How Cisco IT Uses Intrusion Prevention to Protect User Endpoint Devices

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

BUSINESS BENEFITS

- Reduces costs associated with virus and worm remediation
- Increases employee productivity by impeding virus infections
- Detects previously infected systems
- Provides ease of use for employees
- Is easily configured and customized
- Gives companies confidence in executing normal business functions

"The cost of viruses and worms worldwide in 2003 was US$28 billion. The cost is expected to grow to $75 billion by 2007."
– Radicati Group study

Organizations of all sizes are protecting their networks against the catastrophic effects of viruses, worms, and similar network security intrusions.. In late April 2004, an especially malicious virus known as bagle.aa attacked almost every PC and laptop within Cisco's network. Yet Cisco's operations were unaffected thanks to Cisco Security Agent.

Before deploying Cisco Security Agent, Cisco used a multifaceted security approach that included security appliances, network-based detection systems, and antivirus software. But this approach had its limitations, particularly for a mobile workforce often connected to public and client networks that did not offer Cisco network programs or antivirus updates. Additionally, administering security across the wide variety of devices used by Cisco's global workforce was complex.

Cisco implemented Cisco Security Agent to prevent against increasing threats and to simplify administration. Cisco implemented the solution on most of the company's individual computer assets. The solution provides built-in policies that recognize unusual behavior across diverse applications and operating systems. Customizable rule sets, transparent to users, define when and how applications are allowed to access files, networks, and system registries.

Cisco Security Agent proved its value just two months after deployment. Of the 38,370 desktops running Cisco Security Agent, only about 50 (0.14 percent of the total) became infected during the bagle.aa virus outbreak. The infections were due to user error—the users clicked "Yes" twice when warned that a suspicious application was trying to modify their systems. Cisco Security Agent was 99.86 percent effective in stopping the bagle.aa virus at Cisco.

Cisco IT expects the solution to pay for itself quickly. With early notification of new abnormal activity, Cisco IT can take preventive action and implement configuration changes as needed. Employees can feel confident that Cisco Security Agent is protecting their data and applications.

Case Study: http://www.cisco.com/en/US/about/ciscoitatwork/case_studies/security_dl1.html

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

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.**

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, 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, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0705R)