addition to its tight integration with Active Directory, it announced integration with Sun Microsystems' identity management solutions at the recent RSA Conference and plans additional announcements with leading IDM vendors. ›

SILVER | Mu-4000 Security Analyzer

Mu Security • www.musecurity.com
Price: $35,000 to $300,000

The Mu-4000 Security Analyzer conducts torture tests on your network and security tools that will expose even zero-day vulnerabilities. The Mu-4000 bombards products with malicious traffic, laying bare flaws before attackers discover and exploit them. Organizations can use Mu-4000 to test existing tools or reveal weaknesses in products they're considering buying and deploying. Ed Skoudis, writing in *Information Security* ("Don't Just Kick the Tires," December 2006), said the Mu-4000 was the most comprehensive of the tools analyzed, adding it's an optimal choice for its protocol fuzzing, target monitoring and user interface. ›

BRONZE | SecurEdge

KoolSpan • www.koolspan.com • Price: $9,000 for 100 users

"Kool" isn't just cute marketing. *Information Security*'s product review (April 2006) says it all: "KoolSpan's SecurEdge is a remarkably versatile and innovative product for securing connectivity. Using this single security platform, you can secure remote user access, VoIP and WiFi, transparently bridge branch offices to your headquarters, and encrypt connections across some or all of your network." SecurEdge is versatile because it encrypts all traffic with 256-bit AES at layer 2, with a KoolSpan Lock on the network side and KoolSpan Key USB token for the end user. In addition, you secure site-to-site traffic by deploying locks at each location, for example, to provide transparent central network access to branch office users. ›

Selecting the 2007 Readers' Choice Awards

1,595 surveyed; 341 products; 15 winners

Information Security and SearchSecurity.com presented 1,595 readers with a survey of 341 security products, divided into 15 categories. The categories and product lists were determined by *Information Security* and SearchSecurity.com editors, in consultation with recognized information security experts.

Respondents were asked to rate each product based on criteria specific to each category. For each criteria, respondents scored the product on a scale of one (poor) to five (excellent). In addition, each criteria was given a weighted percentage to reflect its importance in that category. Some criteria were applied in multiple product categories, and one, "Investment ROI—are you getting your money's worth?" was asked in each of the 15 product categories.

Respondents also had the ability to opt out of scoring in one or more criteria by indicating that they had "no opinion."

Winners were based on the cumulative weighted responses for each product category criteria. Editors arrived at a product's overall score by calculating the average score it received for each criteria, applying the weighted percentage and adding the adjusted scores. In each category, the highest overall score received the gold medal, the next highest earned the silver medal, and the third highest took the bronze medal.

To prevent products that received a small number of high scores from unduly influencing the results, we instituted a vote qualification minimum: In order to be eligible for award consideration, a product had to get at least 25 percent of the number of responses received by the top vote-getter in its category.

Emerging Technologies awards were determined by *Information Security* and SearchSecurity.com editors, who chose three innovative technologies that address a critical security need for enterprises and/or SMBs.