



Desktop Security Upgrade

How Cisco IT Upgraded Intrusion Prevention Software to Improve Endpoint Security



A Cisco on Cisco Case Study: Inside Cisco IT

Overview

- Challenge

 - Protect 70,000 global desktops from constantly changing threats

- Solution

 - Cisco Security Agent

- Results

 - Increased security and lower IT resource requirements

- Next Steps

 - Enforce new desktop security policies

Challenge

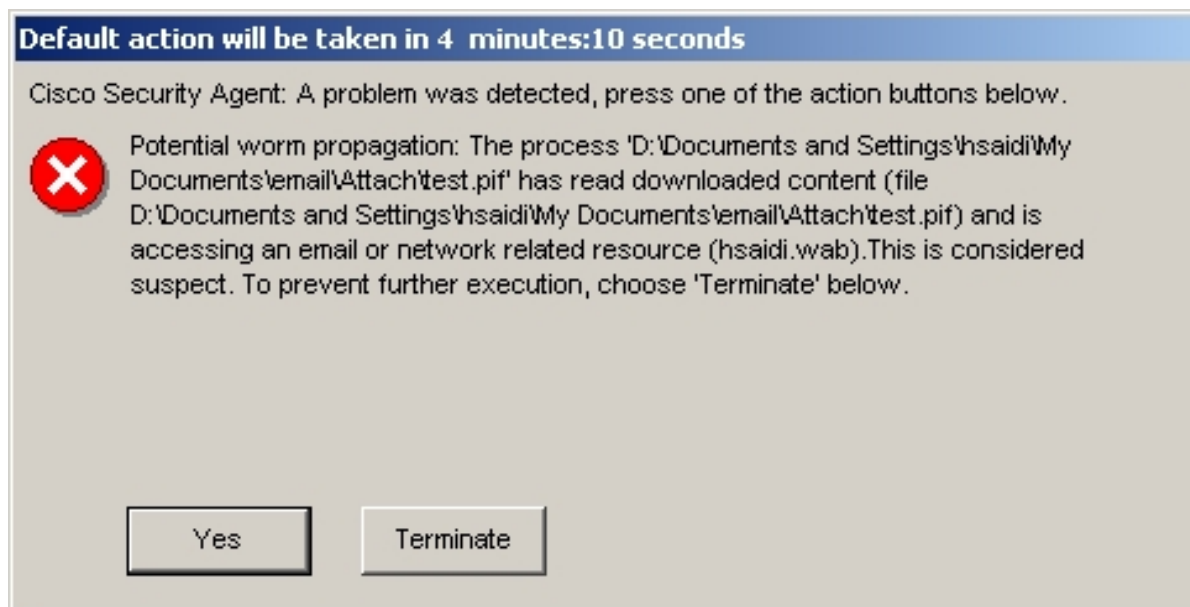
Protect 70,000 global desktops from constantly changing threats

- Adapt to new threat landscape
 - 2004: viruses, worms, trojans
 - 2008: spyware, botnets, rootkits, targeted attacks, social networking sites
 - 2010: not yet known
- Avoid high costs of remediation and cleanup: US\$250K to \$2.5 million per incident
- Diminish the rush to install patches for operating system and application vulnerabilities

Solution

Cisco Security Agent

- Looks for unusual application behavior and responds according to policy: allow, deny, or ask user



Solution

Predefined and Custom Policies

Management Center for Cisco Security Agents V5.2	
Events Systems Configuration Analysis Maintenance Reports Search Help	
Compliance	is necessary for the cardholder data environment.
<input type="checkbox"/> PCI Requirement 1.3.9 Compliance - External Systems	4 rules Installation of personal firewall software required on any mobile or employee-owned computers with direct Internet connectivity.
<input type="checkbox"/> PCI Requirement 1.3.9 Compliance - Internal Systems	5 rules Installation of personal firewall software required on any mobile or employee-owned computers with direct Internet connectivity.
<input type="checkbox"/> PCI Requirement 10.2.1 - 10.2.4 Compliance	2 rules Track and monitor all access to network resources and cardholder data.
<input type="checkbox"/> PCI Requirement 10.2.1 - 10.2.4 Compliance Userstate Admin	1 rule Track and monitor all access to network resources and cardholder data (especially those with administrative privileges).
<input type="checkbox"/> PCI Requirement 10.5.1 10.5.2 User State	1 rule Limit viewing of audit trails to those with a job-related need. Protect audit trail files from unauthorized modifications.
<input type="checkbox"/> PCI Requirement 10.5.1-10.5.5 Compliance	3 rules Limit viewing of audit trails to those with a job-related need. Protect audit trail files from unauthorized modifications.
<input type="checkbox"/> PCI Requirement 11.4 Compliance	7 rules Network intrusion detection systems, host-based intrusion detection systems/intrusion prevention systems to monitor networks

Solution

Deployment

- 400-user pilot
- Used Cisco Security Agent to profile five complex applications for expected application behavior
 - Did not need to profile all 10,000 applications in use at Cisco
- Defined policies, taking care not to require too many actions from users
- Deployed in enterprise
 - Pushed software to tens of thousands of employees worldwide in three weeks
- Deployed in manufacturing environment on 1200 test stations
 - Policy stipulates that test stations can communicate with centralized servers, not each other, to prevent infection spread

Solution

Central Management

- Browser-based Management Center distributes the agent to desktops, creates security policies, monitors alerts, and generates reports
- Initial deployment took approximately 65% of two engineers' time for two or three weeks
- Just two Cisco IT employees spend 10% of their time managing Cisco Security Agent when new policies are needed

Results

Increased Security

- Saved US\$4 million annually on cleanup after attacks
- Reduced IT resource requirements from 12 full-time employees to fewer than one
- Diminished the rush to install patches
- Accommodated varying desktop security needs within the enterprise by applying stricter or less stringent controls

Next Steps

Enforce New Security Policies

- Control use of removable media
- Mark different types of desktop application traffic for special treatment
- Block and control IPv6 exposure on Windows Vista PCs
- Gather more information about application behavior to help plan other security tactics

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



CISCO



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.

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, FastStep, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)