IT STRATEGY GUIDE

InfoWorld

GET TECHNOLOGY RIGHT

STRATEGIES FOR ENDPOINT SECURITY

See the full selection of InfoWorld IT Strategy Guides at http://www.infoworld.com/reports/y/strategy-guide

ENDPOINT SECURITY: IS THE FUTURE IN SOFTWARE SUITES?

SYMANTEC, MCAFEE, OTHERS PUSH SUITES OVER STAND-ALONE PRODUCTS.

BY ELLEN MESSMER, *NETWORK WORLD*

Is corporate endpoint security turning into a “suite” spot?

The market’s top two players, Symantec and McAfee, continue to win about 40% of the highly fragmented corporate endpoint security market, now at about $3 billion. Meanwhile, distant third Trend Micro, at about 6%, suddenly finds itself neck and neck with Sophos, the antimalware vendor that acquired endpoint encryption firm Utimaco in late 2008.

But the race to win the corporate customer is shifting from stand-alone antivirus-style products to burgeoning software suites that combine antimalware, network access control and, now, systems management.

Though dozens of competing vendors craft products for specific security and systems management functions—and many IT managers strongly argue they prefer it that way and fret about vendor lock-in—there’s some cause to think the future may be dominated by endpoint suites.

“The trend for endpoint is primarily that it has been moving to suite solutions,” says IDC security analyst Charles Kolodgy. “There’s a move to incorporate much more than security into the endpoint suites—configuration control, patch management and other systems management capabilities.”

IDC research for the corporate market shows stand-alone antimalware sales stalled in 2007, dropped to $1.14 billion in 2008 and are expected to fall to $1.05 billion in ‘09. But the category IDC calls “security suites” is quickly rising, from $637.7 million in 2007 to a predicted $1.21 billion in 2009.

While Symantec and McAfee already have their own systems management software—Symantec acquired Altiris and McAfee has McAfee Remediation Manager—to integrate into the endpoint agent, Trend Micro elected to team with a partner, somewhat as it has done with Third Brigade on host intrusion detection.

Trend Micro joined forces with BigFix to come up with the Endpoint Security Platform—based on the BigFix management console that Trend Micro will offer under its own brand.

“BigFix has best-of-breed client patch management and security configuration; we have antivirus and Web protection,” says Ron Clarkson, Trend Micro’s director of enterprise endpoint security.” The company views the alliance as strategically important to compete with McAfee and Symantec in the larger corporate market.

Symantec’s souped-up suite in this race is Symantec Endpoint Protection, and McAfee’s is Total Protection for Endpoint Advanced.

The appeal in the security suites is a single code base and smaller footprint than having five or six separate software agents, common management, plus somewhat lower cost, Kolodgy says.

According to McAfee CEO Dave DeWalt, the cost-saving is “at least 30%” in buying the integrated endpoint suite vs. McAfee’s separate software products. DeWalt says a third of McAfee’s installed base in the enterprise market has shifted to the Total Protection suite, with the various security and systems management functions supported by McAfee’s ePolicy Orchestrator management console.

SUITE NOTHINGS?

The fact that endpoint security vendors are packing ever-more functionality into endpoint agents does give some IT professionals pause.

The Sophos Endpoint Security and Control product, which packs in antimalware, desktop firewall, NAC and more, is fine, says Peter Clark, director of information security at Jordan’s Furniture based in Avon, Mass., even as he acknowledges the furniture chain isn’t using the NAC component yet.

But Clark, and Ethan Peterson, Jordan’s network engineer, say they question whether it would be an advantage to also pack in systems management.

“When a vendor tries to do everything, it doesn’t always work out,” Peterson notes, adding, “In some cases stand-alone has better value for the product, and it’s nice to have separation of security and systems management.”

Care New England Health Systems, which includes three hospitals, makes use of Kaspersky’s antimalware/desktop firewall software on 4,000 workstations, mostly Windows XP, says Keith Lee, end-user services manager there. He says he’s more inclined to look for “best of breed” versus combining many separate security and systems management into one single software agent.

Josh Corman, principal security strategist for the IBM Internet Security Systems division, says he’s heard customers call the endpoint suites “suite nothings.”

“With the big suites, some feel they’re giving up choice and they’re afraid of vendor lock-in,” Corman says.

The push to pack more into the security endpoint is bringing in a wave of change in both the systems management market and the security market over the next years, according to IDC.

IDC predicts the worldwide corporate endpoint security market will hit $4.41 billion by 2012. The security suites are expected to comprise almost half of this market by then, eclipsing stand-alone antimalware and other categories such as endpoint threat management, which will be in sharp decline.

CORPORATE SECURITY SUITES ON THE RISE

CUSTOMERS ARE SHOWING A PREFERENCE FOR SUITES OVER STANDALONE PRODUCTS (THOUGH STANDALONE ENCRYPTION PRODUCTS ARE EXPECTED TO HOLD THEIR OWN)

(IN THOUSANDS OF DOLLARS)	2007	2008	2009	2010	2011
ANTIMALWARE	$1260	$1,146	$1,055	$1,002	$950.0
ENDPOINT THREAT MANAGEMENT (INCLUDES DESKTOP FIREWALL, HOST, IDS/IPS	$274.1	$241.2	$219.1	$205.2	$196.9
SECURITY SUITES	$637.7	$914.2	$1,215.8	$1,510	$1,811
OTHER ENDPOINT SECURITY (INCLUDES NAC, ENCRYPTION, DATA-LEAK PROTECTION)	$475,7	$642.3	$802.8	$935.4	$1,071

SOURCE: IDC

See the full selection of InfoWorld IT Strategy Guides at http://www.infoworld.com/reports/y/strategy-guide.

FULL DISK ENCRYPTION DOS AND DON'TS

"JUST ENCRYPT IT!" SEEMS LIKE A SIMPLE WAY TO PROTECT DATA, ESPECIALLY ON LAPTOPS. IT DOES PROTECT DATA, BUT IT'S NOT NECESSARILY SO SIMPLE. SAVE TIME (AND MAYBE YOUR DATA!) WITH THESE PRACTICAL TIPS. BY MARY BRANDEL, *CSO*

Full disk encryption (FDE) systems use strong encryption algorithms to automatically protect all data stored on the hard drives of PCs and laptop computers. Users can access the data via an authentication device, such as a password, token or smart card. This enables the system to retrieve the key that decrypts the disk. On many systems, functions such as key management, access control, lock-outs, reporting and recovery are all managed centrally.

According to John Girard, an analyst at Gartner, the main product differences come from varying approaches to management, encryption strength, user authentication, policy management and value-added features, such as protection of information on removable media.

Here we'll look at two prime considerations in selecting encryption solutions, as well as dos and don'ts suggested by veterans of encryption implementation.

PRIME CONSIDERATIONS

FDE VERSUS FILE OR FOLDER ENCRYPTION SYSTEM. With FDE, data is encrypted automatically when it's stored on the hard disk. This is different from file or folder encryption systems (FES), where it's up to the user to decide which data needs encrypting. FDE's biggest advantage is that there's no room for error if users don't abide by or don't understand encryption policies.

The shortcoming of FDE is that it does not protect data shared between devices or otherwise while in transit, stored on a portable hard drive or USB, or sent through e-mail, says Natalie Lambert, an analyst with Forrester Research. FES, she says, is ideal for this, although it requires a lot of attention to developing a policy for what gets encrypted and what doesn't, as well as training users on the policy. FES is also more compute-intensive than FDE, she says, leading to PC performance hits of 15% to 20%, versus just 3% or 4%.

HARDWARE VERSUS SOFTWARE ENCRYPTION. According to Girard, hardware-based encryption promises significant performance improvements over software-based technologies, and the new Trusted Computing Group (TCG) open standard offers a common management specification for hard-drive manufacturers.

However, there is a lack of real-world products using the standard, he says. Hardware encryption will continue to evolve, he says, and future choices will appear in other device subsystems, such as CPUs or supporting chip sets.

Today's self-encrypting hard drives—such as those from Seagate Technologies—are mainly geared toward consumers, Lambert says.

See the full selection of InfoWorld IT Strategy Guides at http://www.infoworld.com/reports/y/strategy-guide.

That's because without TCG, they do not yet perform better than software-based encryption, and most cannot be centrally managed. An exception, she says, is a partnership among Dell, Seagate and McAfee to provide laptops with encrypted hard drives and enterprise-level management tools. Wave Systems also sells key management software for Seagate drives, says Eric Maiwald, an analyst at Burton Group.

ENCRYPTION DOS AND DON'TS

DO PREP THE MACHINE. According to Girard, the biggest mistake people make when installing encryption is failing to ensure the machine is clean and running properly beforehand. "If there's a disk problem," he says, "parts of the code specific to the encryption engine will not be readable." He suggests defragmenting the hard drive, running Checkdisk several times, backing up the data, administering all patches and optimizing performance before encrypting. While the performance hit for encryption is only 1% to 3%, he says, "why not make the machine faster to minimize that or at least break even?"

> The biggest mistake people make when installing encryption is failing to ensure the machine is clean and running properly beforehand.

At Los Angeles County, which uses Pointsec, now from Check Point Software Technologies, CISO Robert Pittman's team conducted a health check on the hard drives of the county's laptops to see how much free space existed, how badly it was fragmented and the maintenance level of the operating system. His team identified about 20 out of the total 12,500 laptops that would need to be replaced prior to encrypting them.

Frank Ward, a consultant for the state of Connecticut, also ran drive-evaluation software on the state's laptops during the pilot phase of implementing encryption software from McAfee. About 15% of the hard drives failed, he says. By checking all the disks, the failure rate for installing McAfee on the state's 5,000 machines was just 3%.

DON'T JUMP IN TOO QUICKLY. It's also essential to have a clear road map for deployment. Some organizations use a centralized software delivery system. For instance, Raymond James Financial used LANdesk from LANdesk Software to do a mass deployment of Utimaco, says Pat Patterson, enterprise security architect at the St. Petersburg, Fla.-based financial services firm. However, he plans to activate the software one machine at a time, taking what he calls a "low and slow" approach. Not only does he need to remove previously installed encryption software, but he also wants a manageable way to deal with any issues that might arise.

"I don't want to show up on Monday and [see that] every machine is blue-screened," he says. "Utimaco is good about recovering from errors, but there are situations where the drive is on the edge, and spinning it for three hours will push it over. If we go too fast we'll be overwhelmed by support calls."

Most encryption software allows you to push it out to users' machines via a centralized software delivery system, Maiwald says. For instance, McAfee allows you to use its ePolicy Orchestrator for deployment, he says.

However, this is not always possible, as was the case in Connecticut. In the state's distributed environment, Ward found the centralized deployment mechanisms were not ubiquitous enough. He still needed to work fast, due to the state's strategy for accelerated deployment.

To do that, the state created five teams of three people to install McAfee (over a six-week period) on the laptops of 55 agencies and 950 state police trooper cars. The teams consisted of previously trained administrators, McAfee resources and an IT person.

"We'd give the agency a week's notice to get their machines logistically together and then try to get as many done in a day as we could," Ward says.

His team would set up in a conference room or other central location, connect 20 or so machines to a file server to download the software and then pull them offline to finish encrypting, which could take two hours for a 100G drive. "It was very much a production line," Ward says.

The agency continued working on any that didn't get completed, and they could bring any particularly troublesome machines to a centralized depot.

DON'T UNDERESTIMATE DEPLOYMENT TIME. As Ward found, installation takes time, especially for large drives. A good rule of thumb is that it takes two to four hours for the software to encrypt the drive, depending on its size.

Because of this, it's important to choose a system that will be easy to learn for administrators and vendors or resellers that provide customized training. When Pittman chose Check Point, he had about 100 people trained—two or three from each of L.A.'s 38 agencies—to encrypt 12,500 machines. It helped, Pittman says, to create a standardized configuration to be implemented. In all, it took about nine months, although 80% of the agencies were finished in six months.

DO CONSIDER BACKGROUND INSTALLATION. To keep deployment as low-impact as possible, consider a system that enables users to keep working during installation, Girard says. Even better, make sure you don't need to restart the process if it gets interrupted.

DON'T EXPECT FULL USER ACCEPTANCE. Users can be wary of added security, seeing it as an annoying roadblock that hinders technology performance, Lambert warns. One way to head off potential opposition is to fully communicate the what, why, how and when of deployment prior to implementation and stress that performance will be affected minimally, no more than 5%, she says.

DO TEST ON A PILOT GROUP. Pilot testing is important for several reasons, including ironing out potential problems and gauging user resistance and the scope of the full deployment, Lambert says. "User enrollment should be easy, but with some products, users get confused," Girard says. "When that happens en masse, you've got real problems because if you fail to set up enrollment properly, the machine has to be

HOW TO BUY FULL DISK ENCRYPTION

CHARACTERISTICS OF AN EFFECTIVE FULL DISK ENCRYPTION SOLUTION AND CRITICAL SELECTION CRITERIA, ACCORDING TO EXPERTS.

CHARACTERISTICS OF FULL DISK ENCRYPTION

According to research firm IDC, an optimal full disk encryption (FDE) system should be:

- **Centrally managed and controlled**
- **Rapidly deployed and maintained**
- **Policy driven**
- **Transparent to the user**
- **Easily supported by help desk or IT personnel**
- **Able to support removable media**
- **Expandable, allowing new managed encryption applications to be added, as needed**
- **Extensible, enabling organizations to add managed encryption to existing enterprise applications**

SELECTION CRITERIA

According to a presentation by Eric Leighninger, chief security architect at Allstate Insurance, selection criteria he used when choosing an FDE system included:

- **Strong key management**
- **Storage of encrypted keys separate from encrypted data**
- **Controlled views to keying material (separation of duties)**
- **Key recovery (onsite, offsite and disaster recovery)**
- **Interoperability with enterprise software**
- **Support for removable media**
- **Low performance degradation**
- **Background encryption processing capability**
- **Fault tolerance (power outages or user shutdown does not affect encryption process)**
- **Support for suspend and hibernation states**
- **Compliance with FIPS 140-2, a U.S. government computer security standard**

See the full selection of InfoWorld IT Strategy Guides at http://www.infoworld.com/reports/y/strategy-guide.

put into recovery mode. If the user never enrolled with the management console, it can be even trickier."

DO CHECK FOR INTERFERENCE WITH OTHER APPLICATIONS. Another reason for a pilot test is there can be device-driver or BIOS interference between the encryption software and other applications, Girard warns. "You should run it against your standard image, as well as potential things you'll install in the next year," he says.

Conflicts can arise between encryption and some desktop management systems that already have entries in the boot sector of the disk, Maiwald adds. "You can't have two things in the boot sector unless they were made to work together," he says, which some vendors are doing, such as GuardianEdge and Symantec. "We find problems in just about every enterprise, so the best advice is to test it."

DO CONSIDER YOUR AUTHENTICATION OPTIONS. Vendors offer different user authentication mechanisms, including PINs, passwords, smart cards and tokens, but the most popular is the password option. While it might seem more secure to challenge users with two separate passwords—one at preboot and one to enter the network domain—many organizations choose the single sign-on option.

DO CONSIDER AN INTEGRATED SUITE. When Patterson began looking for an encryption system, his search was two-fold, as Raymond James' antivirus software contract was also ending and he wanted to try a different endpoint firewall than what was offered via Windows. This led him to look for products in which these functions could all be managed through a single console. "Otherwise, we'd need a fleet of people to run these systems, and no single picture of what's happening on the network," he says.

With Utimaco, Sophos has created a road map to integrate encryption with a broader security suite, Patterson says. McAfee also offers integrated management of encryption with other endpoint security functions.

Such integration will help ease deployment of these various security functions, Patterson says. "If we tell users we're going to put another agent on their machine, we have to jump through lots of hoops to ensure performance won't go down," he says. "Adding more functionality into one product set is very attractive as far as selling it to both management and end users."

Stanton Gatewood, CISO at the University System of Georgia, on the other hand, wanted a system that specialized in encryption, which is why he selected PGP. "We looked at others, but when it comes to the nuts and bolts of encryption and asking hard, technical questions, their answers weren't readily available. It seemed as though encryption was an add-on—that they were a firewall or antivirus company that now does encryption."

DO PREPARE A STRONG BUSINESS CASE. Although encryption might seem a no-brainer, many businesses still take a "wait and see" approach, Lambert says. Convincing decision makers to get ahead of a breach by implementing FDE may require making a strong business case. Consider, Girard says, that the cost to mitigate a single compromised data record is comparable to or greater than the seat cost of an encryption tool. Furthermore, he says, the cost to mitigate a large number of breached data records is always larger than the total cost to implement encryption for all mobile platforms in a company.

> The cost to mitigate a large number of breached data records is always larger than the total cost to implement encryption for all mobile platforms in a company.

Not that costs are low. While prices are dropping, Girard says, expect to pay over $100 retail per seat for up to 250 seats for a fully managed and audited encryption product with support for removable media. That drops to less than $100 per seat in the 1,000-seat range and below $70 for 5,000 seats or more, he says.

You can get it for less, Ward says. For the state's deployment, he paid about $11.56 per seat instead of the $76 list price when the reseller offered a 30-day deal of 85% off.

DO CONSIDER SUPPORT FOR REMOVABLE MEDIA. With the prevalence of USB media drives, more attention is being paid to removable media encryption and device control, Lambert says. Generally, the same vendors that offer FDE or FES also offer encryption for removable media, she says, and in some cases, such as Check Point, they also integrate port management, content filtering, centralized auditing and management of USB port storage devices.

Removable media encryption was one of Patterson's evaluation criteria. Utimaco's Data Exchange product encrypts one file at a time rather than the entire USB, he says, which is compatible with the types of data users store, ranging from music to spreadsheets. He set company policy to encrypt anything that users copy over from their PCs, with password-based authentication. This does require thorough training, he says, so that users know how to decrypt and share files among coworkers, so he's phasing it in slowly.

Gatewood says PGP enables the encryption administrators to plug in functionality to encrypt e-mail, files being transferred and removable media, down the road. "We selected a system that will grow," he says.

DO LOOK INTO THE VENDOR'S METHOD OF KEY RECOVERY. Vendors offer varying approaches to key recovery, Maiwald says, for users who forget their password. These range from self-service portals for password reset, to help desk support with a challenge-response mechanism or a one-time password or token that a support tech can provide over the phone. "Look for an approach that nicely meshes with your help desk procedures," he says.

DO CONSIDER ACTIVE DIRECTORY INTEGRATION. Systems that integrate with Active Directory simplify management exponentially, users say. "When a machine is added to the Active Directory domain, we can see it in the console and move encryption keys around," Patterson says. "It's a huge help for key escrow."

Ward says Active Directory integration enabled him to do a one-way pull to populate the McAfee database, saving a great deal of time and providing assurance that the database was structured correctly. "It was important that we not put an additional burden on administrators," he says.

DO LOOK INTO REPORTING CAPABILITY. Ease of reporting is another key selection criteria, Patterson says, to prove laptops are encrypted, especially when one goes missing. Other common reports include whether users had any issues with encryption, whether they called the help desk and whether it was resolved, Gatewood says.

DO CHECK ON WHICH PLATFORMS FDE IS SUPPORTED. There are far fewer Macintosh-based encryption platforms than Windows, Lambert says. Gatewood's choice of PGP was partly due to its cross-platform support of many versions of Windows, as well as Mac OSX.

DON'T OVERLOOK KEY MANAGEMENT. Without strong key management, Gatewood says, you're better off not having encryption at all. This is what enables you to restore, revoke and manage keys in any way. Lack of a strong key management system is one reason he bypassed any of the open-source systems he considered. PGP's Universal Server, on the other hand, allows him to not only manage its own keys, but also keys from other systems, as well. "Some management consoles can be a little kludgey," he says. You should also be able to back up the key escrow database.

DO CONSIDER LOCK-OUT. This feature locks the machine if someone hasn't logged on to the network for a certain period of time, typically several weeks. At Connecticut, Ward says network-connected machines ordinarily check in five or six times a day to send logs to the encryption server. If that doesn't happen within the configured lock-out period, the machine won't allow the user to authenticate, and an administrator will need to unlock the machine.

"It enforces discipline so that you're getting client logs on a continual basis and the machines are constantly updated with new software and any changes in policy," Ward says.

SOFTPHONES REQUIRE STRONG ENDPOINT PROTECTION

VoIP AND DATA COMMUNICATIONS BOTH AT RISK. BY JOHNA TILL JOHNSON, *NETWORK WORLD*

What happens when the phone becomes the computer and vice versa?

At Nemertes Research, we're finding that 70% of organizations are using softphones for voice over IP (VoIP) for at least some (on average, 22%) of their employees. And these are not just toys. Among organizations using softphones, a little more than a third are using softphones in lieu of a desktop phone. Just over half are using them primarily as an adjunct to a desktop phone. And the number one role (44%) for softphone use is mobile workers.

This all points to the need for strong endpoint security and authentication. The good news is strong endpoint protection for mobile workers protects both VoIP and data communications.

Keep in mind that by "softphone" we're not talking about Skype or Google Voice. The softphone is a piece of software that provides desktop phone functionality running on Windows or Mac. Softphones require a common signaling protocol and codec to connect to the corporate VoIP PBX. Today, most softphones use session initiation protocol (SIP) as the signaling protocol. And, when the host device is outside the corporate firewall the connection to the PBX is over the Internet. This is why endpoint protection is so important.

As a baseline the endpoint device needs to have basic security functions operating, include antivirus and antimalware. Essentially, any device connecting to the corporate network—voice or data—needs to meet the basic corporate security protection profile. Given that most softphones are on laptops for mobile workers, that's likely to be the case.

The one area that gets tricky is the personal firewall. Most personal firewalls are configurable to allow or deny VoIP/SIP connections. Obviously, softphones require VoIP/SIP connections, but you'll also want to know that the personal firewall protects against VoIP/SIP vulnerability exploits. The best protection from external exploit via the network is to encrypt the communications.

The other issue that is unique to the mobile worker is the requirement for strong authentication. How do you know it's really Joe connecting to the corporate PBX? When Joe is using the softphone in the office there are other mechanisms—building security, LAN connection, social factors—that authenticate Joe. When Joe is on the road we need multifactor authentication (something you know, something you have and/or something you are) to validate that someone else or something else (malware) is not impersonating Joe.

The good news is a corporate VPN meets both the requirement for encryption and authentication. This guarantees the confidentiality of the softphone communications through encryption and the integrity of the connection via multifactor authentication.

Johna Till Johnson is president and senior founding partner of Nemertes Research, where she sets research direction and works with strategic clients.

See the full selection of InfoWorld IT Strategy Guides at http://www.infoworld.com/reports/y/strategy-guide.

USER COMMENTS CARRY MORE MALWARE THAN INSIGHT

A WEBSENSE REPORT ON SECURITY THREAT TRENDS SHOWS SPAMMERS AT WORK THROUGH USER-GENERATED COMMENTS. **BY ELLEN MESSMER, *NETWORK WORLD***

A staggering 95% of all "user-generated comments" for blogs, chat rooms and message boards online are spam or malicious, according to a new Websense report on security threat trends.

"That's the first time we started monitoring that," says Patrick Runald, Websense senior manager for security research, about the level of spam and malware ploys carried out around blogs and chat rooms.

The Websense Security Labs "State of Internet Security Q1 – Q2 2009," which covers the period up to June of this year, also notes that the number of malicious Web sites for the period more than tripled. In addition, 77% of Web sites with malicious code are said to be legitimate sites that have been compromised.

"The bad guys are finding new ways for disseminating malware," Runald says. "It's getting worse."

According to the Websense Security Labs report, based on data collected in part from scanning 40 million Web sites every hour, 61% of the Top 100 sites are said to either be hosting malicious content or containing a masked redirect to lure unsuspecting victims from legitimate sites to malicious ones.

MALWARE MAGNETS

More than 47% of the Top 100 sites, particularly social-networking sites such as Facebook or YouTube, support user-generated content, which the report notes is becoming a significant way to disseminate malware and conduct fraud.

"On Facebook and other social-networking sites, there's an explicit sense of trust," Runald says. "That's why the bad guys are attempting to exploit it, with malware like Koobface, which could hijack your machine and send messages."

In the area of cybercrime, one significant attack that took place involved criminals seizing control of the CheckFree Web site and attempting to re-direct users to a Web site hosted in Ukraine that tried to install malware on victims' computers. The report said CheckFree has more than 24 million customers and controls 70% to 80% of the online bill-payment market.

FIVE TECHNOLOGIES THAT WILL HELP SOLVE THE DLP PUZZLE

BEFORE EMBARKING ON A DATA LOSS PREVENTION PROGRAM, ENTERPRISES MUST FIRST DETERMINE THE ESSENTIAL TECHNICAL INGREDIENTS. **BY BILL BRENNER, *CSO***

Most security vendors will tell you they have just the thing for your data loss prevention (DLP) needs. But some industry experts say enterprises often buy products that, once installed, don't perform all the functions necessary to keep sensitive information safe. Here are five technological approaches that, when used together, offer a solid data defense.

1. DATA DISCOVERY, CLASSIFICATION AND FINGERPRINTING

Richard Stiennon, chief research analyst at IT-Harvest, says a complete DLP solution must be able to identify your IP and make it possible to detect when it is "leaking."

William Pfeifer, CISSP and IT security consultant at the Enforcement Support Agency in San Diego, agrees, calling data classification the prerequisite for everything that follows. "You cannot protect everything," he says. "Therefore methodology, technology, policy and training is involved in this stage to isolate the asset (or assets) that one is protecting and then making that asset the focus of the protection."

Nick Selby, former research director for enterprise security at The 451 Group and CEO/co-founder of Cambridge Infosec Associates, says the key is to develop a data classification system that has a fighting chance of working. To that end, lumping data into too few or too many buckets is a recipe for failure.

"The magic number tends to be three or four buckets—public, internal use only, classified, and so on," he says.

> The key [to data classification] is to develop a data classification system that has a fighting chance of working. To that end, lumping data into too few or too many buckets is a recipe for failure.

2. ENCRYPTION

This is a tricky one, as some security pros will tell you encryption does not equal DLP. And that's true to a point.

As former Gartner analyst and Securosis founder Rich Mogull puts it, encryption is often sold as a DLP product, but it doesn't do the entire job by itself.

Those polled don't disagree with that statement. But they do believe encryption is a necessary part of DLP. "The only thing [encryption doesn't cover] is taking screen shots and printing them out or smuggling them out on a thumb drive. Not sure I have a solution to that one. It also leaves out stereography, but then is anyone really worried about that?" Pfeifer asks. Specifically, he cites encryption as a DLP staple for protecting data at rest, in use and in motion.

Stiennon says that while all encryption vendors are not DLP vendors, applying encryption is a critical component to DLP. "It could be as simple as enforcing a policy," he says. "When you see spreadsheets as attachments, encrypt them."

3. GATEWAY DETECTION AND BLOCKING

This one would seem obvious, since an IT shop can't prevent data loss without deploying tools that can detect and block malicious activity.

Sean Steele, senior security consultant at InfoLock Technologies, says the key is to have something in place that provides real-time (or close to real-time) monitoring and blocking capabilities for data that's headed outbound at the network perimeter, data at rest ("sensitive or interesting/frightening data sitting on my network file shares, SAN, tier 1/2 storage, etc.," he says); and data being used by human beings at the network's endpoints and servers.

4. E-MAIL INTEGRATION

Since e-mail is an easy target for data thieves, whether they are sending e-mails with links to computer-hijacking malware or sending out e-mails from the inside with proprietary company data, partnerships between security vendors and e-mail gateway providers are an essential piece of the DLP puzzle. Fortunately, Stiennon says, "Most DLP vendors formed partnerships with e-mail gateways early on."

5. DEVICE MANAGEMENT

Given the mobility of workers and their computing devices these days [laptops, smartphones, USB sticks], security tools that help the IT shop control what can and can't be done with mobile devices is a key ingredient of DLP.

Stiennon is particularly concerned about the USB devices that could be used to steal data. "Being able to control the use of USB devices is a key requirement of a DLP solution," he says.

FIVE WAYS EMPLOYEES SPILL SENSITIVE DATA

HERE ARE FIVE WAYS IN WHICH EMPLOYEES MALICIOUSLY OR UNWITTINGLY LOSE SENSITIVE DATA, AND HOW A DATA LOSS PREVENTION PROGRAM WITH THE RIGHT PEOPLE POLICIES CAN MAKE A DIFFERENCE. **BY BILL BRENNER, *CSO***

A company can buy every top-of-the-line security product known to man, but it won't make a difference for data loss prevention (DLP) unless end users are educated on their own role. Technology is indeed critical to DLP, but security experts say user awareness is key to keeping sensitive data safe from online predators.

"DLP is a process first. The technology is simply an enabler for the automation of the process," says Rick Lawhorn, a Richmond, Va.-based chief security officer. "The process needs to include education and awareness training and cover human resources, records management and compliance. The objective is to continuously train data owners and data custodians (the employees) on the company policies to reduce instances of non-compliance."

Based on feedback from several security practitioners, here are five ways in which employees maliciously or unwittingly lose sensitive data, and how a DLP program with the right people policies can make a difference.

1. E-MAIL MAYHEM

IT administrators have had success detecting and blocking malicious e-mail, but users continue to let sensitive data outside the company walls by hitting "send" at inappropriate moments—like when they've just copied and pasted customer information or intellectual property details into a message box. Many times the e-mail is meant for recipients inside the company, but the user might include outside addresses in the message without thinking.

Meanwhile, e-mail filters can't stop every phishing attempt. URLs to malicious sites will still get through, and all it takes is one user to click on it to infect one or more machines with malware that finds and steals data.

This is where the user policies and awareness training can make a difference, Lawhorn and others note. Policies should be clear on the type of content that users can and cannot send out, including such things as customer credit-card numbers, detail on the company's intellectual property and the medical records of fellow employees. Attackers typically latch onto news events like hurricanes or celebrity deaths to concoct bogus headlines that, once clicked, open the door to insidious Web sites designed to drop malware onto the user's machine. An awareness program can reduce the risk by constantly alerting employees to malicious social engineering schemes making the rounds.

2. THE PERILS OF PINGING

Instant messaging programs like AOL Instant Messenger and Trillian have become routine applications in an increasingly mobile workforce. Employees often rely on these programs to communicate remotely with their bosses and department mates. Along the way, attackers have found ways to send malicious links and attachments to users by creating imposter accounts that look like legitimate messages from colleagues. Adding insult to injury is that many IM applications can be downloaded for free and, once installed, are pretty much beyond the control of enterprise IT shops. Like the e-mail problem, this is a case where user awareness training and policies are critical. Policies should be clear about information that can and can't be sent by IM.

3. SOCIAL NETWORKING ABUSE

While IT shops continue to struggle with the insecurities of e-mail and IM, attackers are increasingly setting their sights on such social networking sites as LinkedIn, Myspace, Facebook and Twitter.

It turns out the bad guys can use these sites to do all the nasty things they learned to do by e-mail and IM.

Facebook in particular is notorious as a place where inboxes are stuffed with everything from drink requests to cause requests. For some social networkers, clicking on such requests is as natural as breathing. Unfortunately, the bad guys know this and will send you links that appear to be from legitimate friends. Open the link and you're inviting a piece of malware to infect your machine. Christophe Veltsos, president of Prudent Security, describes this as being "click-happy" and warns, "Don't click unless you're ready to deal with drive-by downloads and zero-day attacks."

User awareness programs must address the myriad tricks attackers can employ on these sites, whether it's a bogus group invite on LinkedIn or a photo on Myspace that hides malware that's unleashed when the user runs the curser over the image.

4. PASSING UP SECURE PASSWORDS

This is another old problem that attackers continue to exploit with plenty of success. Users have a growing pile of passwords they need to keep for access to everything from the work e-mail application to their social networking accounts and banking sites. Since memories are short and people tend to forget the password to a program they might only use once a month, the typical tactic is to use the same password for everything.

"Using the same password on several sites is like trusting the weakest link in a chain to carry the same weight. Every site has vulnerabilities, plan for them to be exploited," says Daniel Philpott, information security engineer at OnPoint Consulting Inc.

Lawhorn cites this as an example of something an employee user policy should address. A good policy would require employees to use a different password for each work-related account with upper and lowercase letters and numbers, for example.

5. HAVING TOO MUCH ACCESS

Another common problem is that employees are often given access to more enterprise applications than they need to do their jobs. All it takes is one disgruntled employee with too much access to go in and steal enough sensitive data to put the company in serious jeopardy.

The best defense here, security experts say, is to allow employees access only to applications and databases they need to do their jobs.

ENDPOINT SECURITY SHOOTOUT

FIVE PRODUCTS COMPETE TO PROTECT CLIENT SYSTEMS. BY KEITH SCHULTZ, *INFOWORLD*

Every computer that connects to the Internet must have some form of anti-virus protection installed. The number and type of virus threats increase every year, with new ones appearing at an alarming rate. However, threats to the desktop are not limited to simple viruses, but often come as a coordinated attack via drive-by installation of malware and spyware. Further, not all threats are from the Internet: Unprotected vendor laptops can inject malicious programs directly into the enterprise, or malicious employees can siphon secrets to USB thumb drives. Security applications must be able to protect the desktop from both internal and external threats.

Because securing the client device–the endpoint, if you will–is so important, I decided to put five of the top enterprise endpoint security packages to the test. They include: Check Point Endpoint Security - Secure Access Edition; McAfee Total Protection for Endpoint 4.0; Sophos Endpoint Security and Control; Symantec Endpoint Protection 11; and Trend Micro OfficeScan Client/Server Edition 8.0.

All five products worked well in my test lab, performing their anti-virus and anti-spyware security duties flawlessly. However, there were other factors to consider in evaluating these products beyond the effectiveness of their virus and malware protection, as well as their other security services. I looked at how easy they are to administer, how straightforward it is to update and manage clients, and how well the systems report back the security health of the enterprise. I also considered OS support; some of the products support an array of platforms, whereas others are Windows-only.

CHECK POINT ENDPOINT SECURITY – SECURE ACCESS EDITION

Endpoint Security - Secure Access Edition from Check Point is a good all-around package of client-security services for Windows users. The package includes anti-virus, anti-spyware, a desktop firewall, NAC, program control, and a VPN client bundled in a single agent. The browser-based management console is less cumbersome than McAfee Total Protection's, but it's also not as intuitive as that of Trend Micro OfficeScan. Check Point's reporting engine is very utilitarian but provides all of the information IT needs to keep up with the network's security status without information overload.

I installed Endpoint Security on a virtualized Windows Server 2003 server and had no trouble loading the associated applications. Endpoint Security's management platform runs on a Windows Server 2003 or Check Point SecurePlatform (Check Point's version of Linux). Unlike offerings from McAfee and Sophos, the Endpoint Security client supports only Windows 2000 Pro (SP4), Windows XP Pro (SP2), and Vista Enterprise.

Once up and running, the Endpoint Security management platform consumed more than 350MB of RAM (mostly in use by the included Web engine, Tomcat) but had minimal CPU impact on the server. The client claimed about 102MB of RAM, both at idle and during a manual scan, with a rise in CPU usage from about 0 percent to approximately 55 percent. As expected, Endpoint Security detected, caught, and handled all threats without fail.

Check Point's protection engine is based on anti-virus and anti-spyware technology licensed from Kaspersky Labs in addition to Check

See the full selection of InfoWorld IT Strategy Guides at http://www.infoworld.com/reports/y/strategy-guide.

Point's own anti-spyware technology. This two-pronged approach uses both signatures and heuristics to detect potential threats before they land on the system.

Unlike with all of the other reviewed products in this roundup, admins must either install the Endpoint Security client via traditional software-distribution methods or from a shared location; there is no push support in the Endpoint Security Dashboard. For organizations already running a Check Point firewall, the vendor offers an interesting method for installing the client on captive portal users' systems: Admins can force users to install the client in order to gain access to the Internet.

I like the level of control offered by Check Point's policy editor. Each policy falls into either a trusted zone (that is, a local network) or an untrusted zone (the Internet and all other networks) and provides different levels of access for each. The client firewall comes with a decent set of predefined rules, and it's easy to customize inbound and outbound rules to meet your needs. The application control gives IT broad yet easily manageable control over programs. Each policy includes "enforcement settings," Check Point-speak for NAC, which worked well in my test scenarios.

All five products worked well in my test lab, performing their anti-virus and anti-spyware security duties flawlessly. However, there were other factors to consider ...

The application permissions engine provides an easy-to-manage system for allowing or denying program execution on both clients and servers. This whitelisting service allows admins to create logical groups of applications, such as browsers and mail clients, and to determine whether each program is permitted to run. I could restrict which browsers my test clients could run by simply adding the specific executable to the Browsers group, then denying access. I find this to be very powerful yet easy to use.

At first glance, Check Point's reporting engine seems a bit sparse, as if reports and charts are missing. But upon further inspection, when compared to Symantec Endpoint Protection's information overload, Check Point's almost simplistic reporting engine is a nice change of pace. Three major groups of reports–endpoint monitor, endpoint activity, and infection history–break out nicely, allowing a quick and uncluttered view into each endpoint's status. Unfortunately, infection history detail goes back only 14 days.

Check Point's Endpoint Security - Secure Access Edition is a good mix of endpoint protection and flexibility. I like the granular control available in each policy definition, and the concept of trusted and untrusted zones doubles the security footprint. Unfortunately, client OS support is limited to Windows systems, and there is no push installation support in the product.

MCAFEE TOTAL PROTECTION FOR ENDPOINT 4.0

McAfee Total Protection for Endpoint bundles anti-virus, anti-spyware, host intrusion prevention, and network access control. All of these systems are tied together with the management console, ePolicy Orchestrator (ePO) 4.0, which is a welcome upgrade from previous versions, featuring a completely retooled reporting engine that allows admins to create many different custom reports. Total Protection is not Windows-centric and provides protection for other popular operating systems.

When I first received Total Protection for Endpoint, I had a pre-release installation package that required following a convoluted script that would make Cecil B. DeMille proud. Fortunately, the shipping install package was a single setup program that does all the heavy lifting for admins. Other than specifying the database engine to use (it included MSDE), installation was relatively straightforward. Upon the setup's completion, my system was up and running, ready for me to check in the various packages and download all available updates.

I really like the breadth of OS support found in Total Protection. From ePO, you can deploy and manage policies on all 32-bit Windows platforms (including NT 4.0 with SP6a) and 64-bit Windows systems, as well as Novell NetWare, Linux, Mac OS X, Citrix MetaFrame 1.8, and XP Tablet PCs. As with the Sophos and Symantec products, I found that being able to manage a heterogeneous enterprise from a single console was a big plus.

Total Protection provides a couple of methods for deploying the ePO agent to unprotected desktops. Unlike with Check Point Endpoint Security, I can push the agent out to my test systems from ePolicy Orchestrator by selecting systems in the Lost & Found group and clicking the Deploy Agent button. ePO also synchronizes with Microsoft Active Directory, automatically adding any new systems added to AD. ePO constantly monitors the local network for unknown systems, making it easy to identify and update unprotected machines.

Assigning and defining security policies in ePO aren't nearly as intuitive as in other packages. Although ePO provides access to groups, users, systems, policies, and more, it suffers from a bit of drop-down box overload. It's difficult to see at a glance how policies are assigned and which ones are enabled on a per-client and per-group basis.

McAfee Total Protection for Endpoint comes pretty close to being exactly what its name says: absolute protection for clients. VirusScan Enterprise and McAfee Anti-Spyware deliver two flavors of scans, providing excellent real-time, on-demand protection from viruses and other potentially unwanted programs using a mix of signatures and heuristics. Total Protection didn't have any trouble identifying and trapping threats, whether from a questionable Web site or an infected file.

Total Protection uses a single scanning engine, allowing for a slightly smaller (80MB of RAM) footprint while in use. An on-demand scan consumed about 100MB of RAM and averaged 37 percent CPU usage with peaks to 100 percent.

Helping to lock down the desktop, Host Intrusion Prevention (HIP) provides application blocking, a client firewall, and general IPS rules such as buffer overflow and known application exploits. As with Trend Micro's Intrusion Defense Firewall, IT can create various rules with Total Protection as to what type of traffic is allowed or denied, both to and from a client. The application-blocking support is good, but it does not provide the same granular level of configuration found in Check Point's offering. Admins are limited to basic Allow and Block selections for each defined application.

The reporting module is where McAfee Total Protection shines. With this release of ePO, the reporting and dashboard services receive a major retooling, allowing admins to create custom reports and attach them to a dashboard for easy monitoring. In fact, ePO allows admins to create multiple dashboards for grouping related reports. The number of predefined reports is staggering, and I really like that I could quickly and easily create new exports in a variety of formats.

Total Protection is a solid, well-rounded endpoint security package that fires on all cylinders. I like the enhanced reporting capabilities in ePO, and the single-engine virus and malware scanner works very well. Moreover, the expanded platform support fits in nicely with most large organizations. My biggest complaint is that it's hard to easily see my policies and how they're assigned to each group or individual client.

SOPHOS ENDPOINT SECURITY AND CONTROL

Sophos Endpoint Security and Control offers a tight mix of virus and spyware protection, along with client firewall, application control, host intrusion protection, and network access control. Furthermore, its intuitive browser-based management platform works well.

I had no trouble installing Sophos' Enterprise Console on my Windows Server 2003 virtual test bed. Like Trend Micro's OfficeScan, server resources were pleasingly light, requiring only about 100MB of RAM when logged into the console using Internet Explorer. During installation, I chose to have Sophos install MSDE on my server. Alternatively, admins can elect to use an existing Microsoft SQL server.

Deploying the Sophos client to users' PCs is a push process from the Enterprise Console. The Find New Computers wizard lets admins choose between importing a list of computers from Active Directory or performing a network scan based on network (NetBIOS name) or IP address range. I used the Active Directory method and had no problems installing the full client to my test machines.

Endpoint Security provides protection for not only Windows machines, but also Mac, Linux, Unix, NetWare, and OpenVMS systems. The list of supported platforms is extensive and includes both 32- and 64-bit platforms. Best of all, admins can manage and monitor all flavors of clients from a single Sophos Enterprise Console. Like Trend Micro's and Symantec's respective products, Sophos includes virtual environments as part of the supported package.

One feature that busy admins will appreciate is Sophos' ability to uninstall any third-party anti-virus programs already present on users' PC. One of my target systems came with another vendor's endpoint client package, and Sophos cleanly removed it prior to installing the new package.

Endpoint Security and Control is exactly what its name suggests: a full suite of security services blended together to allow administrators to tailor both inbound and outbound security. The real-time anti-virus and anti-spyware detectors share the same engine and the same virus/malware definitions. Endpoint Security generates an MD5 hash of each scanned file. If, on subsequent scans, the hash is unchanged, then Sophos skips scanning the file, saving CPU cycles.

Complementing the signature-based detection is what Sophos calls Behavioral Genotyping. This behavioral engine checks potentially malicious traffic against existing definitions in order to help stop new or unknown attacks. As long as the attack is a variant of an existing virus—and most viruses are—Sophos will detect it and block it. Each threat I threw at Endpoint Security was caught and handled according to my security policy. No surprises here.

Sophos' Application Control allows admins to create whitelists of approved programs: You can block specific applications or entire groups, such as remote-management tools. Beyond application control, Sophos also helps cut down on data leakage by blocking users' access to local storage devices, wireless connections such as Wi-Fi and infrared, instant messaging, and file-sharing applications.

Network access control is managed through a separate browser-based user interface accessible from the Enterprise Console. The predefined policies and profiles make quick work of getting a NAC system up and running, and the wide range of configuration options means admins can create a system to meet just about any situation.

The Enterprise Console is where admins will spend most of their time, and unlike with McAfee's ePO, it is time well spent. The console is well laid out and easy to navigate, with the graphical dashboard providing at-a-glance status reports of the network. The reporting engine is good if not overly flashy. I like that I can click on a detected item name in the Alerts report and find out additional information about the threat.

I was really impressed with Sophos Enterprise Security and Control. The administrative console provides an overview into the health of the enterprise, and the policy quick links make accessing specific policy items fast and easy. I like that I can manage my heterogeneous enterprise from one console, and the level of protection is top notch.

> The Sophos Enterprise Console is where admins will spend most of their time, and unlike with McAfee's ePO, it is time well spent. The console is well laid out and easy to navigate, with the graphical dashboard providing at-a-glance status reports of the network.

SYMANTEC ENDPOINT PROTECTION 11

One of the best-known vendors of anti-virus software, Symantec scores with its latest offering, Symantec Endpoint Protection (SEP) 11. A bundled mix of anti-virus, anti-spyware, firewall, intrusion prevention, and application and device control, SEP provides a well-rounded suite of protection for both clients and servers. The centralized management console, Endpoint Protection Manager, does a good job of providing a one-stop management tool for admins, and the reporting engine issues a wealth of information, but only if you know how to look for it.

Installation of SEP on my test Windows 2003 Server went off without a hitch. Make sure your host server has plenty of resources: Between SEP's database engine and other core services, it consumed more than 300MB of RAM. Also, Endpoint Protection is the only product in this roundup that has a Java-based management console, and it suffers from mild Java lag. On the client side, RAM demand is light, with only about 10MB in use at idle and less than 55MB and 28 percent CPU utilization during a full system scan.

SEP comes with a nifty deployment wizard that walks admins through the process of pushing out the agent to unprotected clients. If your organization has a standard software-distribution system in place, you can simply distribute a single executable install package to unprotected systems or allow individuals to launch the install from a shared folder. SEP can also talk to Active Directory to import organizational groups for better client management.

Like McAfee's and Sophos' offerings, SEP will protect not only 32- and 64-bit Windows systems, but also 32- and 64-bit Linux, Novell Open Enterprise Server, and VMware ESX. Unlike Sophos, SEP does not currently support Mac.

The heart of SEP is the anti-virus and anti-spyware detection engine. SEP employs a single-protection technology composed of multiple scan engines to detect and scan for viruses and malware. As files are copied or created, SEP intercepts them and passes them to the appropriate scan engine.

Much like Sophos' Behavioral Genotyping, Symantec's TruScan Proactive Threat component protects the client from unknown and zero-day threats by monitoring the behavior of programs to determine their intent. TruScan detects and logs discovered instances of potential unwanted programs for admins to review. TruScan can also detect commercial keyloggers and remote-control applications, and admins can log, ignore, terminate, or quarantine these programs.

The firewall engine built into SEP is first rate and provides a very fine level of control over protocols, ports, and applications. The default firewall rule set is very detailed, providing a secure out-of-the-box configuration. A handy firewall rule wizard helps admins create any additional custom rules as necessary. The intrusion-prevention engine complements the client firewall, but other than a couple of check boxes, it doesn't allow for any real customization.

Application control in SEP is not nearly as intuitive as that of Check Point Endpoint Security. The rule builder is very extensive, allowing the agent to check for many different conditions, such as Registry access, launch process attempt, and terminate process attempt. The application control rule builder would benefit from an interview-based wizard to walk admins through the rule-creation process. The current rule engine is powerful, but it's not very intuitive, making it cumbersome to use. Admins who take the time to learn the application-control rules engine will find it more than capable of locking down not only applications but the behavior of devices, such as USB drives.

SEP's reporting engine could also welcome a user-friendliness makeover. There is a wealth of information available to the admin, but because the report engine generates so much information, finding what you're looking for can be difficult. In a future version, I would like to see interactive reports. For example, I was able to create a chart of attacked PCs, but all that was reported was the group and number of attacks. I'd like to be able to drill down into the chart to see which systems were attacked for further analysis.

Overall, SEP is a good all-around security package. Its only real weakness is its reporting engine. The anti-virus/anti-spyware protection is solid, and I like that wider range of operating systems supported. The client firewall is one of the best going, but the application protection is a bit of a management chore.

TREND MICRO OFFICESCAN CLIENT/SERVER EDITION 8.0

Trend Micro's OfficeScan Client/Server Edition 8.0 bundles all of the required protection services into a platform that's easy to install and deploy. OfficeScan includes anti-virus and anti-spyware protection, firewall, intrusion prevention and detection, Web-threat security, and integration with Cisco Network Access and Control 2.0. Admins centrally manage OfficeScan via their browser, and the product is capable of overseeing multiple domains.

Installing OfficeScan took about 45 minutes on my virtual test bed. Server resources were light, requiring less than 100MB of RAM with the management console open (including Internet Explorer usage). The console was easy to handle and fairly intuitive to navigate, unlike McAfee's ePolicy Orchestrator. Admins can install the client engine either through a Web link to the OfficeScan server or via push from the management user interface.

The OfficeScan client will run on any version of Windows from 2000 to 2008, including 64-bit Vista. The OfficeScan Server requires Windows Server 2000 through Server 2003. Virtualized environments such as those from Microsoft, Citrix, and VMware are also supported. Unlike the products from McAfee, Sophos, and Symantec, Trend Micro's offering does not support non-Windows platforms.

The heart of any anti-virus system is its real-time protection. OfficeScan uses separate engines to inspect traffic for virus and spyware activity. Both engines use signature matching to detect the digital nasties, and unlike Symantec's and Sophos' respective products, OfficeScan does not have a behavioral detection engine for spotting zero-day attacks. A behavioral detection engine is in the works and should be available in the next major release.

During my tests, OfficeScan detected and blocked all of the viruses I threw at it, and it had little trouble picking out malware from a malicious overseas Web site. It processed the threats based on the policy in place, cleaning, quarantining, or deleting as prescribed. The real-time protection worked well in all my tests, and resource usage was very low: about 50 percent CPU usage and 55MB of RAM during an active scan.

The client firewall included in OfficeScan is solid if not flashy. Defining firewall settings entails defining a security policy, then assigning the policy to a user profile. The security policy dictates how the firewall will function, blocking all inbound and outbound traffic, blocking all inbound traffic, or allowing all traffic. Admins can add exceptions to each policy, for example, to allow remote connection to the desktop while denying all other inbound traffic. You can also define exceptions based on protocol, port, and IP address.

A step above the built-in OfficeScan client firewall is the Intrusion Defense Firewall (IDF) plug-in, available as a separate license from Trend Micro. IDF performs deep-packet inspection on all incoming and outgoing traffic and helps eliminate illegitimate network traffic. It is a full-featured stateful packet inspection engine that doesn't require additional RAM or add any noticeable latency on the network.

OfficeScan is the only package in this roundup that includes built-in support for Cisco NAC policies and agents. For those companies already deploying Cisco NAC, OfficeScan can directly integrate with your existing policy servers, providing network access control through the included Cisco Trust Agent.

The reporting engine is a weak area in OfficeScan, numbering a summary page in the management interface. To be fair, graphical representations of outbreaks and client connections are easy to read, as is the Update Status section showing signature and application versions. Unlike with McAfee ePolicy Orchestrator, admins cannot create customized reports or charts with OfficeScan.

Trend Micro's OfficeScan is a good all-around package for securing Windows-based clients. The management console suffers from some organizational problems, but access to all systems and policy objects is only a click or two away. Reporting is limited, but the tight integration with Cisco NAC is a definite plus.

CLOSING THOUGHTS

I went into this review without any preconceived notions as to which product would fare the best, and I was pleasantly surprised to see that Sophos Endpoint Security and Control just edged out Symantec Endpoint Protection for top honors. The Sophos solution provides excellent client platform support and includes the core services to keep endpoints secure. At the same time, it's easy to use and administer. Its well-rounded reporting engine is key in garnering the top score in this roundup.

INFOWORLD TEST CENTER SCORECARD

	Threat defense	Features	Management	Reporting	Platform support	Value	Overall score
Percent of total score	25%	20%	20%	15%	10%	10%	
Check Point Endpoint Security – Security Access Edition	9	8	8	7	6	7	7.8 GOOD
McAfee Total Protection for Endpoint	9	8	7	9	9	8	8.3 VERY GOOD
Sophos Endpoint Security and Control	9	8	9	8	9	9	8.7 VERY GOOD
Symantec Endpoint Protection 11	9	8	8	7	9	9	8.3 VERY GOOD
Trend Micro OfficeScan Client/Server Edition 8.0	9	7	8	7	6	7	7.6 GOOD

See the full selection of InfoWorld IT Strategy Guides at http://www.infoworld.com/reports/y/strategy-guide.