

NetworkWorld Reprint

The leader in network knowledge ■ www.nwfusion.com

September 20, 2004 ■ Volume 21, Number 38

End point security products aid in client defense

■ BY MANDY ANDRESS AND RODNEY THAYER, NETWORK WORLD LAB ALLIANCE

Regardless of the computing device in hand, or network connection at hand, end users need access. But from a security perspective, the price of this flexibility is an ever-growing, distributed perimeter that you can't always control.

Enterprise endpoint security safeguards can help rein in your distributed client security concerns. But that market encompasses an array of products, ranging from software that only will execute allowed applications to products that monitor application or network activity for malicious or abnormal behavior.

In this round of testing, we focused on products that take some type of action in the face of an attack, such as blocking a port or stopping an executable. Products that focus solely on endpoint policy enforcement, such as warning that anti-virus definitions are out-of-date, are not included, nor are products that specifically address mobile devices such as handheld models. However, both of these classes of products will be covered in future tests.

Nine vendors submitted products for this test. They include eEye Digital Security's Blink 1.0; Finjan Software's Vital Security for Clients; F-Secure's Anti-Virus Client Security; InfoExpress' CyberArmor 3.0; SecureWave's Sanctuary 2.8; Sygate Technologies' Secure Enterprise 4.0; Symantec's Client Security 2.0, WholeSecurity's Confidence Online 4.0.3; and Zone Labs' — which is now a Check Point company — Integrity 5.0.

Cisco, McAfee and StillSecure offer products that fit the criteria of our test, but declined to participate.

Each vendor takes a different approach to end-point security. Some — F-Secure and Symantec — combine anti-virus with firewall technologies. Others — eEye, InfoExpress, Sygate and Check Point — try to combine intrusion prevention, "classic" firewall rules and application protection into the mix. Still others — Finjan, SecureWave and WholeSecurity — focus strictly on regulating applications running on the system. For the sake of a fair comparison, we pulled these last three products out into a separate test category.

eEye's Blink wins our Clear Choice designation because of its solid reporting and hybrid approach to client defense. F-Secure, Check Point and Sygate also make the short list of contenders because they registered strong performances across test categories.

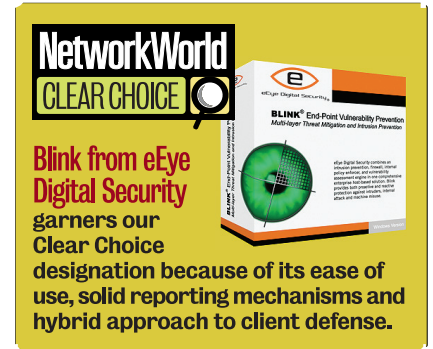
To test the products, we approached them from two directions. First, we installed the products in our lab to define policy, deploy clients, and view reports. We then set up a scenario in which an attacker would attempt to compromise the client system being defended. We developed an attack plan and executed attacks against each product so we could evaluate how well their defenses worked.

From the top

Because setting up and deploying software that touches every client on your corporate network is no trivial matter, we assessed how each vendor handled this daunting process.

Sygate and eEye provided on-site installs of the management server/console and several clients because it is included in standard purchases. We then re-performed their work to make sure there were no hidden "gotchas" in the process.

For Check Point, we ran the installer, followed the instructions and were up and running in just a few minutes. Client deployments



are available through a download link, but they also can be pushed out via any other deployment mechanism used in the company, such as Microsoft's Group Policy setting or System Management Server.

We ran into one problem during the F-Secure console installation. The company did not provide all the software necessary for us to follow its install instructions, so we had to place a service call.

For Symantec, we followed the installation instructions but found various components not always showing up in the console, and the client firewall was not being deployed when we pushed software to clients. We ended up re-installing all Symantec server components from scratch, which resolved some issues, but the Alert Management System did not always show up in the console as expected.

For the firewall client component, we spoke with Symantec support and found that this is not installed by default. We needed to create a custom installation path. Because we were testing Symantec Client Security, we would like to see the firewall component installed by default, not just the anti-virus software.

With InfoExpress, we did not have complete, or even accurate, installation instructions. The documentation refers to out-of-date product components' names. We did not receive a license key and did not know we needed one until we attempted to log on to the console and were asked to enter one. Despite rebooting the system, there was a period of days that we could not access the administrator account, until it inexplicably began to work. Once we logged on, we could create new users, but could not create new accounts using the installation account name. We also had issues creating client software deployment packages. The documented instructions were not clear or detailed. It was only through a support call that we found we needed to state a URL path for a region before a deployment package could be created.

Net Results	Overall Rating	Overall Rating	Overall Rating	Overall Rating	Overall Rating	Overall Rating	
Blink 1.0 Company: eEye Digital Security, www.eeye.com, (866) 338-3732. Cost: Starts at \$30 per node. Pros: IPS notifications were useful; excellent reporting capabilities; built-in client deployment. Cons: Connecting to remote hosts for log viewing was non-intuitive.	4.13	Anti-Virus Client Security Company: F-Secure, www.fsecure.com, (408) 938-6700. Cost: Starts at \$32 per client. Pros: Strong reporting engine; built-in client deployment that is easy to use; single product can provide anti-virus and firewall. Cons: No anomaly detection; hard to get management logging working.	3.5	Integrity 5.0 Company: Zone Labs, a Check Point company www.zonelabs.com, (415) 633-4500. Cost: Starts at \$65 per end user. Pros: Intuitive GUI; resilient client. Cons: No anomaly detection; does not include a complete reporting engine.	3.5	Secure Enterprise 4.0 Company: Sygate Technologies, www.sygate.com, (510) 741-2600. Cost: Starts at \$20 to \$70 per seat. Pros: Combines network and application policy rules well; can create graphs from the GUI to analyze log data. Cons: No anomaly detection; no full report generation functionality.	3.38
		Client Security 2.0 Company: Symantec, www.symantec.com, (408) 517-8000. Cost: Starts at \$43.40 per user. Pros: Single product provides anti-virus and firewall. Cons: Spoofing possible because of logs being stored on the client; no anomaly detection; separate components not well integrated.	2.5	CyberArmor 3.0 Company: InfoExpress, www.infoexpress.com, (650) 623-0260. Cost: Starts at \$55 per seat. Pros: Strong policy development engine. Cons: Firewalling component reports many sockets as closed, which suggest a less-sophisticated firewalling algorithm; inadequate documentation; poor GUI.	2.0		
The breakdown	eEye	F-Secure	Zone Labs/Check Point	Sygate	Symantec	InfoExpress	
Policy management 25%	3.5	3	3.5	3	2.5	3	
Setup, deployment and documentation 25%	4.5	4.5	4.5	4.5	2.5	2	
Reporting capabilities 25%	5	5	2.5	3	1.5	1	
Attack defense capabilities 25%	3.5	1.5	3.5	3	3.5	2	
TOTAL SCORE	4.13	3.5	3.5	3.38	2.5	2	

Scoring Key: 5: Exceptional; 4: Very good; 3: Average; 2: Below average; 1: Consistently subpar

Check Point provided the best documentation that was clearly written, detailed, accurate and easy to understand. F-Secure and Sygate provide adequate documentation. Symantec provides a lot of documentation, including a lengthy installation guide, but we feel the installation guide needs to be revamped so users can avoid the installation hassles we encountered. As mentioned, InfoExpress documentation needs drastic improvement. It was difficult to perform any task because the product is not easy to use, and the documentation did not explain how things worked. eEye did not provide any documentation, but its product was intuitive and easy to use. We did not find ourselves looking for much documentation, and when we did, the online help was useful.

Policy configuration and deployment

From our perspective, the most important component of these products is policy configuration, which is where you define how this product will protect your endpoint devices. With a poorly defined policy, you easily can prohibit valid communications or applications required to perform day-to-day business tasks or let malicious traffic/applications access your systems.

The tested products take completely different approaches to securing clients.

Some products only look at applications that receive or generate network traffic; others watch application behavior for signs of malicious activity. Still more take a hybrid approach and combine technologies including network-based firewall rules, application control mechanisms, protocol analysis and intrusion-detection signatures.

To test policy functionality, we attempted to create and deploy a policy that would block all inbound traffic except remote desktop, block outbound traffic to Port 23 on remote systems, block Netcat from binding to Port 468, and block Solitaire (sol.exe) from running. Once the policy should have been deployed, we tested remote desktop connectivity, telnet connections and our ability to play Solitaire. By trying to control these four processes, we can gain a good understanding of the parameters around which you can use these products to set policy across a broader set of application and network activities.

The most interesting policy definition test was prohibiting sol.exe execution. For Symantec and eEye, you can specify files to trust or deny, but you need to specify the file path. This is a challenge because sol.exe resides in WINNT\system32 in Windows 2000 Server, which is where the management console resides for each product, and Windows\system32 on Windows XP, which is what the system that should be enforcing the policy is running. We could not test the policy for execution blocking on these products because neither would let us manually enter the path to the file. We needed to browse to the file, which was not feasible because the file we would need to browse to does not exist on the management server.

Check Point, Sygate and F-Secure only appear to look at applications that attempt to access the network because Solitaire never showed up in the applications list each product generates for applications that run on the system. On the other hand, telnet shows up immediately after execution.

To block outbound telnet connections, Symantec, Check Point, InfoExpress, Sygate and eEye all were successful at blocking Port 23 outbound. Configuring

an outbound rule to block Port 23 on F-Secure did not work, but prohibiting telnet.exe from executing did work as expected.

We then configured each policy to allow inbound Port 3389 for Microsoft's Remote Desktop Connection Utility. eEye, F-Secure, InfoExpress, Sygate and Check Point successfully allowed the remote connection. We could not get inbound Remote Desktop to work on the Symantec client, even though the policy was configured to do so.

Overall, policy generation was challenging across products when determining how a specific product can implement a specific policy. Network-based policies were easier to implement than application-based policies.

We ran into a few issues with several products. When we created System Rules in eEye, we attempted to increase the rule priority, but this functionality failed periodically with a SQL server error. We reported this to eEye, but have not been able to reproduce it since then. We also often received a "Server Busy" error on the system running the Blink client.

The Symantec Client Firewall Administrator used to create the Symantec policy was difficult to use and locked up on several occasions.

The InfoExpress policy-creation process is the least-intuitive implementation we have seen. After spending twice as much time on policy creation as we did on any other product, we still had difficulty generating three simple policy rules. A support call provided some assistance, but policy creation shouldn't be this difficult.

Attacking the clients

Our attack testing against each client was designed to exercise the defenses we expected to find.

We tested application control (also referred to as execution containment) features by running an application that accessed the network in a way prohibited by policy. We tested intrusion detection by performing a port scan. We tested intrusion prevention (which is implemented as anomaly detection, if at all) by running a Universal Plug and Play Protocol (UPNP) attack. We tested defense resilience by performing a "coarse uninstall" of the product. We defined a coarse uninstall as the deletion of files from the product's program files folder. We deleted all the files we could, as an attacker would.

eEye performed application control, detected our network intrusion and detected the specific network attack. We did, however, coarsely deinstall the product, as an attacker might, and disabled the defenses.

F-Secure, InfoExpress, Sygate and Symantec all handled execution containment and detected the network intrusion, but did not detect the specific attack. The Symantec client did not report the UPNP ports as open, so we did not execute that attack.

We coarsely uninstalled F-Secure, Info Express and Sygate. We couldn't uninstall Symantec or Check Point. When we restarted the F-Secure client, it only caused a mildly worded dialog box to appear, and dismissing that still allowed the client to run. A typical end user probably would just dismiss the warning and continue to use the machine. The InfoExpress client machine simply restarted with no errors, and we executed the previously blocked application. The Sygate client also simply restarted with no notification. Symantec also had a warning, but it was a large notice with a bright yellow border and would be very difficult to misinterpret as a benign message.

An attacker who is targeting a company would

expect the client systems to be communicating with some sort of security infrastructure and try to avoid detection by that. We wanted to test how well the clients reported attacks to the server, but all the products tested had limitations in their reporting. For example, no product detected client reboot events, which an attacker might cause.

Reporting

We defined reporting as the ability to see alerts and trends regarding all clients from a central location.

Out of the box, eEye's Blink provides the ability to directly view the logs on the remote client if the machine is online. Central reporting requires installation of the REMstet Security Management Console reporting system, which is included with Blink but runs separately. Events are sent to the REM database where numerous queries and reports can be generated, including reports on attack trends and client status. Reports also can be printed to PDF.

F-Secure provides an excellent Web-based reporting module for generating graphs on a number of data points, including virus infections, general alerts, system status and attack details. Reports can be exported to a variety of formats including CSV, HTML and XML.

Sygate provides some log viewers and a mechanism for generating graphs from the logs in the database. It also includes the ability to view statistics on client status by group or individual system, which lets you see which clients have not reported in for a while that may require investigation. We would like to see reports generated for this information.

Check Point includes a reporting section, but it generally is just providing query results from the logs. We would like to be able to create graphs and summary reports, and export to PDF or another format. Print views are available in HTML, but they only show the query results displayed onscreen, not all of the results. We also would like to see options for custom reports and the ability to generate reports from the client status monitor information.

Symantec does not include any reporting functionality. If the client is online, you can remotely view the local client logs. InfoExpress includes a Web reporting console, but it needs to provide more information and options. The reports generated are minimal and did not provide a way to export them.

Conclusions

From an attacker's perspective, a client endpoint system is a viable path of attack into a company. Therefore, the ability to defend these systems and the ability to centrally manage and monitor their defenses are important components of any network defense strategy.

While these products offer significant defensive capabilities, depending on which defenses are important in a network, the state of the art is not at the level where it offers a sufficient level of resilience against the state of the state of the attackers. Improvements in reporting and management, improvements in containment techniques and improvements in the types of attacks the products detect are needed.

Andress is president of ArcSec Technologies, a security company focusing on product reviews and analysis. She can be reached at mandy@arcsec.com. Thayer is an independent security consultant. He can be reached at rodney@canola-jones.com.