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.

With more than 70,000 global desktops, Cisco IT needs an effective, flexible, easy-to-manage threat-prevention solution. Adaptability to new types of threats is crucial. In 2004, the biggest threats were viruses, worms, and trojans. In 2008, more urgent threats are spyware, botnets, rootkits, targeted attacks, and threats from social-networking sites. In 2010, the most dangerous threats might be unimagined today.

Cisco also wanted to diminish the rush to install patches for operating system and application vulnerabilities. The company prefers to perform thorough testing on patches before installing them, but had to balance this with the risks of unprotected vulnerabilities.

Today, Cisco Security Agent protects all 70,000 global desktops by looking for unusual application behavior. Unusual behavior can be stopped even if the threat signature is not known. Cisco® IT used some predefined policies and also developed custom policies.

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

Cisco has shifted from a reactive to a proactive approach to security. The company saves more than US$4 million annually in personnel costs for reacting to infections.

Fewer IT resources are needed for desktop security. Protecting desktops now requires just 20 to 30 hours a week of effort—not the 12 full-time employees previously required.

Cisco can apply stricter or less stringent controls in different parts of the enterprise. One Cisco division applies stricter controls if employees connect from outside the company.

Patch management is more efficient. Cisco IT now has the freedom to thoroughly test patches before deployment and to wait to distribute multiple patches at once.

For More Information
Case Study: http://www.cisco.com/web/about/ciscoitatwork/case_study.html

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.