

Technology Best Practices for **Endpoint** Security

Introduction

As technologies such as high-speed networks, switching, and end-to-end encryption are more widely adopted, providing desired security at the network level becomes a major challenge. One important place to enforce security is at the endpoint, where data resides and the potential for damage is greatest. Today, businesses are confronted with the availability of several point products, each attempting to solve a part of the endpoint security problem. These include distributed personal firewalls for protection against network-borne threats, antivirus scanners for detection of file-based threats, and audit or integrity products for detection of malicious configuration activity. These technologies do not address new attacks that are carried over existing protocols to attack applications, or new content-based attacks that attack systems before vendors are able to release and distribute signatures and other responses.

This document outlines the technology best practices for endpoint security solutions, to help organizations make informed decisions when choosing endpoint security products.

Best Practices

Any organization that intends to protect itself through the use of endpoint security technology should consider several factors when evaluating products that address the

organization's defined security requirements. Chosen solutions must meet corporate security, manageability, and flexibility requirements; otherwise, the solution will be incomplete or will introduce a significant management burden that overshadows the security benefits.

Best practices should include the following:

1. *Real-time prevention decisions*

To ensure the highest levels of security and minimize the ability to bypass the security policy on a host, application calls must be intercepted at the kernel level where their adherence to policy is determined. Solutions that are implemented by replacing shared libraries or analyzing system audit logs can be bypassed relatively easily. An effective endpoint security strategy includes preventing violations in real time, rather than noting attacks or system changes after they have occurred.

2. *Defense-in-depth protection from attacks*

To completely enforce a company's security policy, endpoint security must intercept all major points of communication between applications and the underlying system. Network control must limit client/server communications at the port and protocol levels, as well as hosts for permitted communications; file system



controls must allow or deny read or write access to folders and files on an individual and group basis; registry controls must prevent the overwriting of important registry keys that control how the system and other applications operate; and COM controls must restrict interprocess communications to allowable access.

Attacks have multiple phases, exploiting network and application-level weaknesses, replicating and distributing themselves, and making unauthorized changes to the system. A complete endpoint security strategy must protect systems from all of these phases, so that if a new class of attack is released, it will be thwarted at one or more of the stages.

3. *Real-time correlation at the agent and enterprise levels*

Correlation is vital for an endpoint security technology. Correlation deployed at the agent provides a level of accuracy on prevention decisions that does not exist with signature matching approaches. Correlating sequences of events within the context of an application's behavior eliminates the potential for false positives, and correlation at the enterprise level enables security to be adaptive. By correlating the events on distributed agents, endpoint security policies can be dynamically updated to prevent propagation of malicious code, preventing widespread damage to numerous resources.

4. *Behavioral approach*

The endpoint security approach must enforce appropriate system and application behaviors to ensure that the security implemented is proactive, not reactive. Solutions that rely on signatures provide security only to the release of the most recent signature update.

5. *Flexibility to meet unique corporate needs*

Every corporation is unique in the details of how it configures and manages its systems and corporate applications. Endpoint security solutions must be flexible to accommodate this uniqueness, by permitting the customization of existing policies and the creation of new policies that accommodate both unique applications and unique implementations. The solution must support automated policy creation to ease the management burden of manually creating policies.

6. *Ease of deployment*

The endpoint security strategy should minimize the personnel overhead associated with agent deployments. Solutions must provide ready-to-use functions to allow rapid deployment of the desired security policies, and must allow for new and custom policies to be rolled out as needed without additional intervention at the host level. Solutions must support Web-based deployment, and allow for easy integration with standard corporate software distribution mechanisms.

7. *Centralized event management*

All events generated by the agents must roll up into a centralized repository from which alerts and reports may be generated. Solutions that are considered must support standard alerting interfaces such as Simple Network Management Protocol (SNMP), paging, e-mail, and flat files, and must allow custom interfaces to the alerting system to easily integrate with corporate systems.

8. Platform coverage, with support for desktops and servers

Solutions that are considered must provide coverage for the critical operating systems that the corporation wants to protect. In light of recent attacks like NIMDA, which target multiple hosts, the same management and enforcement paradigm must apply to both desktop and server-based systems.

9. Administration

To ease policy management, policies must be centrally definable, and automatically distributed to agents on a configurable interval. Policies must also be exportable for replication and archive purposes. Companies with more than one administrator require a “manage from anywhere” capability to ease management of their environments. Endpoint security solutions should be manageable from anywhere using a standard Web browser to avoid the installation of custom software at each administrator’s desktop, to avoid the installation of insecure and difficult-to-maintain software that enables remote administration, and to lower the learning curve for IT staff.

Large corporations that have thousands of systems requiring protection should consider solutions where a single manager can support thousands of agents, and allow for the replication of policy across organizational or regional boundaries.

Summary

Companies should ensure that their endpoint security solutions meet the security, manageability, and flexibility requirements outlined in this document to avoid limited or unmanageable solutions.



Corporate 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: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0304R)

BU/LW4850 07/03