# How Cisco IT Upgraded Intrusion Prevention Software to Improve Endpoint Security

## Cisco Security Agent Version 5.2 detects and stops security threats to 70,000 employee desktops worldwide.

**Cisco IT Case Study/Security/Cisco Security Agent:** The Cisco® IT team protects the company's desktops and servers from constantly changing malware and new vulnerabilities. Threat-protection methods must be easy to deploy and manage in a global enterprise, unobtrusive for employees when possible, and flexible to enforce different policies based on the connection method, department, or user. Cisco IT achieved these goals with Cisco Security Agent, a behavior-based threat-prevention system. This case study describes Cisco IT's use of Cisco Security Agent on Windows desktops across the Cisco global network, an innovative enterprise environment that is one of the largest and most complex in the world. Cisco customers can refer to Cisco IT's real-world deployments to help support similar enterprise needs.

> "Cisco Security Agent is the best security technology we've deployed in the last five years."
>
> **John Stewart, Vice President and Chief Security Officer, Cisco**

## Challenge

With more than 70,000 desktops worldwide, Cisco IT needs an effective, flexible, easily manageable threat-prevention solution that can protect against constantly changing types of malware. For example, in 2004, the biggest threats to Cisco desktops were viruses, worms, and trojans. In 2008, Cisco IT is more concerned with spyware, botnets, rootkits, targeted attacks, and threats from social networking sites. In 2010, the most dangerous threats might be unimagined today. Protecting desktops is crucial to help ensure business continuity, prevent information theft, and minimize cleanup costs after infections. In 2003, Cisco estimated that each minor malware outbreak cost US$250,000 in IT remediation and cleanup efforts, and that severe incidents cost up to US$2.5 million. And these costs do not include lost productivity, damage to critical systems, and possible information loss.

Although Cisco used leading antivirus solutions, desktops remained vulnerable to day-zero threats, whose signatures are not yet known. "Traditional antivirus solutions are at best 90 percent effective, but 10 percent of malware still gets through," says John Stewart, vice president and chief security officer at Cisco. At one point, Cisco IT spent US$1 million quarterly in operational costs related to cleanup efforts. "We needed a different approach to security because we couldn't sustain the required levels of spending to battle the escalating attacks," says Stewart.

Cisco IT also wanted to forestall the rush to install vendors' patches for newly discovered operating system and application vulnerabilities. "We prefer to perform full quality-assurance testing on all patches before deploying them in the Cisco development environment," says Paul Mauvais, a senior security architect at Cisco. "In the past, we had to balance the need for thorough testing with the need to quickly install patches to avoid exposure." Cisco's global and mobile workforce makes it even more important to protect desktops before patches can be installed. If Cisco sends out a patch at 1:00 p.m. Pacific time, employees in other parts of the world might not receive it until the next day, when their site's network might already be infected. Furthermore, many Cisco employees work for days or weeks at customer sites and do not receive patches until they reconnect to the Cisco network. This leaves them vulnerable during critical outbreak periods.

## EXECUTIVE SUMMARY

**CHALLENGE**

- Protect 70,000 systems from constantly changing threats
- Minimize IT resource requirements for desktop protection
- Reduce reliance on patching
- Gain flexibility to tighten or loosen restrictions on application behavior for different subnets and employees

**SOLUTION**

- Deployed Cisco Security Agent on all Windows desktops
- Centrally managed all desktop agents

**RESULTS**

- Saved US$4 million annually on remediation after attacks
- Reduced IT resource requirements from 12 full-time employees to less than one full-time employee
- Gained ability to thoroughly test patches before deploying, and to distribute them when convenient rather than immediately
- Flexibly accommodated differing desktop security needs within the global enterprise

**LESSONS LEARNED**

- Introduce policies gradually
- Minimize actions required by employees
- Use Cisco Security Agent as part of an integrated security plan with antivirus, e-mail filters, and patching

**NEXT STEPS**

- Deploy Cisco Security Agent on Windows servers (in progress)
- Track and control use of removable media
- Mark application traffic and files for differential treatment
- Protect against IPv6 operating system vulnerabilities

To augment its antivirus and patching solutions, Cisco IT wanted a new approach to desktop protection that met the following requirements:

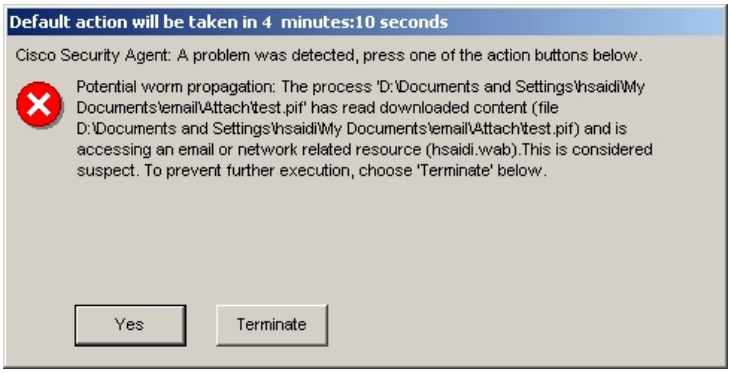
- Low management requirements from Cisco IT
- Minimal action required from employees, to protect their productivity and avoid tempting them to disable or circumvent the solution
- Flexibility to apply different security policies based on connection type, place in the network, or employee role. “Cisco employees who work with U.S. government customers, for example, need a stronger desktop encryption program,” says John Ireland, system administrator for Cisco’s host security architecture.

## Solution

With executive-level support and collaboration with the Cisco Information Security (InfoSec) Services team, Cisco IT adopted Cisco Security Agent in 2004. Currently deployed on more than 70,000 systems, Cisco Security Agent provides proactive protection against day-zero threats, brand-new exploits, and variants trying to take advantage of recently announced vulnerabilities.

Cisco Security Agent complements antivirus solutions and patching efforts by looking for unusual application behavior. Malware is often the culprit for unexpected behavior, such as an application’s attempt to open a Cisco employee’s e-mail address book, an external Website’s attempt to install an application, or an unexpected network connection attempt. When Cisco Security Agent detects a policy violation, it responds in the way that Cisco IT specified: allow the action, deny it outright without informing the user, or ask the user (Figure 1).

**Figure 1.** Employees Must Explicitly Allow Actions That Appear to Be Malicious




Unlike antivirus solutions, Cisco Security Agent does not need to recognize a known signature to detect malware. “Cisco Security Agent is a heuristic way of protecting a computer from attacks, particularly attacks that have not been seen before,” says Stewart. And unlike personal firewalls, which have the potential to allow malicious traffic if it is from a trusted source, Cisco Security Agent protects desktops even against threats that originate from inside the Cisco network. These can include malicious scanning, as well as connection attempts by vendors using infected laptops.

Cisco Security Agent comes with dozens of predefined policies (Figure 2). Cisco IT uses some of the predefined policies and has also developed custom policies, including:

- Allowing the software delivery agent used within Cisco to perform its functions, which might ordinarily be considered suspect
- Allowing desktops that use a particular e-mail client to access internal e-mail servers by dynamic name or IP address. This action is blocked for employees using all other e-mail clients.
- Permitting the WebEx conferencing solution to launch its applets.

**Figure 2.** Sample Policy


### Pilot Deployment

Before deploying Cisco Security Agent companywide, Cisco IT conducted a 400-user pilot to develop and test policies and help ensure that the new solution would be acceptable to users. To plan and manage the pilot, Cisco IT assembled a project management team with representatives from the Personal Computing Solutions group that handles PC support, engineering, InfoSec, and the helpdesk support team of the Global Technical Resource Center. Global employees who volunteered to participate in the pilot agreed to provide specific types of information at specified times and were instructed to download the Cisco Security Agent software from an internal Web page.

Cisco IT set up a Windows server at Cisco headquarters in San Jose, California, installed the Cisco Security Agent management software, and began developing policies. When defining policies, Cisco IT took care to not require too many actions from users, because this might interfere with productivity or encourage employees to try to circumvent or disable the software.

Cisco Security Agent already understands normal application behavior for commonly used applications, which enables it to block suspicious actions. To understand expected behavior for the other applications in use at Cisco, Cisco IT used Cisco Security Agent to create a profile for five complex applications, including the one used to distribute software to desktops. “We did not have to profile all 10,000 applications in use at Cisco,” says Mauvais. “Profiling a few of the more complex applications gave us a starting point that we could refine after testing within the

pilot environment." Pilot participants were asked to operate the application as they normally do over the course of a day, which gave Cisco IT the information that it needed to identify allowed actions and set up the policy to deny all other actions.

At the outset of the pilot, Cisco IT configured Cisco Security Agent to send all messages about suspicious application behavior directly to a management console rather than users' desktops. This avoided unnecessary disruptions for employees, while giving IT the opportunity to learn about normal behaviors. While refining its policies, Cisco IT also fine-tuned its global support processes for Cisco Security Agent by defining criteria for escalation, internal service-level agreements, the mechanism used to distribute the software, and communications policies with users. The four-month pilot with 400 users gave the Cisco teams confidence that the initial policies would not impede employee productivity or overwhelm the support organization.

### Enterprise Deployment

After the pilot, Cisco IT deployed production management servers for Cisco Security Agent. Cisco pushed the software to all employees worldwide using its software distribution application, over the Cisco Application Content and Networking System (ACNS) distribution network. "The introduction of Cisco Security Agent was extremely efficient, and we scaled to tens of thousands of desktops in less than three weeks," says Stewart. "With the deployment, we effectively shifted from solely relying on blocking of known threats to a more heuristic approach that adds a new layer of intelligence."

If communication between Cisco Security Agent and the Management Center is temporarily disrupted, for example, if a laptop user has not connected to the VPN, Cisco Security Agent continues to enforce security policy. It captures any security alerts and uploads them to the Management Center when communication is restored. Cisco IT regularly updates Cisco Security Agent to take advantage of new features.

### Deployment in Manufacturing Environment

Cisco's Scientific Atlanta Division uses Cisco Security Agent in its manufacturing facility in Juarez, Mexico. Manufacturing and test engineers have the flexibility to install a variety of applications on test stations, and as a result, the Juarez facility previously experienced significant virus activity, which sometimes resulted in production outages. When all 1200 test systems were allowed to communicate with each other, as well as centralized servers, nothing was able to stop worms from spreading. Identifying all infected systems could take a month or more, diverting IT resources from other projects. "Our goal for deploying Cisco Security Agent was to increase our test systems' availability, which is of paramount importance to the business," says Scott Stanton, and information security architect for Scientific Atlanta.

The Scientific Atlanta IT group met its goals by deploying Cisco Security Agent on all 1200 test stations and developing a strict policy governing which test stations could communicate with which servers. For example, an assembly line for set-top boxes might have 30 test stations, each of which communicates over the network to a central server to indicate whether the unit passed or failed. "We set up Cisco Security Agent to enforce a policy that test stations can only communicate with the required servers; not the Internet or other clients," says Stanton. "As a result, viruses can no longer spread from station to station." The policy has also reduced bandwidth consumption.

Before developing Cisco Security Agent policies, the Scientific Atlanta IT team took approximately two months to identify the processes and protocols used on the manufacturing floor. To collect baseline information, the IT group installed Cisco Security Agent on approximately two dozen test stations and logged, but did not block, all application activity. "First we analyzed 100 applications to determine typical transactions, processes, protocols, ports, and IP addresses," says Galo Guzman, manager for Juarez IT security. "Based on that information, we configured several dozen rules for allowed application behavior on test stations." For example, some desktop applications are set up by default to call home to an Internet server to update themselves, and the IT group decided to disallow this activity. To simplify policy configuration, the IT group standardized the file path for its test application suites. "By storing all

allowed applications for test engineers in the same folder, we were able to develop a simple policy that allows access to applications in that file path to access the network servers, and disallows access to applications stored anywhere else," says Guzman.

The benefits of deploying Cisco Security Agent on the manufacturing floor were immediate and measurable. "We deployed Cisco Security Agent on more than 1200 test stations with no impact to the manufacturing process, and infections have decreased significantly," says Galo. "In addition, the Cisco IPS [Intrusion Prevention System] is detecting far less malicious activity on manufacturing network segments." The number of incidents reported monthly decreased from 31 to 11 the month after Cisco Security Agent was deployed, and only one trouble ticket was issued in December and January of 2008. "That represents enormous time savings for the IT group," Galo says.

### Education

To educate users on the value of the software and what to expect from it, Cisco IT issued announcements on the corporate intranet, in an IT newsletter, and through companywide e-mail.

### Central Management

Cisco IT centrally manages all 70,000 agents using the browser-based Management Center to distribute the agent to desktops, create or modify security policies, monitor alerts, and generate reports. "Now just two Cisco IT employees manage Cisco Security Agent on a part-time basis," says Kathy Tucker, IT engineer with the Cisco Desktop Management Team. Initial deployment took approximately 65 percent of the two engineers' time for two or three weeks. Now Tucker estimates that she and another engineer spend just 10 percent of their time developing new policies in response to requests from InfoSec or when a specific user or group needs a policy tightened or relaxed. "Once a set of policies is in place and tested for the environment, no IT effort is required until a new situation arises," she says.

### Server-Based Protection

After deploying Cisco Security Agent on desktops, Cisco IT also deployed specialized versions on the company's Cisco Unity® and Cisco Unified Communications Manager (formerly Cisco CallManager) servers.

## Results

### Increased Security

"Our deployment of Cisco Security Agent has changed the way that our defense mechanisms work together," says Stewart. "We have shifted from a reactive to a proactive approach to security. Cisco Security Agent is the best security technology we've deployed in the last five years." Ireland adds, "Cisco used to regard desktops as one of the most insecure aspects of the Cisco network. Now we regard them as one of the most secure."

Just two months after deployment, the solution proved its worth during a major virus outbreak. Although Cisco IT applied the new virus filters to Cisco's e-mail servers just minutes after the virus hit, it had already been spread from everyone in the company to everyone else through e-mail. Of all the desktops running Cisco Security Agent, only a small fraction became infected, and those only because the employees clicked "Yes" twice when warned that a suspicious application was attempting to write to the run key of their registry and access e-mail resources. Cisco IT has since changed its policies to rely less on employees' judgment regarding whether or not to allow suspicious application behavior.

### Lower IT Resource Requirements

Before deploying Cisco Security Agent, 12 Cisco IT engineers were dedicated to desktop security, according to Robert Rimar, manager of the desktop engineering group. Now Cisco IT can protect 70,000 desktops with just 20 to 30 hours per week of effort. "By reducing our workload, Cisco Security Agent has freed up time for Cisco IT to improve desktop usability and undertake strategic projects," says Rimar. IT employee satisfaction has also improved.

"Cisco Security Agent has eliminated the need for those dreaded 2:00 a.m. conference calls to plan our response to a new virus outbreak," says Tucker.

### Reduced Costs for Cleanup After Infection

With early notification of new abnormal activity, Cisco IT can take early preventive action, minimizing the cost of infection and avoiding losses of productivity for Cisco employees worldwide. The cost savings for remediation are significant. Since deploying Cisco Security Agent companywide in 2004, the company has saved more than US$4 million annually in personnel costs for reacting to malware incidents.

### Adaptability to New Types of Threats, Different Needs Within Cisco

Because it looks for aberrant application behavior rather than signatures, Cisco Security Agent detects and stops threats that have never before been seen, including new types of spyware, bots, rootkits, viruses, worms, and trojans. "Cisco Security Agent catches a lot of malicious behavior right out of the box," says Ireland. "And Cisco IT develops new policies as needed for different users and places in the network."

In 2008, Cisco IT uses Cisco Security Agent in different ways than it did in 2003, when the solution was first deployed. For example, the Scientific Atlanta Division is using Cisco Security Agent to apply stricter or less strict controls on allowed application behavior based on whether the employee is connecting internally or from outside the company. "We configured a dynamic policy dependent on system state," says Stanton. Cisco Security Agent knows the range of internal IP addresses in use at the company. If the user's network interface has one of these addresses, Cisco Security Agent applies a policy that allows administrative access and the use of additional applications. If the interface has any other address, Cisco Security Agent applies a stricter policy that prohibits administrative access, restricts access to certain applications, and blocks inbound traffic, preventing intruders from performing reconnaissance or sending worms, viruses, or other malicious payloads. And when Cisco employees use a public wireless hotspot, Cisco Security Agent can implement the personal firewall differently, so that other people connected to the network cannot access their ports. "Microsoft Vista performs a one-time check, but Cisco Security Agent takes it a step further by constantly watching for undesired application behavior that would occur if the port were accessed," says Ireland.

### More Efficient Patch Management

Although software patches are being released with increasing frequency, Cisco IT now has the freedom to thoroughly test patches before deployment, and to wait to distribute multiple patches at once. By avoiding hurried releases, Cisco has reduced application issues arising from new patches, reduced downtime from installation errors, and applied better change management, reducing risk. "Uptime is critical in a manufacturing environment, so we welcome any solution that reduces the need to shut down and restart PCs," says Bob Scalise, director of enterprise security, Cisco Scientific Atlanta Division. "Cisco Security Agent allows us to expand our patching windows to accommodate additional testing and validation, instead of being forced into a strict monthly patching schedule. If a vendor discovers a new vulnerability and releases a patch, Cisco Security Agent can mitigate the risk and allow us to select a lower-impact deployment window for the patch."

## Lessons Learned

Cisco IT offers the following advice to other companies deploying Cisco Security Agent:

- Introduce new policies gradually. "Take your time with policy testing and assemble the broadest variety of people and applications, because Cisco Security Agent concerns itself with the interactions among applications on a desktop," says Mauvais. "Be willing to start with a policy that's a bit weaker than what you eventually want, to help ensure user acceptance."

- Educate employees so that they make responsible decisions. The policy might ask the user to make a decision to allow or deny an application behavior. If they make uneducated choices, infections can still occur. In particular, remind employees to never open unexpected e-mail attachments, and to not ignore Cisco Security Agent warnings of suspicious activity.
- Use Cisco Security Agent with e-mail filters, antivirus, and patching. The damage caused by an outbreak happens within the first few hours. Using multiple layers of security to limit the number of infected PCs reduces the time, cost, and effort of cleaning up after a virus attack.

## Next Steps

### Protecting Servers

Cisco has deployed Cisco Security Agent on the majority of its Windows applications servers. “Cisco Security Agent allows us to proactively protect our servers instead of having to interrupt our other activities whenever a new threat arises,” says Michael Rea, systems administrator for Microsoft infrastructure hosting.

### Controlling Use of Removable Media

Cisco IT plans to use Cisco Security Agent to gather data on employees’ use of removable media, such as USB drives and MP3 players. “By collecting baseline usage data for different groups within Cisco, such as salespeople and engineers, we will be able to create intelligent policies,” says Ireland. For example, the Cisco customer service group is considering developing a Cisco Security Agent policy that requires data from Cisco customers to be stored on an encrypted area on employees’ laptops.

### Application Marking

Cisco IT is also considering using Cisco Security Agent to mark different types of desktop application traffic for special treatment, such as priority on the network. Ideas include:

- Sending a message to the Management Console whenever a file marked confidential or containing certain words is copied, e-mailed, or opened by an application.
- Marking application traffic from social networking sites. Attackers are targeting these sites because their combination of Web, e-mail, instant messaging, and file transfer capabilities make it easier to distribute malware in ways that traditional desktop-protection systems cannot detect.
- Enabling Cisco Adaptive Security Appliances to apply application-specific inspection policies.

### Protection Against IPv6 Security Vulnerabilities

Cisco is currently integrating IPv6 into its network, and Cisco Security Agent will help protect against new security vulnerabilities during the transition. “The Microsoft Vista operating system has IPv6 capabilities, which creates exposure in areas of the Cisco network that are not IPv6-ready,” says Ireland. “Cisco Security Agent will help us block and control IPv6 exposure on Vista PCs.”

Stewart concludes, “The ability to protect our desktops without having to constantly react to new malware is creating significant operational savings at Cisco. Cisco Security Agent is an incredible tool to protect the company from known and unknown threats.”

### Gathering Event Data

Cisco IT plans to increase its use of Cisco Security Agent to gather more information about application behavior, which will help IT to plan other security tactics.

## For More Information

To read additional Cisco IT case studies on information security, 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.
San Jose, CA

**Asia Pacific Headquarters**
Cisco Systems (USA) Pte. Ltd.
Singapore

**Europe Headquarters**
Cisco Systems International BV
Amsterdam, The Netherlands

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.**



Printed in USA

C00-000000-00 08/07