How Cisco IT Upgraded Intrusion Prevention Software to Improve Endpoint Security

Cisco Security Agent Version 4.5 thwarts malicious behavior while reducing costs associated with virus and worm remediation.

Cisco IT Case Study / Security and VPN / Endpoint Intrusion Prevention Upgrade: This case study describes Cisco IT's internal deployment of Cisco Security Agent Version 4.5 to Windows desktop systems across Cisco's global network, a leading-edge enterprise environment that is one of the largest and most complex in the world. Customers can draw on Cisco IT's real-world experience to help support similar enterprise needs.

"Security is no longer a 'network-only' proposition. Data must also be protected where it resides–the endpoint."

– Paul Mauvais, Senior Security Architect, Cisco Systems

BACKGROUND

The steep cost of viruses and worms, which includes both remediation and loss of productivity, is a powerful incentive for prevention. Cisco Systems® uses a multipronged approach to protect its network from various types of attacks, including use of Cisco® PIX® security appliances, network-based intrusion detection systems (IDSs), and antivirus software residing on desktops and e-mail gateways. None of these methods alone, however, is completely effective for protecting individual assets like PCs and handheld devices at the desktop level. Consider that firewalls protecting the Cisco network cannot prevent a sales engineer's laptop from becoming infected when plugged into a partner's or a customer's network. Nor can they prevent the spread of infection when a Cisco employee's laptop becomes infected at home and then is reconnected to the corporate intranet. Antivirus software also has limitations for protecting individual PCs and servers. Although antivirus software is effective in warding off viruses with known signatures, it does not protect the desktop between the time the virus is introduced and when a new virus definitions file with the new signature is installed—by which time the harm is done.

The same problem applies to patches that vendors release for newly discovered operating system and application vulnerabilities. Patching also poses logistical problems for the mobile and global Cisco workforce. Cisco employees who work for days or weeks at a customer site during an outbreak might not receive a patch during the critical period. To stop new attacks that attempt malicious activity, Cisco IT resolved to shift from a signature-based to a behavior-based solution. In a behavior-based solution, policies allow normal application behaviors while preventing abnormal, potentially "bad" behaviors, such as when a downloaded file opens an e-mail address book.

In February 2004, Cisco IT successfully deployed Cisco Security Agent Version 4.0, protecting more than 38,000 desktops across the enterprise from worms and viruses. Cisco Security Agent is an intrusion prevention solution installed on employees' computers. Intrusion prevention systems (IPSs) provide all the features of a personal firewall, plus more. A personal firewall allows or denies actions based on rudimentary rules, usually based on source or destination network addresses. Cisco Security Agent offers built-in policies as well as the option to develop custom policies. For example, Windows system processes normally access Active Directory servers for authentication, but applications that are downloaded from the network typically should not access the user's address book. Built-in policies recognize bad behavior across a diverse set of applications and operating system versions. Administrators can customize policies to fine-tune the security posture for their own environment and applications. An advantage of Cisco Security Agent for Cisco IT is the relatively small set of rules to maintain. The few rules sets define when and

how applications are allowed to access files, networks, and system registrations. Cisco Security Agent blocks any action that violates rules and stores a log of violation attempts. For each type of deviation from expected application behavior, Cisco IT can configure Cisco Security Agent to allow the action, deny it outright without informing the user, or ask the user.

The first test for Cisco Security Agent came soon after deployment with the outbreak of the bagel.aa virus. Of the 38,370 desktops running Cisco Security Agent, only 0.14 percent (about 50) became infected—and those only because the users clicked “Yes” twice when warned that a suspicious application was trying to write to the run key of their registry and trying to access e-mail resources. Since deployment, Cisco Security Agent has resulted in cost savings, increased productivity, easier identification of infected systems, and the confidence of knowing there is a robust layer of defense in place. For a complete description of the challenges, solution, results, and lessons learned in deploying Cisco Security Agent Version 4.0, refer to the case study at http://www.cisco.com/web/about/ciscoitatwork/security/endpoint_intrusion_prevention.html.

CHALLENGE

Even with the successful deployment of Cisco Security Agent Version 4.0 in February 2004, threats to the network continued to grow. Each new worm, virus, or attack made it more important to secure the network from malicious behavior. New features and capabilities were needed beyond those found in Cisco Security Agent Version 4.0. Cisco IT worked to identify areas where improvements could be made and develop and test new features and capabilities.

SOLUTION

Cisco Security Agent Version 4.5 goes beyond conventional endpoint security solutions by identifying and preventing malicious behavior before it can occur, removing potential known and unknown security risks that threaten enterprise networks and applications. Building on the capabilities of Cisco Security Agent Version 4.0, this new version delivers enhancements that improve security, manageability, and scalability; expand language and platform support; and add new forensic capabilities. Although enhancements are numerous, there are nine significant improvements in Cisco Security Agent Version 4.5.

Added scalability

Cisco Security Agent Version 4.5 has increased the maximum allowable number of agents per CiscoWorks Management Center for Cisco Security Agents to 100,000. This enables truly enterprise-scale deployments with centralized policy creation and alert reporting.

Internationalization

Cisco Security Agent Version 4.5 can run on international versions of Microsoft Windows. This includes versions in French, German, and Japanese (Kanji). However, the agent does not support languages that display characters right to left, such as Arabic and Hebrew, and the Management Console cannot be localized.

User-based rules and policies

Cisco Security Agent Version 4.5 can apply security rules and policies based on the current logged-in user context, as defined in Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP), and other directory protocols. These rules can use both user ID and group ID.

Location-based rules and policies

With Cisco Security Agent Version 4.5, several rules and policies can be applied based on the physical or logical location of a computer. For example, a laptop computer could have less stringent security policies when it is connected to the network at the office, but a more stringent policy when connected remotely. Rules and policies can also be applied based on the Network Admission Control (NAC) status reported by the router or switch that the computer is in the process of connecting to.

Application inventory and tracking

Cisco Security Agent Version 4.5 can track which applications are installed on a computer or group of computers as well as which applications are running, which are using the network, whether the application is a network client or server, and which remote IP addresses it communicates with.

Hot-fix/service-pack checking

Cisco Security Agent Version 4.5 can track which hot fixes or service packs are installed on a computer or group of computers.

Secure clipboard data

Cisco Security Agent Version 4.5 can control data written to the clipboard by applications reading sensitive data, and can restrict whether other applications can read the sensitive data.

Antivirus DAT version check

Cisco Security Agent Version 4.5 can check the installation status and antivirus DAT version level for Symantec and McAfee antivirus agents.

Added platform support

Cisco Security Agent Version 4.5 can now run on Microsoft Windows clusters; Red Hat Enterprise Linux 3.0 (Workstation Server, Enterprise Server, and Advanced Server); and Windows XP Home Edition.

Pilot

As with the previous version of Cisco Security Agent, a pilot program was established to test features and capabilities before releasing the application to the entire Cisco network and to customers. But while many pilots are conducted to provide real-world feedback on applications that are relatively complete and stable, the software for Cisco Security Agent Version 4.5 was anything but complete and stable. “The application was evolving. The final capabilities and features were changing radically as the pilot went on, based upon feedback we were receiving and because code was still being written,” says Paul Mauvais, Senior Security Architect at Cisco. “It was more complicated than an average pilot.”

The pilot lasted from August 2004 until April 2005. Approximately 200 desktop and laptop users participated. “The pilot went on right up to pre-release, when we released it to internal folks in mid-April,” says Mauvais. “We had two to three weeks at the end to determine whether everything worked.”

One interesting observation during the pilot involved a feature known as Global Event Correlation. This feature was present in Version 4.0, but was enhanced for Version 4.5. Global Event Correlation has the ability to monitor potentially malicious events around the network. If the number of such events reaches a specified threshold on any given host, Cisco Security Agent can automatically place such devices on an untrusted or quarantine list. “Right from the beginning of the pilot we noticed the difference. That feature made it simple to pick out those IP addresses and identify the hosts in question—which in nearly all instances were infected,” says Mauvais. “We got them cleaned up, helped the users rebuild their machines, and moved on.”

Production

After the pilot, Cisco pushed the software to all employees worldwide, as it typically does, using Altiris over the Cisco Application Content and Networking System distribution network. For more details on deploying applications through Altiris, read the Cisco IT Software Development case study at http://www.cisco.com/web/about/ciscoitatwork/data_center/enterprise_software_delivery_web.html

Users were made aware of the upgrade through a series of e-mail notices. At the time of the upgrade, users received a notice on their screen informing them that, during the upgrade process, their connection would be dropped for a few seconds. This small window of time was necessary to swap out drivers to perform the installation of the software.

Once complete, the connection was reinstated. Most users were unaffected. However, users who had programs running overnight were directly impacted.

Deployment of Cisco Security Agent Version 4.5, which was completed in just one week, went smoothly. During the deployment of Version 4.0, approximately 270 cases were escalated to second-level support personnel. During the deployment of Version 4.5, however, only 25 cases were escalated out of more than 38,000 desktops and laptops that were upgraded. “Cisco TRC will often receive hundreds of cases per day for large application deployments,” says Mauvais. “The Cisco Security Agent Version 4.5 deployment was considerably better than any office deployment the TRC had ever done.”

RESULTS

The experience gained from deploying Cisco Security Agent Version 4.0 prepared Cisco IT for the subsequent rollout of Version 4.5. Trouble cases were minimal and cases escalated were nearly nil, as referenced above. More than 38,000 devices were successfully migrated in just one week, with minimal impact on productivity.

The cost of holding viruses and malicious activities at bay represents a real cost savings. Cisco IT estimates that it costs approximately $300 to “clean up” an infected PC. A single outbreak, unchecked, could cost thousands of dollars. To date, Cisco Security Agent Version 4.5 has proved very effective. Only 15 to 20 infected hosts are discovered each week. More importantly, Cisco has not experienced a P1 virus outbreak in over 18 months. A P1 outbreak denotes a threshold of a certain number of hosts that requires immediate activation of the P1 response team. Cisco Security Agent Version 4.5 has done a better job of slowing the progress of viruses than Version 4.0. When an action is denied, a message is sent to the central servers, which produce reports on demand as requested by IT. With early notification of new abnormal activity, Cisco IT can take early preventive action, minimizing the cost of infection and boosting productivity.

In addition to cost savings and productivity, Cisco Security Agent Version 4.5 provides a new level of confidence. When the next malicious code or virus outbreak occurs, Cisco will have a robust layer of defenses in place. If the next virus manages to circumvent e-mail gateway filters and virus scanning software, Cisco Security Agent is there on each desktop waiting to prevent it from spreading any further.

LESSONS LEARNED

Cisco Security Agent Version 4.5 was a resounding success, in large part due to a tight working relationship between Cisco IT and the business units. “The pilot group that I led worked very closely with the business units,” says Mauvais. “That teamwork ranged from the product requirements documents and engineering all the way up through the various commit stages, including product concept, deliverables, feedback and feature requests, and bug fixes.”

The pilot for Cisco Security Agent Version 4.5 took a nontraditional approach, testing and developing simultaneously and constantly over a nine-month period. Had Cisco IT and the business units chosen to develop Cisco Security Agent Version 4.5 in its entirety first and then pilot that largely complete application, at least some of the capabilities available in Version 4.5 may not have been included.

As with the earlier version of Cisco Security Agent, decisions made by users remain a potential source of problems. Mauvais emphasizes that user education is critical to success. “Do what it takes to educate users thoroughly. There will be some application behaviors that you neither allow nor explicitly deny, but rather ask the user to decide. If they make uneducated choices, infections can still occur.” Users should never open e-mail attachments that they are not expecting. Users should be made aware of the consequences of ignoring Cisco Security Agent warnings of suspicious activity when they are opening suspect attachments. Even a single compromised machine can spread a flood of infected e-mail throughout the corporation, resulting in lost work time and the cost and time of cleaning up.

NEXT STEPS

Cisco IT next plans to install Cisco Security Agent on its internal and customer-facing Windows 2000 servers,

including those that run Cisco Unified CallManager and Cisco Unity® software. The Cisco CallManager and Cisco Unity business units have developed their own policies for their servers. “Windows servers are just as important as desktops and just as vulnerable,” says Mauvais. “Installing Cisco Security Agent is an essential part of our strategy to ensure availability of voice over IP and other critical IP applications.”

Cisco Security Agent Version 4.0 established a strong defense against various types of attacks. Cisco Security Agent Version 4.5 has expanded those capabilities, adding an even higher level of network security. But network security is not a final solution. Like quality, it is a continuous improvement process. Threats will continue to escalate and to become more sophisticated. Network professionals must keep pace with these threats. Further enhancements to Cisco Security Agent are already underway.

FOR MORE INFORMATION

To read the entire case study or for additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit

NOTE

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**