



WHITE PAPER

PREVENTING INFORMATION THEFT WITH CISCO SELF-DEFENDING NETWORKS

SUMMARY

Many organizations have extended their networks to include data centers, remote business travelers, and business partners, reaping the benefits of increased productivity through accessibility. However, this increased connectivity offers new opportunities for theft of critical intellectual property. Employees and trusted insiders are often (sometimes unknowingly) the perpetrators of information theft. Cisco Systems® offers unique integrated security solutions that allow organizations to protect themselves against information theft from both external and internal sources, using their existing investment in computing, network and security platforms.

THE SECURITY LANDSCAPE

Computer and network technology has allowed organizations to operate more efficiently and serve clients more effectively. However, the increasing mobility and accessibility of today's business networks bring increased security challenges. Wireless networking, employee remote access, and the prevalence of teleworking provide more network entry points for malicious users or code.

Network security is a fairly new discipline, so finding qualified security professionals is challenging. It can be a struggle for organizations to justify additional security spending. Network and IT spending is often justified based on return on investment (ROI), whereas network security has been traditionally viewed as a cost center. This perception is changing, as organizations discover that better network security makes business transactions safer and more efficient across the entire network infrastructure. In the long term, network security saves money for organizations.

INFORMATION THEFT CHALLENGES

For organizations, many thefts involve corporate intellectual property, stolen to sell to competitors for financial gain. Organizations report* that theft of proprietary information causes the greatest security-related financial losses, with an average cost of \$2.7 million per incident. Another lucrative target is identity theft, such as stealing the social security numbers of employees or credit information of clients. In a recent study, more than 70 percent of customers surveyed consider theft of bank account number, social security number, and credit card information of very high concern**.

Thieves can come in many forms. Some may be hackers outside your organization trying to penetrate your external network defenses. Others may simply walk in a building behind employees, then attempt to steal information using their own or another computer. Some may be your employees, contractors, business partners, or other trusted individuals, attempting to steal information for profit or revenge. Industry reports indicate that employees are responsible for 70 percent of unauthorized access to information systems, and more than 95 percent of intrusions that result in financial losses.* Organizations must anticipate and guard against each of these scenarios in a continuous, coordinated manner.

* Source: CSI/FBI Security Study, 2003

** Source: Gartner Research, 2004

To mitigate and prevent information theft, organizations must adapt to a new security paradigm based upon explicit trust rather than implicit trust. No longer can all employees be considered trusted users on the network. To begin implementing this new view of user trust, organizations must:

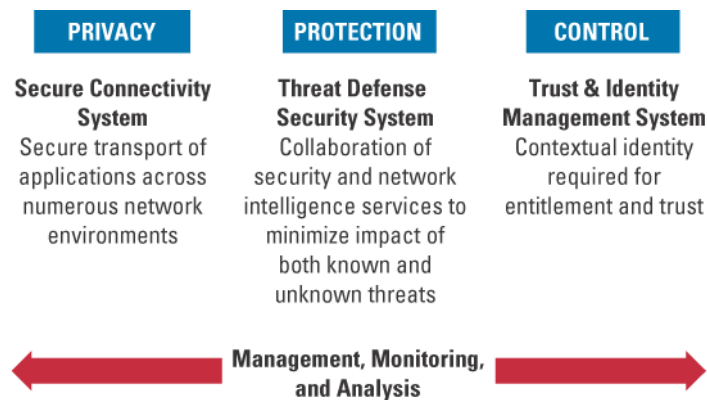
- Establish and adhere to a formal organizational security policy or set of policies
- Challenge the user to validate they are trusted
- Grant and enforce access rights and privileges to trusted, authenticated users
- Protect network endpoints (desktops, servers, and laptops, for example) against infiltration
- Protect network resources against internal and external attacks (routers, switches, and wireless access points, for example)
- Secure the transport of data and voice communications to help ensure privacy and confidentiality of the trusted users

THE CISCO SELF-DEFENDING NETWORK STRATEGY

Information theft often occurs without network or security personnel suspecting it. Therefore, security systems must react quickly and automatically to suspicious network behavior. A security system must be fully integrated into all aspects of the network, so that the network and its managers can proactively recognize suspicious activity, identify if the threat is real, react appropriately and quickly to the theft attempt. The Cisco Self-Defending Network strategy outlines comprehensive theft of information protection. Organizations can use their existing investments in routing, switching, wireless, and security platforms to deploy a self-defending network that will help them identify, prevent, and adapt to security threats originating both inside and outside of the organization. Only Cisco offers a unique, systemic approach to business security based on the intelligent collaboration of networking and security technologies and services.

The Cisco Self-Defending Network strategy consists of three security disciplines, each with a specific purpose (Figure 1). These systems work together to identify and block attempts to steal organizational information.

Figure 1. Components of the Cisco Self-Defending Network



Cisco Secure Connectivity System

In any organization, privacy is an important consideration. Users expect that their phone and computer communications are private, and not accessible by unauthorized individuals. Through virtual private networks (VPNs), the Cisco Secure Connectivity System thwarts theft of data, video, and voice over IP (VoIP) communications by protecting the integrity and confidentiality of information traveling over public and private networks.

Cisco Threat Defense System

Networks must be able to resist both external and internal attacks. To prevent theft of information, the Cisco Threat Defense System guards against malicious activity targeted at endpoints such as desktops and servers, and intelligently detects, identifies, and blocks suspicious behavior anywhere on the network.

Cisco Trust and Identity System

The first line of defense in a network infrastructure is to determine who or what is accessing the network, the state of the accessing device, and what its resource privileges and rights are. The Cisco Trust and Identity System inhibits theft of information by helping to ensure that only trusted users and trusted devices can connect to an organization's network, and that trusted users and resources can retrieve only the information they are entitled to access.

PREVENT INFORMATION THEFT FROM EXTERNAL SOURCES

Information theft has been occurring for a long time. With the sophistication of the Internet, however, information can be stolen from outside the company's doors. There are numerous ways to accomplish information theft from outside and inside an organization or network. For example, hackers can attempt to intercept information going across public networks through what are commonly known as "man-in-the-middle" attacks. Or, they can infiltrate corporate computers with malicious software that open "back doors" into servers and desktops. With the prevalence of wireless LANs in campus environments, they can loiter outside corporate buildings looking for unsecured wireless access points. Cisco integrated security solutions provide a multifaceted approach to securing the network from threats outside the organization.

Verify Trusted Users and Access Privileges

The first step in securing a network environment is to verify the identity and connectivity privileges of users. The Cisco Trust and Identity System validates the identity of a user through standard authentication protocols and technologies such as 802.1X and authentication, authorization, and accounting (AAA) capabilities integrated into Cisco Catalyst® switches and routers. Once a user identity is verified, access privileges can be granted. The Cisco Secure Access Control Server (ACS) governs policy control for network access. Via Cisco Secure ACS, network managers can control user access to different network segments, authorize different types of network services for users or groups of users, and keep an accounting record of all user actions in the network.

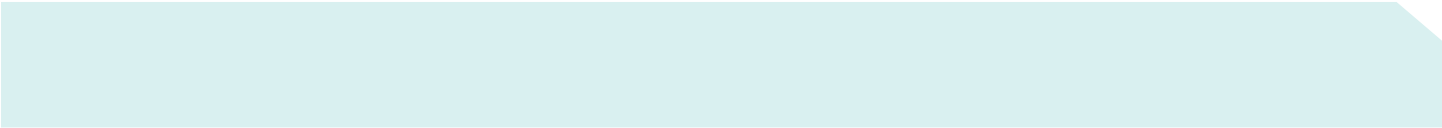
Verify Trusted Devices

Before gaining access to the network, the device needs to be checked for compliance of the security policy for endpoints. The Cisco Network Admission Control (NAC) solution compares the device's system status against the security policy. Working with industry partners such as Trend Micro and IBM, the network intelligently determines whether the endpoint is compliant with established security policies and gains access to the network or not.

Secure Public Networks Carrying Private Information

Remote access and teleworking are a boon for business productivity, but they put network operators in the position of having to allow corporate network access across a public network. The Cisco Secure Connectivity System helps to ensure privacy for information transported across insecure networks.

Cisco Remote Access VPN solutions extend the privacy of the corporate network to branch offices and remote workers via Secure Sockets Layer (SSL) or IP Security (IPSec) standards. These solutions provide the highest security user authentication and data encryption standards—only valid users can access the network. The data is unintelligible to anyone intercepting the communications.



The Cisco VPN client is a software application, compatible with a large range of operating systems that enables secure connectivity for remote-access VPNs, including support for e-commerce, mobile user, and telecommuting applications. It is supported across most Cisco headend platforms, including Cisco routers, Cisco VPN 3000 Series Concentrators, and Cisco PIX[®] Security Appliances.

Keep Intruders Out

Hackers commonly scan corporate networks for vulnerable entry points and devices before attempting to gain access. Next, they try to penetrate the network by modifying traffic of common applications, such as HTTP traffic with Web applications. Network-based intrusion detection and prevention systems (IDSs/IPSs) analyze all traffic traversing the network, recognize when a scan is occurring, identify the attack pattern, and react to stop the threat. This will often deter a hacker from attempting to infiltrate the network further.

Cisco's comprehensive family of IPS solutions includes software features embedded in routers, switches, and wireless access points; dedicated, high-performance hardware modules for Cisco Catalyst switches; and standalone, powerful appliances. Cisco IPS solutions provide unsurpassed threat protection for small office, branch office, and enterprise networks.

Secure the Airwaves

Organizations have embraced wireless LAN technology as a convenient and cost-effective solution for campus networking environments. Unfortunately, wireless networks can be easy to access. While most wireless networks use 802.1X user authentication and static data encryption for secure wireless networks, there are a few common wireless security breaches.

Whether by design or ignorance, wireless access points can be improperly installed, allowing network access to unauthenticated users. These "rogue" access points can be discovered instantly using IDS-like features within the Cisco Structured Wireless-Aware Network (SWAN) architecture. Cisco SWAN, incorporated into access points and Cisco Catalyst 6500 Series modules, pinpoints the location of any rogue access point so that network managers can easily identify and disable it.

Current wireless static encryption keys can be broken using publicly available hacking tools. Cisco wireless solutions use the Wi-Fi Protected Access (WPA) industry standard, which incorporates a temporary key encryption solution. Cisco wireless solutions help ensure that wireless networks are just as secure as wired networks. With Cisco SWAN and Cisco Catalyst 6500 Series switches, wired and wireless networks are fully secure and integrated, enabling simplified configuration, management, and security policy enforcement.

PREVENT INFORMATION THEFT FROM WITHIN

Most organizations invest heavily in physical security for their buildings—locks on doors, cardkey passes, even video surveillance and security guards. These do deter many intruders, but some manage to penetrate these defenses, often by simply following employees into the building. Information theft can also be perpetrated by employees or other trusted insiders. A multilayered defense system effectively deters unauthorized employees, contractors, or visitors from accessing and stealing corporate information.

Create "Islands" of Security

While firewalls play an essential role in protecting the network from external intruders, they also have a valuable role within the network. Firewalls are the locked door and cardkey access between network groups, creating "islands" of security within the network. Firewalls can block users in one group from accessing resources in another network group. For example, partners and suppliers on an extranet can be prevented from accessing sensitive information in finance, human resources, and accounting.

Cisco has the broadest range of complete firewall capabilities in the industry, appropriate for networks of any size. Firewall features are embedded in all Cisco routers and Cisco Catalyst switches. For high-performance applications, firewall hardware modules are available for Cisco Catalyst switches. A family of powerful standalone Cisco firewalls—provided via the PIX Security Appliances - protects home office, branch office, campus, and data center environments.

Secure User Workgroups

Cisco Trust and Identity System solutions can segment users into different workgroups or virtual LANs (VLANs) based on who they are, not where they are. For example, campus and branch office organizations may want to offer Internet access to visitors without compromising corporate security. Network operations staff can create a guest VLAN, where visitors are virtually segmented from the rest of the corporate network and granted only Internet access. VLANs can also be used to segment different organizational functions. For example, only users authenticated and identified as marketing staff could have access to marketing servers on the marketing VLAN. VLAN capabilities are integrated into all Cisco Catalyst switches.

Stop Spying, Snooping, and Spoofing

Trusted employees with valid authentication and login access can use publicly available software to “spy” on employee data traversing the network, including IP phone calls and passwords. Malicious applications can also be unknowingly added to desktops, laptops and servers—via worms and ‘trojan’ applications—to spy on and steal corporate information such as passwords, account numbers and employee information. Other tools can attempt to “spoof” the network into thinking that User A is User B, in order to gain access to User B’s information. Cisco Catalyst Integrated Security offers a broad range of embedded security mechanisms that protect against these types of attacks. Stealing can be prevented or, if a theft attempt is underway, it can be mitigated quickly and successfully. Integrated Security is a software feature set available in Cisco Catalyst switches. Cisco Security Agent (CSA) can also mitigate spyware within host systems throughout business organizations. When CSA is deployed, users are notified of all software that is downloaded and installed on their systems, as well as notified of any applications that are downloaded and installed that exhibit intrusive behavior like ‘hooking’ the keyboard and opening outbound network connections. Collectively, solutions like CSA and the Catalyst Integrated Security Feature Set mitigate the most common malevolent activity seen within businesses today.

MONITORING AND MANAGING THE SECURITY STATE OF THE NETWORK

In a large, distributed network, a consolidated view of all network devices, security devices, and security services allows IT staff to efficiently monitor the network. With Cisco integrated security, information from all routers, switches, intrusion detection and prevention systems, firewalls, VPN devices, and secured endpoints is collected and analyzed by CiscoWorks Security Information Management Solution (SIMS), which helps security staff quickly identify and respond to threats in a coordinated manner.

Similarly, CiscoWorks VPN/Security Management Solution (VMS) contributes to organizational productivity by combining Web-based tools for configuring, monitoring, and troubleshooting VPNs, firewalls, and network and host IPSs from a central location. Rules and configurations can be globally applied to the network, greatly simplifying deployment of network-wide security policies.

PROTECT YOUR INFORMATION FROM THEFT WITH CISCO SELF-DEFENDING NETWORKS

Information theft is the most costly security breach for organizations today, resulting in a reported average of \$2.7 million in losses *per incident* in 2003 to businesses within the United States*. The total loss is significantly larger than this reported amount, based on worldwide estimates. The consequences of the breaches are tremendous, ranging from productivity losses to financial losses.

With many thefts originating internally, organizations need to secure their networks both inside and out. Cisco integrated security solutions let organizations use their existing investments in network infrastructure and staff expertise to build self-defending networks. A Cisco Self-Defending Network integrates security intelligence into the network, protecting corporate assets while using the existing network infrastructure, containing the total cost of ownership. Operations staff will have better insight into the users that are on a network, where they are, and what information they are trying to access, allowing staff to devote more time to making their networked organizations as efficient and productive as possible.

Cisco is the industry leader in networking and security solutions. Only Cisco offers a unique, systemic approach to business security based on the intelligent collaboration of networking and security technologies and services. Based on three essential pillars of solutions comprising secure connectivity, threat defense, and trust and identity products, Cisco provides the most comprehensive range of integrated security solutions in the industry to best protect all-sized organizations from theft.

For more information on protecting your organization from theft and on the Cisco Self-Defending Network strategy, please visit:

<http://www.cisco.com/go/selfdefend>

* Source: 2004 CSI/FBI Computer Crime and Security Survey



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.
168 Robinson Road
#28-01 Capital Tower
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 • Cyprus • 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

Copyright © 2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Catalyst, and PIX 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 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. (0402R) 204107_ETMG_Rdlc_12.04

Printed in the USA

