BUYING SPREE

2003 ISM Product Survey

IT professionals are planning massive security rollouts over the next three years. But shrinking budgets may throw a wrench in the works.

by ANDREW BRINEY and FRANK PRINCE

You've heard it a million times: Infosecurity is a process, not a product. But don't try telling that to the 1,138 respondents to *Information Security*'s 2003 Product Survey. These IT security professionals never met a product they didn't like.

With few exceptions, survey respondents predict that security product deployments over the next two years will outstrip the past two years. Intrusion detection and prevention will be red hot, with 2001-2005 compound annual growth rates (CAGRs) exceeding 40 percent per year. Products with a smaller current installation base—say, identity management—are growing even faster.

And we're not just talking about one-off point installations. Over 40 percent of organizations plan to deploy more than three security products between now and 2005.

"We're investing in firewalls this year, and will be adding antivirus products and evaluating and likely purchasing IDSes," says Rick Richmond, manager of the Computing Laboratories at the University of Wisconsin at Eau Claire.

Despite these sunny predictions, clouds loom on the horizon. Many security vendors failed to make their Q1 numbers, and the economic recession and political instability in many parts of the world may cripple enterprise spending for months to come *(see "Fiscal Reality Check," p. 34)*.

INSIDE...

image by MIKE RADENCICH

What's Hot, What's Not

So, what are the "hot" technology areas? The answer is, "It depends on your point of view." An IT security officer might want to know which technologies are must-have IT security "standards." But a vendor, stock analyst or venture capitalist may want to know what technologies are growing most rapidly year-to-year.

The point is that a hot technology from one perspective may not be hot from another. With that in mind, the products in this year's survey are broken out into three primary categories, each of which uses a different success metric: "Standards," "Emerging Standards" and "Fast Movers." Identification and authentication (I&A) is presented in a separate section from these three, because solutions in this category are affected by different market forces than other security solutions. Similarly, third-party security services, such as managed monitoring and penetration testing, are discussed separately *(see "At Your Service," p. 36)*.

Standards

Standards are defined as security technologies that are deployed in more than 75 percent of respondent organizations. These technologies are the most mature and established security products in the industry, regarded by most organizations as fundamental to the protection of critical information resources.

In 2003, three products fit into the Standards category: antivirus (present in 95 percent of organizations), firewalls (88 percent) and virtual private networks (77 percent) *(see Figure 1, right)*. By 2005, all three technologies will be deployed in 19 out of 20 organizations.

Antivirus. AV is a universally accepted security product, so its low compound annual growth rate (.5 percent) between 2001 and 2005 is understandable *(see Figure 4, p. 33)*. While some smaller organizations will be acquiring AV for the first time, other enterprises will be retiring old AV solutions in favor of new technologies with enhanced scanning and management capabilities.

Typically, product implementation occurs in three stages: evaluation, rollout and full deployment. Between 2001 and 2003, AV deployments grew while evaluations and rollouts declined. But between 2003 and 2005, that trend reverses. Deployments will decrease while evaluations and rollouts increase.

"I'm seeking a more centralized AV solution," says Ken Buszta, CISO of the city of Cincinnati. "We use AV software now, but each department will have 15 or 20 or 100 licenses rather than a central location. Like all local governments,

Upshot

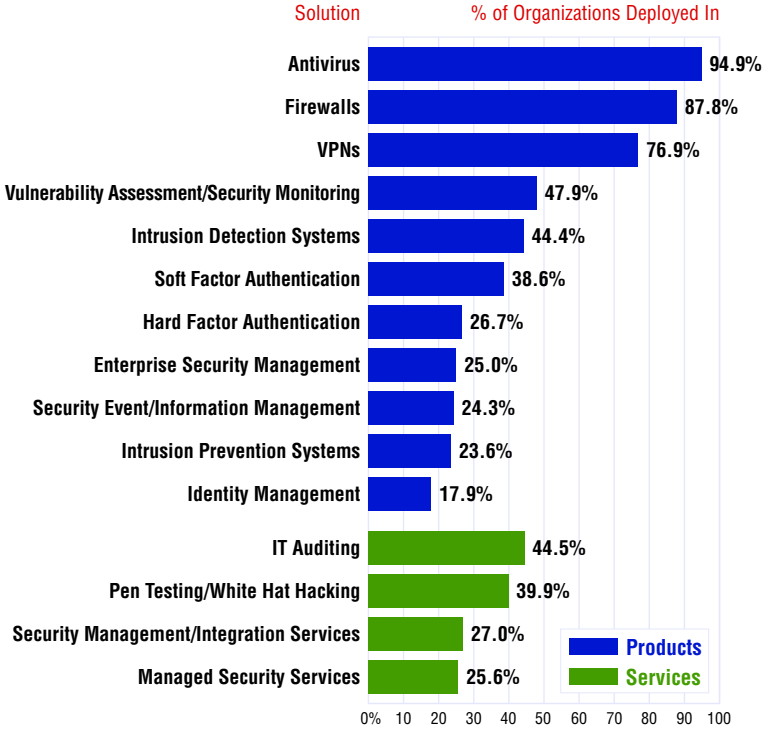
The 2003 *Information Security* Product Survey was completed by 1,138 IT security professionals in February 2003.

- By 2005, **antivirus**, **firewalls** and **VPNs** will be deployed in 95 percent of organizations.
- **Identity management** and **intrusion prevention** are the fastest-growing security products, with 45 and 43 percent compound annual growth rates (CAGRs), respectively.
- By 2005, 60 percent of organizations will have *both* **IDS** and **vulnerability analysis** tools deployed, up from only 7 percent in 2001.
- **Security services** are a mixed bag. Overall, they're experiencing greater than 25 percent CAGR, but primarily within a narrow community of organizations. More than 44 percent won't even consider **managed monitoring** by 2005.
- **Security budgets** continue to shrink, both in total dollars and as a proportion of IT spending. Security spending is one of the first budget cuts during lean times.

FIGURE 1

2003 Deployment Rate

Percentage of organizations that will have these technologies fully deployed in 2003.



Category Definitions

Products

Intrusion Detection Systems (IDSes)
Hardware and software systems that perform network intrusion detection or host intrusion detection via inline traffic analysis, passive monitoring, signatures or statistical anomaly detection.

Intrusion Prevention Systems (IPSes)
Trusted OSes, kernel-hardening tools, host application access control, Web server shields and Web application firewalls.

Firewalls
Enterprise gateway hardware and software (packet filters, circuit/app proxy servers, stateful inspection), PC firewalls and application filters, and embedded/hardware firewalls.

Antivirus Tools (AV)
Traditional gateway, server or PC-based AV scanning engines and heuristic pattern matching. Doesn't include URL or spam blockers or active content scanners.

Virtual Private Networks (VPNs)
Software and hardware, bundled or unbundled from firewalls, routers or gateway servers. Includes server- and client-based solutions, both link and application-layer, as well as session authentication tools (SSH).

Enterprise Security Management
Policy creation/management/automation tools, password reset tools, configuration/patch management, rule set management, remote device management.

Security Event/Information Management Tools (SEM/SIM)
Centralized correlation, analysis and data mining of security events or alerts triggered on remote, multivendor, heterogeneous security devices.

Identity Management
Access control tools, directory servers, authorization, user account provisioning and administration, automated password reset, Web and enterprise single sign-on, Web services tools.

Vulnerability Assessment/Security Monitoring
Vulnerability scanners, forensics analysis, penetration-testing tools, audit tools and network traffic monitors/sniffers.

Authentication (Soft Form Factor)
"Strong" or two-factor network or host authentication products, such as UserID/password security tools, soft tokens, public-key infrastructure (PKI) software and biometrics.

Authentication (Hard Form Factor)
"Strong" or two-factor network or host client-side authentication products, such as tokens, smart cards, USB tokens and RF proximity devices. Doesn't include password reset/automation tools.

Services

Managed Monitoring Services
Monitoring and/or management of firewalls, IDSes, AV, etc., using an outsourced provider's security operations center.

Security Management/Integration Services
Traditional consulting services involving security program development, policy creation/development, employee device training, security assurance services or installation/deployment of third-party technologies.

IT Audit Services
Third-party IT auditors for policy/regulatory compliance.

White-Hat Hacking/Penetration Testing Services
Services that perform security assessments, cyberattack simulation or platform/device vulnerability analysis.

we're in a tighter budget situation, so we're looking to show some savings."

Another factor in the continued growth of AV is that, of all the "external" security-related threats, viruses and worms have the most visible and direct impact on enterprise computing. When a virus or worm infects the network, it has an operational impact that everyone in the organization feels—including those who authorize security purchases. Combine that with a vital and competitive AV industry, and it's clear why those who haven't deployed an AV solution (or who have let their solution lapse) will reconsider their position in the coming years.

Firewalls. The survey data for firewalls show a similar pattern. Firewalls have the second-lowest overall CAGR—only 3.2 percent—a reflection of its already full installation base. Firewall deployments stay steady over the next two years, and new rollouts continue to decline slightly. But evaluations will actually begin to ramp up during the same period, indicating that organizations will be revisiting their firewall decisions.

Some organizations, like Minneapolis-based St. Jude Medical, are standardizing on a particular firewall technology—in St. Jude's case, Check Point's FireWall-1. Other organizations, such as Catholic Health Systems of Buffalo, N.Y., are going in the opposite direction, diversifying firewall types and brands to add defense-in-depth. Still others are simply abandoning legacy solutions for tools that better meet their security needs.

"We're going to change some products we have today and move to other vendors," says Tapan Shah, director of information technology at Del Global Technologies. "We're abandoning, for instance, the Microsoft ISA server platform [because] we find it too restrictive to deploy effectively. We think that hardware-based firewalls are better for us, so we're moving away from Microsoft to Cisco PIX firewalls."

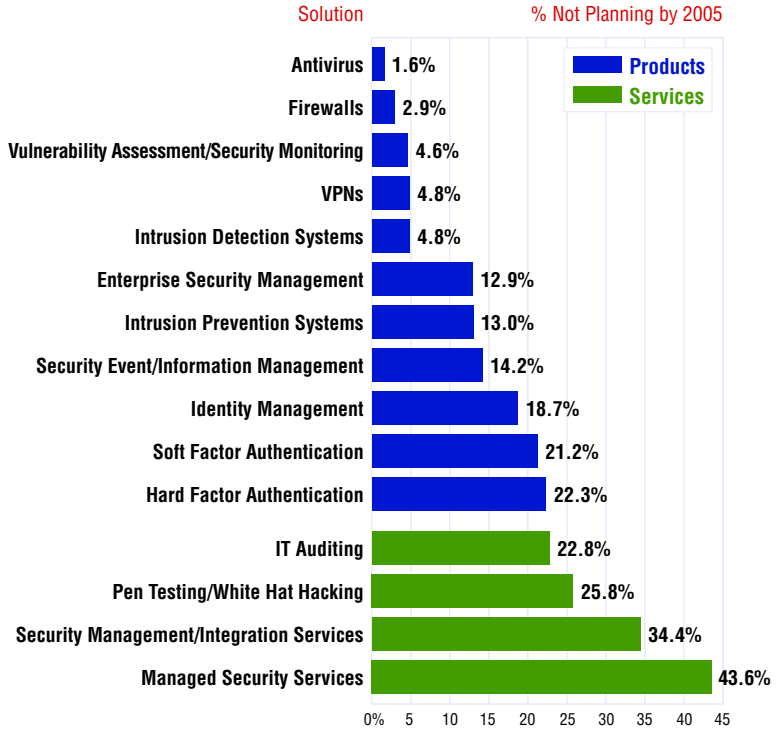
Virtual private networks. VPNs are the survey's winner in the balance between growth and staying power. More than three out of four organizations deploy some type of VPN, and yet the technology is growing at 16 percent CAGR. By 2005, 87 percent of organizations plan on deploying a VPN, and 95 percent plan on at least considering one *(see Figure 2, p. 32)*.

One of the reasons that VPNs can maintain strong growth rates despite a wide deployment base is that the technology comes in many shapes and sizes. For example, a company that does IPSec tunneling between routers may expand its VPN rollout to include PPTP VPNs for road warrior connections into a RAS. Organizations

FIGURE 2

(Un)Tapped Markets

Percentage of organizations that ***don't*** plan to deploy or evaluate these technologies by 2005.



are also rolling out clientless "VPN-like" services using SSL for data integrity and confidentiality, which also may be included under future VPN deployments.

Selim Nart, a network architect at application services provider Vignette, is investing in a clientless Web-based VPN for remote employees. "We have home office users who live out in the country, and they don't have DSL or cable modems, so the only solution [for broadband] is satellite Internet, which doesn't work at all with the regular VPN solutions."

VPNs also lead the pack when it comes to conversion rates *(see Table 4, p. 39)*. In 2002-2003, nearly eight out of 10 VPN evaluations turned into a rollout, and 100 percent of the rollouts turned into full-scale deployments. Translation: Organizations that consider buying a VPN usually do, and when they do, it doesn't take long to get them up and fully operational.

Emerging Standards

What's the difference between "Standard" and "Emerging Standard"? If Standards are a "must-have" for most organizations, emerging standards soon will be. On the other hand, Emerging Standards have a much higher growth rate than Standards, though not the fastest growth of all the products in the survey.

In 2001, only 7 percent of surveyed organizations had implemented both products in the Emerging Standard category: intrusion detection systems (IDSes) and vulnerability assessment/security monitoring (VA/SM). By 2005, 60 percent will have both deployed, and 75 percent will have one or the other installed.

Intrusion detection systems. For a product set that's only been around for five years, IDSes have an unusually checkered past. Their reputation for false positives, complex configuration and expensive maintenance still plague them.

"Everybody found out that buying IDSes doesn't solve any issues," says Vignette's Nart. "They found that by buying these things, they had to train people and hire extra hands to monitor all the IDSes."

Despite these problems—or, perhaps, because of them—organizations continue to evaluate and deploy IDSes in droves. In 2003, 45 percent of surveyed organizations have IDSes deployed. Of those that don't, more than half are considering them. The 42 percent CAGR for IDSes puts them in the top four of our product rankings.

Part of the growth is attributable to companies supplementing freeware or custom-developed IDSes with new commercial tools.

"Intrusion detection is something we've done before, and it's also a new product to us," says Richard Pendergast, VP of systems at Travelocity. "We did it mostly with homegrown stuff. We're looking for the bulk of it to be commercial going forward."

Other companies are holding back on IDSes for a different reason: they're waiting for the problems in early versions to be resolved, and looking for more advanced reporting capabilities.

"We're definitely looking at intrusion detection, but I want more than that," says Buszta of the city of Cincinnati. "I want something that's going to help me not only recognize that I've got a problem on my network, but help me start mitigating the problem.

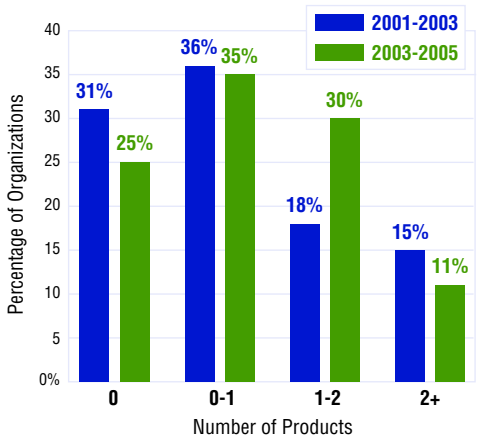
"I don't want something that's just going to alert me to the problem and that's it," Buszta adds. "I need something that can go in and mitigate an intrusion as well. Even if it doesn't take care of the whole problem, it buys me some time to develop a fix."

Vulnerability assessment/security monitoring. The VA/SM market also shows robust growth

Figure 3

Multiple Rollouts

Between 2003 and 2005, organizations will accelerate the number of security products and services they deploy.



given its relatively strong installation base. Roughly half of surveyed organizations have a VA/SM solution in place right now, so the technology is well established. Of those who don't license their own VA gear, many contract with third-party security assessment services.

Overall deployments will grow at more than 36 percent CAGR for the years 2001 through 2005, ultimately resulting in an 85 percent deployment rate (and 95 percent "consideration rate") by 2005. While showing strong deployment growth, the data on evaluations and rollouts paint a bleaker picture. Unlike IDSes, VA scanners will experience a slower growth rate between 2003 and 2005 than they did between 2001 and 2003. Both rollouts and evaluations drop off sharply over the next three years.

Taken together, the metrics in the survey suggest that organizations that intend to implement VA technology have already started to roll it out. It will take a few years, but after that, growth will slow.

Fast Movers

Stability and acceptance may be the measure of current and emerging standards, but what comes next? What technologies will be stable and accepted in the future, yet still show the strongest growth in the present?

According to the survey, three technologies make the cut: intrusion prevention systems (IPSes), enterprise security management (ESM) and security incident/event management (SIM or SEM) tools.

Intrusion prevention. While only 24 percent of organizations currently have an IPS fully deployed, that number will grow to 62 percent over the next two years. Only one in eight companies say they have no plans to evaluate intrusion prevention solutions by 2005. It's not surprising, then, that the CAGR for IPSes—43 percent—is second only to identity management, which is starting from a much smaller installed base.

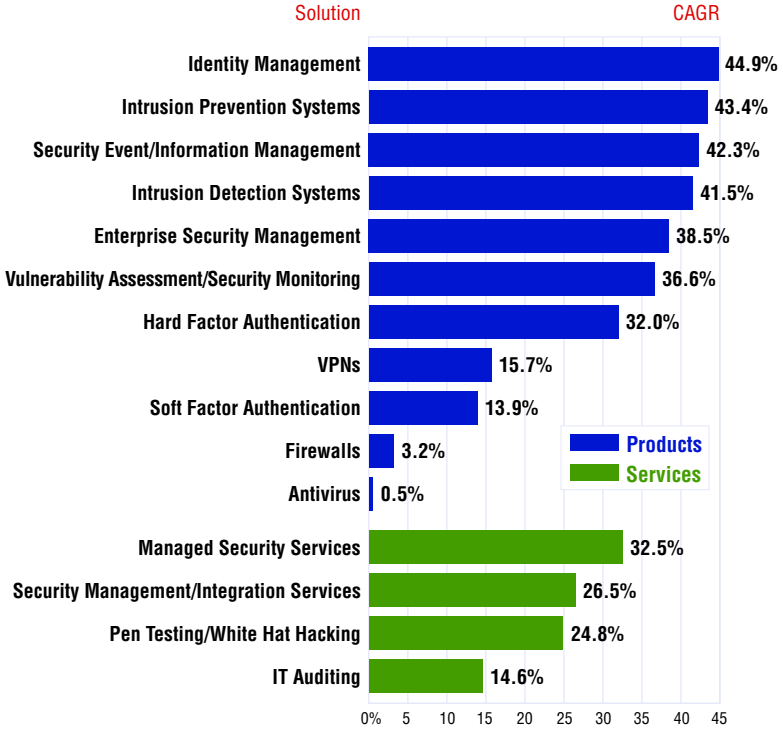
"I see intrusion prevention as the next wave," says Samantha Thomas, CISO of the California State Teachers' Retirement System. "The technology is robust enough now. Vendors have listened, and the smart engineers out there have been working hard on some interesting products."

Unlike VA scanners, demand for IPS solutions remains strong going forward. While early-stage evaluations weaken over the next three years, rollouts actually increase slightly between 2003 and 2005.

Enterprise security management. While only about one-quarter of surveyed organizations currently have an ESM platform in place, the prod-

Figure 4

Compound Annual Growth Rate (CAGR), 2001-2005



SECURITY BUDGETS

Fiscal Reality Check

The road to hell is paved with good intention… but not enough cash.

Most organizations are planning massive security rollouts over the next few years. More than 40 percent, in fact, say they'll deploy three or more new security technologies between now and 2005.

But there's a big difference between *planning* a deployment and actually doing it. In tight economic times, all capital expenditure requests get examined under a microscope. Do you really need this now? Can it wait until next year? Is there a legitimate business need? What's our ROI? And even if you clear these hurdles, the P.O. may stall on the CFO's desk for months.

If organizations have a prayer of funding their security plans over the next two years, IT security budgets will have to increase substantially. Unfortunately, just the opposite has happened since fall 2002, according to two *Information Security* surveys on security spending. Overall security budgets as well as security spending per user and per machine *(Table 1)* are decreasing in many organizations.

"We aren't investing in too much," says David Stacey, global IT security director of St. Jude Medical, a 4,000-employee medical equipment manufacturer. Stacy says St. Jude already has security products installed, including firewalls and IDSes, "but for the most part, those products were purchased in the past."

What's more, survey data show that IT security budgets are decreasing 10 percent faster than IT budgets. That suggests that, when times are tough, the security budget is among the first IT line items slashed *(Table 2)*.

However, comparing one budget cycle to the next isn't necessarily an apples-to-apples exercise. Security budgets are often decentralized, making it difficult to account for total organization-wide security spending. Changes in employee responsibilities and accounting practices could also account for disparities.

Even chief security staffers have a hard time getting a handle on total security spending. "I'd say spending is up," says Ken Buszta, CISO of the city of Cincinnati. "But there's no one or group centrally focused on it." ◗

–ANDREW BRINEY

Table 1

Security Budgets

Security budget per managed machine by organization size, 2002-2003

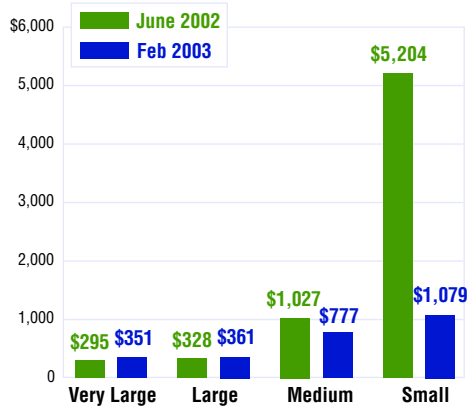
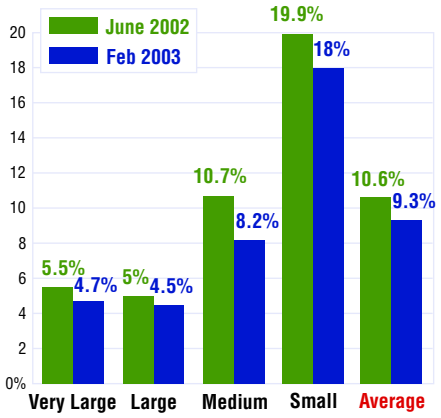


Table 2

% of IT Budget

Security budget as a percentage of IT budget by organization size, 2002-2003



uct space will experience a robust 39 percent CAGR between 2001 and 2005, at which point it will be deployed in two-thirds of organizations. Only 13 percent of companies have no plans to consider ESM in the next two years.

Today, ESM solutions are deployed most frequently in very large enterprises. This isn't surprising, given that larger enterprises have significantly more policy and configuration management problems than smaller organizations, not to mention a larger discretionary security budget to spend on management tools.

But by 2005, medium- and large-sized organizations will begin to catch up with their very large colleagues, as ESM solutions get more granular and extensible—and more integrated with network management systems. In 2001 only half as many medium-sized organizations as very large organizations had deployed ESM. By 2005, the proportion grows to two-thirds. Large organizations grow even faster, from half the deployments of very large organizations to three quarters.

Security event/information management (SIM/SEM). Functionally, SIM solutions are on the flip side of the coin from ESM. Where ESM pushes policy, configuration, patching and rule set updates to distributed devices, SIM tools collect, correlate and analyze security-relevant

At Your Service

While the security services market is growing, many organizations are still reluctant to outsource.

When it comes to security, "to outsource or not?" is never an easily answered question. On the one hand, outsourced services usually cost less than equivalent in-house product deployment, operation and management. Why devote two full-time admins to IDS alert duty when you can pay an MSSP to do it for you?

On the other hand, you're giving the keys to the kingdom to an outsider, and who knows how much you can trust them to protect your information and do the job right. How many intrusions will that MSSP miss because they don't really understand your infrastructure? And will they still be around next year?

The industry's mixed attitude toward security services is reflected in the 2003 Product Survey. Each of the services in the survey is growing rapidly between 2001 and 2005—as much as 33 percent CAGR. That growth, however, is partly attributable to their small initial deployment base, as low as 26 percent in 2003 *(Table 3)*. Moreover, by 2005 a substantial proportion of organizations will still have no plans to use security services—a stark contrast to attitudes about most products in the survey.

Managed monitoring services. The MMS offering is near the bottom of the survey's performance list. Only 26 percent of organizations are using outsourced monitoring this year, and 44 percent have no plans for them through 2005.

Still, the MMS space shows strong compound growth: 33 percent CAGR from 2001 to 2005—an indication that the market is stabilizing after some early fits and starts. That growth rate may be deceiving, however. While increasing market penetration from 26 to 40 percent will be easy, capturing the remaining 60 percent of the market promises to be an uphill battle.

Security management/integration services. Not surprisingly, traditional security integration and consulting services fared better than MMSes in the survey. As security hardware and software becomes more pervasive and more integrated into the network infrastructure, demand for these services will continue to rise. By 2005, two out of every three organizations will use some type of security consulting or integration service.

Table 3

Security Services Trends

SERVICE	2003 DEPLOYMENT RATE	CAGR, 2001-2005	NOT PLANNED BY 2005
Managed Security Services	25.6%	32.5%	43.6%
Security Management/ Integration Services	27.0%	26.5%	34.4%
Pen Testing/ White Hat Hacking	39.9%	24.8%	25.8%
IT Auditing	44.5%	14.6%	22.8%

Penetration testing/white hat hacking. The deliverable for this service is also becoming more standardized. It's an easily packaged service: the provider gets in, gets the job done and gets out. Some 40 percent of organizations currently buy this service, and 74 percent will consider it by 2005.

The downside to this type of service is that service providers often use it as a "nose in the tent" for further consulting services. Moreover, the quality of the service is inconsistent.

"We're a little skeptical about vulnerability analysis [services]," says Richard Pendergast, VP of systems at Travelocity. "It's a great way for a board of directors to feel good about the company. The consultants get a couple of hundred thousand dollars to wander around and tell you everything you already know."

IT auditing. Many organizations are required by law or regulation to contract with third-party auditing services. This and the fact that IT audit is a standardized activity in most organizations explains the stable pipeline and more modest growth rate of this service set. IT audit services will continue to be popular in years to come, eventually used by nearly eight out of 10 organizations. ◗

–ANDREW BRINEY

alert, event or log data.

SIM products are less mature than ESM. While some ESM solutions are in their third and fourth generation, most SIM products are in their first or second. However, the 2003 deployments are virtually identical for both solutions—about 25 percent in both cases. Moreover, both products have "low" conversion ratings, indicative of long evaluation and rollout life cycles.

Identification and Authentication

Three technologies fall into our breakout of I&A solutions: authentication software, authentication hardware and identity management. While I&A is important to organizations of all types and sizes—if only for auditing purposes—several factors differentiate these solutions from others in the product survey: they are highly dependent on

CONTINUED ON P. 39

EA WINNER 2003 EXCELLENCE AWARDS

Product Ratings by Category

In March, *Information Security* presented its third annual Excellence Awards in recognition of the industry's top commercial security products in 10 categories. Award winners were selected based on two criteria: installation base and quality.

The magazine's subscribers were asked to indicate which of 217 candidate products they deployed in their organization, and then rate those installed products on a scale of 1 (low) to 5 (high) in terms of "overall quality, performance, features, security, documentation and vendor support/service."

Listed below are the top five products by installation base in each category (including ties). From these five, three finalists were selected based on quality rating. The winner had the top rating of the three finalists.

NOTE: The awards balloting was conducted *separately* from the 2003 Product Survey. A total of 474 subscribers completed the awards ballot in January and February 2003.

PRODUCT	MARKET SHARE†	QUALITY RATING, 1-5
Intrusion Detection Systems		
EA WINNER **Tripwire, Tripwire Inc.**	**16%**	**3.94**
NFR NIDS, NFR Security	6%	3.84
Cisco IDS, Cisco Systems	18%	3.81
Sentarus, Silicon Defense	6%	3.71
RealSecure, Internet Security Systems	23%	3.69
Intrusion Prevention Systems		
EA WINNER **StormWatch, OKENA**	**6%**	**4.63**
STAT Neutralizer, Harris	6%	4.17
SecureIIS, eEye Digital Security	11%	4.05
NetScreen IDP, NetScreen	13%	4.04
Trusted OS, Sun Microsystems	7%	3.92
Entercept, Entercept Security Technologies	13%	3.76
AppShield, Sanctum	6%	3.73
Firewalls		
EA WINNER **FireWall-1, Check Point Software Technologies**	**23%**	**4.23**
NetScreen Firewall, NetScreen	6%	4.00
ZoneAlarm Pro, Zone Labs	13%	3.99
PIX, Cisco Systems	18%	3.92
Norton Personal Firewall, Symantec	6%	3.71
Antivirus Tools		
EA WINNER **Norton AV, Symantec**	**38%**	**4.24**
Antigen, Sybari Software	3%	4.23
Trend Micro AV, Trend Micro	16%	4.18
Sophos AV, Sophos	4%	4.07
McAfee AV, Network Associates	28%	3.95
Virtual Private Networks		
EA WINNER **Nokia VPN, Nokia**	**7%**	**4.18**
Contivity VPN Switch, Nortel	11%	4.14
VPN-1, Check Point Software Technologies	22%	4.12
VPN Concentrator, Cisco Systems	21%	4.06
Windows 2000 VPN, Microsoft	9%	3.26

PRODUCT	MARKET SHARE†	QUALITY RATING, 1-5
Network Security Management		
EA WINNER **Network Security Manager, Intellitactics**	**9%**	**4.64**
bv-Control, BindView	9%	4.17
Security Manager, NetIQ	16%	4.05
ESM/Security Management System, Symantec	13%	3.91
McAfee ePolicy Orchestrator, Network Associates	13%	3.69
Identity Management		
EA WINNER **ClearTrust, RSA Security**	**14%**	**4.16**
eDirectory, Novell	9%	4.06
Tivoli Identity Manager, IBM/Tivoli	6%	3.85
SiteMinder, Netegrity	8%	3.80
Active Directory, Microsoft	32%	3.53
Vulnerability Assessment/ Security Monitoring		
EA WINNER **Retina, eEye Digital Security**	**11%**	**4.06**
STAT Analyzer, Harris Corp.	5%	4.05
Sniffer Pro, Network Associates	17%	3.99
SAINT, SAINT Corp.	8%	3.97
Scanner Suite, Internet Security Systems	19%	3.94
Authentication–Soft Form Factor		
EA WINNER **SSH Secure Shell, SSH Communications**	**26%**	**4.17**
Steel-Belted RADIUS, Funk Software	8%	4.14
Keon, RSA Security	13%	4.09
VeriSign PKI, VeriSign	21%	3.87
Entrust PKI, Entrust	11%	3.81
Authentication–Hard Form Factor		
EA WINNER **SecurID, RSA Security**	**61%**	**4.28**
Smart Card, ActivCard	9%	4.17
e-Token, Aladdin Knowledge Systems	3%	4.13
Token/Smart Card, CryptoCard	3%	4.12
iKey, Rainbow Technologies	4%	4.10

† "Market Share" refers to the percentage of total product installations (not total organizations) in each category.

Table 4

Conversion Life Cycles

All product purchases follow a "deployment life cycle." First, organizations evaluate a technology. Then, if they license it, there's an initial rollout period that lasts between a few weeks and several months. Once that period is over, the product is considered fully deployed. After that, it may be retired or abandoned. One stage logically feeds into the next.

The following table charts the conversion rates of various security solutions in two areas: The proportion of evaluations that turned into rollouts within a year ("Evaluation Conversion Rate" or ECR); and the proportion of rollouts that turned into deployments ("Rollout Conversion Rate" or RCR). Products and services with a "High" conversion rating were faster to roll out and deploy than those with a "Medium" or "Low" rating.

	2003 ECR	2003 RCR	OVERALL CONVERSION RATING
Products			
VPNs	78.2%	100.0%	High
Firewalls	68.5%	86.7%	High
Intrusion Detection Systems	48.6%	74.9%	High
Vulnerability Assessment/ Security Monitoring	54.9%	68.0%	Medium
Antivirus	21.9%	100.0%	Medium
Hard Factor Authentication	25.8%	74.0%	Medium
Intrusion Prevention Systems	19.0%	44.7%	Low
Soft Factor Authentication	24.8%	36.5%	Low
Security Event/Information Management	34.6%	31.3%	Low
Enterprise Security Management	34.7%	22.5%	Low
Identity Management	27.5%	26.5%	Low
Services			
Penetration Testing/White Hat Hacking	47.9%	91.1%	High
Managed Security Services	50.1%	84.1%	Medium
Security Management/ Integration Services	40.1%	48.7%	Medium
IT Auditing	34.9%	40.1%	Low

CONTINUED FROM P. 36

the state of the Internet economy, on the scale of an organization's operations, on the distribution of the user base, and on the core need for security.

For instance, a five-employee company that only uses the Internet for e-mail and Web surfing won't question if they need a firewall or antivirus scanner. But if they don't have an interactive Web site or connected business partners, they won't be looking at provisioning software—ever. On the other hand, if an organization has a lot of business partners and mobile users, or a complex environment, these technologies are no longer discretionary; they become essential.

Authentication software. Arguably, any organization that requires a user ID and password uses authentication software. And any organization that uses Windows 2000 uses a Kerberos authentication scheme by default. So, strictly speaking, the 38 percent deployment rate and 14 percent CAGR paint a pretty bleak picture for basic authentication.

But since we asked our readers only about application-layer and "add-on" authentication software, the numbers look a little better.

"We are continuing to develop our directory infrastructure and to tie it to other authentication methods like [RSA Security's] SecurID and RADIUS," says Doug Torre, director of networking and technical services at Catholic Health Systems.

PKI's ongoing problems with deployment complexity and interoperability are reflected in the low evaluation and rollout conversion ratings for authentication software: 25 and 37 percent, respectively. More than 21 percent of organizations in the survey have no plans to evaluate any authentication software. That lends credence to

VENDOR SELECTION

WANTED: Stability and Support

In an industry dominated by startups, enterprise buyers place a premium on tech support and product features and functionality.

The security industry has its share of 800-pound gorillas: Symantec, Network Associates, ISS and RSA Security immediately come to mind. But the marketplace is dominated by thousands of hungry startups with $10 million in VC and a gizmo that will change the world—or so they claim.

While startups may offer a new twist to an old problem—and at a significantly lower price than the 800-pound gorilla—there's a risk they won't be around long enough to support it.

"If you're using a commercial product, it's always important to have good technical support, especially if it's a security product and the enterprise is dependent on it," says Chris Barry, manager of information systems at InfiniCon Systems.

In an industry populated by one-hit wonders, vendors that can provide top-notch tech support, maintain market share and demonstrate financial stability will have a leg up on the competition, according to the survey *(Figure 5)*.

"If you purchase a product and don't have good tech support, it's a useless product," says Selim Nart, a network architect at Vignette. "It's like buying a car and not buying any warranty on it, and it breaks down. That's why you see large companies rarely using freeware products."

Security technology also has to perform, or security professionals won't put up with it for long. The most important single factor in product selection, named by 58 percent of survey respondents, was features and functions *(Figure 6)*. The number two spot went to a technology's ability to fit in with the rest of an organization's security infrastructure.

For most of the technology categories in our survey, no one vendor has a dominant position. So if a technology doesn't show strong overall growth, vendors won't be able to provide the kind of services or achieve the stability that our readers judge critical to their success. ◗ –ANDREW BRINEY

Figure 5

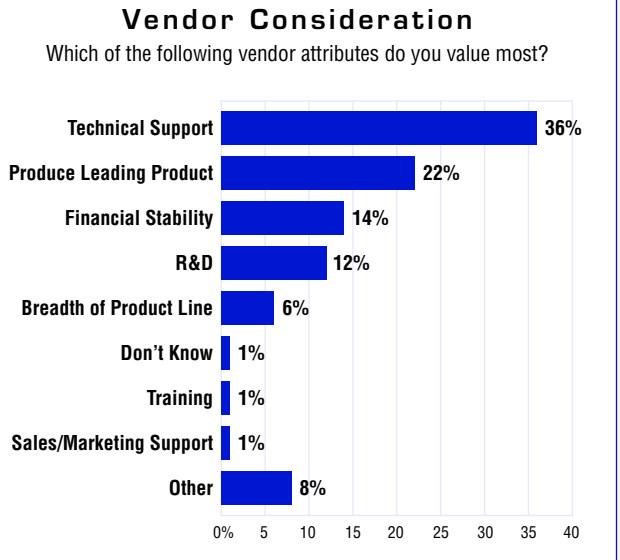
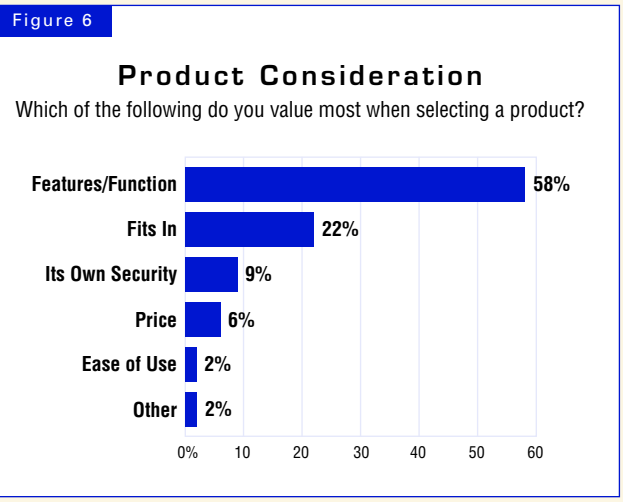


Figure 6



the old gag about PKI: "It's the technology of the future, and always will be."

Authentication hardware. Though less fully deployed than authentication software, authentication hardware shows a much stronger growth rate (32 percent CAGR compared to 14 percent). And while only one in four evaluations turn into a rollout, three-quarters of implementations are successful.

Hardware tokens also have managed to strike a good balance between security and ease of use. And while the survey didn't specifically address them, all indications are that the adoption of smart cards for network and physical authentication will also increase dramatically over the next three years.

Identity management. In spite of very low 2003 deployments (18 percent), the fastest growing authentication and access control technology is identity management, which leads the pack in

growth rate with a 45 percent CAGR. By 2005, fully 77 percent of organizations plan to evaluate ID management solutions.

The immaturity of the ID management solution space is reflected in the lowest conversion rates in the survey. Only 28 percent of evaluations converted to rollout or deployment in a later year. And of all the rollouts, only 27 percent actually completed in a year.

The Four "P's"

To put it bluntly, the whole industry is growing like weeds. Deployments of 13 out of the 15 products and services in the survey will grow by more than 15 percent between 2001 and 2005.

However, predictions of substantial security rollouts may be optimistic in light of current fiscal realities. Unless organizations loosen the IT purse strings, all this planning will be for naught.

While an economic turnaround would surely give rise to increased security spending, labor costs will remain a major (and often overlooked) component of security budgeting.

"Products are not a silver bullet," says David Stacy of St. Jude Medical. "A lot of them have a long tail from an administrative standpoint. You have to maintain them, enhance them and, sometimes, pay additional staff to administer them."

There is also the risk that organizations are viewing technology solutions as the cure-all to security ailments. Effective product use is obviously critical to reducing enterprise risk, but a well-rounded security program must also include budget for policies, people and process.

"Not all security issues are solved with security products," says Stacy. "There's the personnel aspect of it, managing the workforce and users, setting policies and procedures. The purchase of products is complementary to those other activities." ◗

ANDREW BRINEY, CISSP (**abriney@infosecuritymag.com**), is editor-in-chief of *Information Security*.
FRANK PRINCE (**fpsec1@grumpybear.com**) is an independent IT research consultant and former senior analyst at Forrester Research.