Cisco Protects Data Center Assets with Network-Based Intrusion Prevention

BUSINESS BENEFITS
• Protects data center assets • Identifies events before harm is caused • Enables early detection and remediation • Helps prevent data loss or service interruption

Company detects and mitigates network threats before experiencing data loss or service interruption

To protect network availability and intellectual property, Cisco constantly monitors its network for a large assortment of threats, including insider threats and unauthorized access to data center assets. Malicious activity can originate from outside the company walls or from within, usually from infected or compromised hosts.

The perimeter-based intrusion prevention system (IPS) did not provide visibility into security events inside data centers, where the company's most valuable assets reside. Perimeter-based IPS only detects threats contained in traffic that flowed into or out of the company. Therefore, the Cisco Computer Security Incident Response Team (CSIRT) only became aware of unwanted network traffic after it had caused a problem such as sluggish performance on a WAN link from a branch office to headquarters**.**

Now CSIRT uses network-based IPS to detect and mitigate internal security events before users experience a secondary impact. In 2007, the CSIRT team discovered 97 percent of security incidents before anyone else did—compared to 8 percent in 2004, before the deployment.

> "Network-based IPS enables us to detect and mitigate internal security events before users experience a secondary impact, such as… service disruption, loss of intellectual property, or infection."
>
> **Gavin Reid, Manager of Computer Security Incident Response Team, Cisco**

The network-based IPS detected the Rinbot virus before it was known. CSIRT was able to develop a signature and push it out to the IPS sensors, which identified a few hundred affected lab systems. Early detection and remediation prevented further damage.

CSIRT has become proactive in mitigating network threats before they cause data loss or service interruption. Every week between March and June 2007, Cisco found and mitigated multiple command-and-control servers that were being used to remotely control systems within Cisco.

For More Information

Case Study: http://www.cisco.com/web/about/ciscoitatwork/case_studies.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.

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 (USA) Pte. Ltd.
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.**

Printed in USA

C00-000000-00 08/07