



## WHITE PAPER

# PREVENTING WORM AND VIRUS OUTBREAKS WITH CISCO SELF-DEFENDING NETWORKS

**Worm and virus attacks are among the most common security breaches for organizations today\*. A server, laptop, or personal digital assistant (PDA) can be exposed to a worm or virus at any time and easily propagate that worm throughout an organization. In recent years, infections such as MyDoom, Blaster, Sasser, SQL Slammer, and SoBig have disrupted corporate applications, Websites, banks, and airlines, and have shown how vulnerable organizations are to attack. These attacks are increasing in severity, speed, and number, leaving organizations in need of greater security resources. The Cisco® Self-Defending Network strategy allows organizations to protect their assets against current and future worm and virus attacks, using their existing investments in their computing, network, and security infrastructures.**

## THE SECURITY LANDSCAPE

Networked applications have allowed organizations to become more productive and serve clients more effectively. However, the increasing mobility and accessibility of today's global networks bring new security challenges. Wireless access points, employee remote access, and the prevalence of teleworking provide more network entry points for malicious users or code.

Finding and retaining qualified security professionals is challenging. It can be also a struggle for organizations to justify additional security investment. 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.

## OUTBREAK PREVENTION CHALLENGES

Worms, viruses, and "flash" outbreaks are an increasing security problem for organizations. These attacks can cost organizations more than lost sales and employee productivity. Some worms and viruses can open "back doors" into personal computers to enable theft of information, or use infected computers as "zombies" to propagate more viruses, spam, or other attacks. For example, many worms currently in circulation are designed to generate distributed denial of service (DDoS) attacks on unsuspecting organizations.

Security threats are constantly changing, requiring defenses to adapt and change with them. As network connectivity becomes more pervasive and bandwidth increases, the spread of worms and viruses can happen at a faster pace, further compounding the problem. For example, the Blaster/Lovsan worm infected more than 1.4 million hosts worldwide, with 138,000 infected within four hours of its release\*\*.

Conventional, up-to-date antivirus software installed on personal computers and servers does a good job of preventing known worms and viruses, but new or unknown ("day zero") attacks can penetrate these defenses. Further, in large campus environments or distributed organizations, it is difficult to ensure that all computers have the latest antivirus software or other software security patches. Distributing and downloading software patches can be laborious and time-consuming for network operations staff. Testing and verification must take place, to make sure these patches do not adversely affect other business critical programs. In the meantime, their networks are vulnerable to attack. A recent study\*\*\* predicted that through 2005, 90 percent of cyberattacks will exploit security flaws for which a patch is available or a solution is known. Having antivirus software is a good start, but is not enough.

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

\*\* Source: Hackerwatch.org

\*\*\* Source: GartnerG2 Research, 2002

Finally, it is difficult to control human curiosity. Many worms or viruses are still spread by users accessing malicious Websites, downloading untrustworthy material, or opening malicious e-mail attachments. These attacks, while unintentional, still result in significant financial and productivity losses to organizations. It is important for IT managers to educate their employees and users on the value of adhering to security policies and processes.

To effectively avoid disruptions caused by worm or virus outbreaks, organizations must:

- Protect network endpoints (desktops, servers, and laptops, for example) from attack
- Prevent infections from spreading through the network infrastructure
- Monitor and manage their networks in an efficient, comprehensive manner in order to respond rapidly to outbreaks.

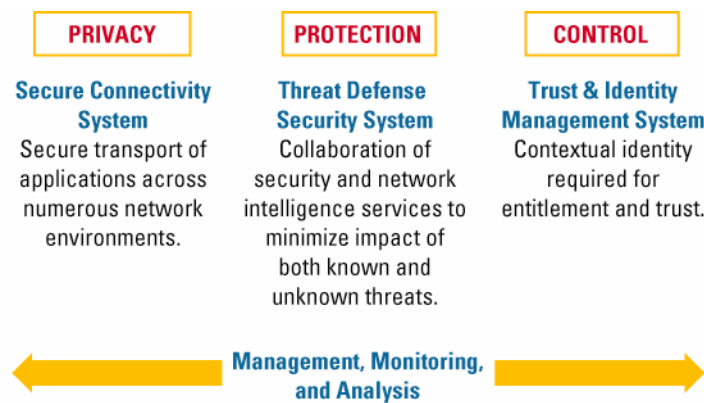
Achieving these goals requires a global systems-based view of network security, where every device connected to the network plays a role in securing the network from unwanted intrusions.

### THE CISCO SELF-DEFENDING NETWORK STRATEGY

Worms and viruses can spread across the world in a matter of minutes or seconds. Security systems must therefore react instantly and automatically. A security system that is fully integrated into all aspects of the network can proactively identify threats, quarantine infections, and facilitate a coordinated response to attacks. The Cisco Self-Defending Network strategy is Cisco’s vision for integrated network security. 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 both known and unknown security threats. Only Cisco Systems 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 has three components (Figure 1). Out of these components, the Cisco Threat Defense System and the Cisco Trust and Identity System specifically work together to effectively repel outbreaks.

**Figure 1.** Components of the Cisco Self-Defending Network



### Cisco Threat Defense System

Networks must be able to recognize and resist both external and internal attacks, and to recover quickly if an attack is launched. To prevent outbreaks, the Cisco Threat Defense System integrates endpoint and network protection to identify attacks and stops them from propagating throughout the network.

## **Cisco Trust and Identity System**

The first line of defense in an organization's network infrastructure is to determine who or what is accessing the network, the state of the accessing device, and what resources it should have access to. The Cisco Trust and Identity System provides network access and security policy control, to ensure that only trusted users, and devices adhering to corporate security policy, can connect to an organization's network and send and receive data.

## **PROTECT THE ENDPOINTS**

Worms and viruses attack applications running on desktops, servers, and other endpoints. While antivirus and personal firewall software is effective against threats with recognizable "signatures", it is often not enough. Cisco Security Agent uses behavior-based assessment to identify and prevent malicious or anomalous behavior on endpoints. It analyzes system behavior, and can eliminate both known and unknown security risks based on this behavior. Cisco Security Agent aggregates multiple security functions by providing host intrusion prevention, distributed firewall capabilities, malicious mobile code protection, operating system integrity assurance, and audit log consolidation—in a single, powerful software package. All Cisco Security Agent policies and activities are easily configured and monitored from a central location through the CiscoWorks VPN/Security Management Solution (VMS).

## **What Computers Bring into a Network**

Laptops and remote-access virtual private networks (VPNs) have made business travelers more productive. At the same time, they increase the challenges facing network and security operations staff. For example, while working away from the office, a business user may find it cumbersome to download large antivirus updates or operating system patches. Hotels, airports, and coffee houses may have insecure wireless access points, allowing infected computers to pass worms or viruses along. When the business user connects to the corporate network, the infection propagates throughout the company.

Network Admission Control (NAC) is an industrywide collaboration led by Cisco that focuses on limiting damage from security threats such as viruses and worms. Using NAC, organizations can allow network access only to compliant and trusted endpoint devices and can restrict the access of noncompliant devices. Currently, NAC enables Cisco routers to enforce access privileges when an endpoint device attempts to connect to a network. This decision can be based on information about the endpoint device such as its current antivirus state and operating system patch level. NAC allows noncompliant devices to be denied access, placed in a quarantined area, or given restricted access to computing resources.

## **LIMIT THE SPREAD OF INFECTION**

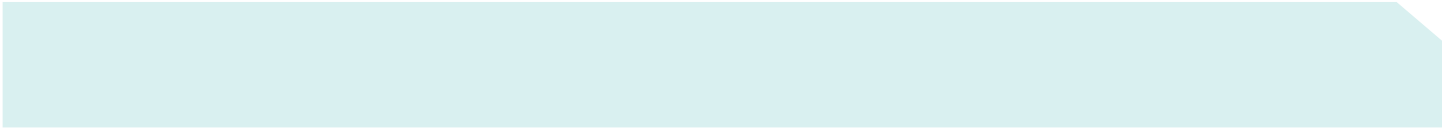
Sometimes, despite an organization's best efforts, a worm or virus gains entry to a network. Since today's viruses and worms spread so quickly, an automated and rapid response is required. This is only possible with integrated security capabilities woven into the very fabric of the network.

### **Raise the Alarm**

Without instant outbreak identification and reaction, a network can be brought down in minutes. Cisco network-based intrusion detection and prevention systems (IPSs) accurately identify, classify, and stop malicious traffic in real time. Cisco IPS intelligence analyzes all traffic traversing the network, recognizes an attack, analyzes its severity, raises appropriate alarms to network managers, and takes corrective action. For example, a Cisco IPS-equipped branch office router (such as a Cisco 2800 Series router) would recognize a MyDoom attack as it attempted to enter the network. It would block it and simultaneously issue alerts.

### **Segment the Network into "Islands" of Security**

Firewalls are traditionally used on the perimeter of an organization's network—such as an Internet connection—to prevent malicious or unnecessary traffic or users from entering. They are equally useful in protect the network interior. Firewalls can be configured to recognize and block many known worms, and to block ports that should not be used on particular network segments. During a worm or virus attack, firewalls prevent the spread of infection by segmenting the internal network into "islands" of security and controlling connectivity to network resources on particular islands. For



example, a SQL Slammer worm attempting to get to a campus Web server beyond an internal firewall will not succeed if the firewall is configured to allow only Web traffic.

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.

### **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 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 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.

### **PREVENT YOUR NETWORK FROM OUTBREAKS WITH THE CISCO SELF-DEFENDING NETWORK**

Organizations need to avoid the disruption caused by outbreaks, while controlling the costs of deploying and maintaining a secure network. Cisco integrated security solutions allow an organization to maximize the security utility of its existing network infrastructure and build a truly self-defending network. A Cisco Self-Defending Network uniquely integrates security intelligence into the network, protecting corporate assets while reducing the total cost of ownership. Security and network operations staff can spend less time reacting to and cleaning up virus and worm outbreaks, and spend more time making their networked organizations as efficient, productive, and safe 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. With threat defense and trust and identity solutions, Cisco provides the most comprehensive range of integrated security solutions in the industry to best protect all-sized organizations from devastating outbreaks due to worms and viruses.

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

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

**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](http://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. Catalyst, Cisco, Cisco Systems, and the Cisco Systems 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 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\_RdIC\_12.04

Printed in the USA

