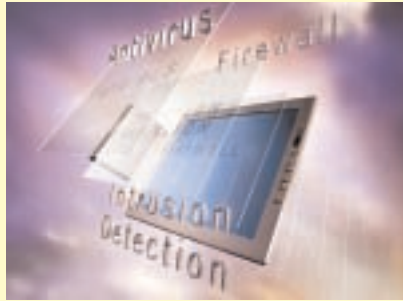
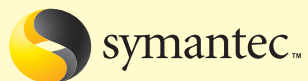


## Symantec™ Client Security

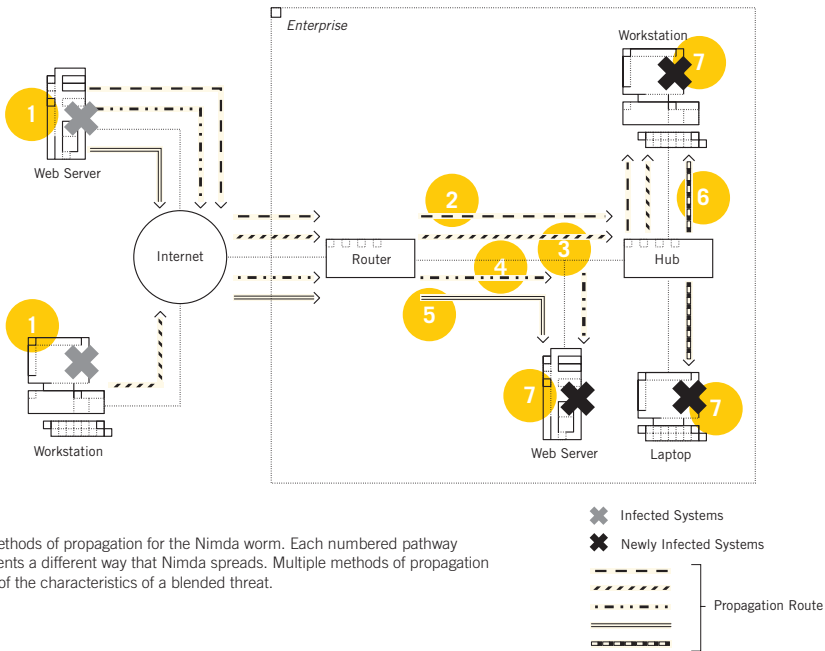


**Integrated protection for  
network and remote clients.**



# Complex Internet threats require comprehensive security.

Today's complex threats require comprehensive security solutions that provide multiple layers of defense and response at each network tier, including at the client level. For better protection, solutions should be able to apply multiple security functions in a synergistic, efficient and cost effective fashion.



The methods of propagation for the Nimda worm. Each numbered pathway represents a different way that Nimda spreads. Multiple methods of propagation is one of the characteristics of a blended threat.

- 1 **✕**  
**INFECTED SYSTEMS — ATTACK PREPARATION**  
 Nimda-infected systems scan for and exploit vulnerable systems on the LAN and Internet.

- 2 **---**  
**INFECTED BY BROWSING COMPROMISED IIS WEB SERVER**  
 Any vulnerable IE browsers contacting compromised web servers become infected.

- 3 **.....**  
**HOSTILE EMAIL ATTACHMENT**  
 Infected Nimda systems open the system's email address book and sends an email file attachment to each address. Users which preview or open the attachment become infected.

- 4 **-.-.-.-**  
**EXPLOIT VULNERABLE IIS WEB SERVER**  
 Nimda infected systems scan for and compromise IIS web servers on the LAN or Internet through unpatched IIS vulnerabilities.

- 5 **=====**  
**PREVIOUSLY COMPROMISED WEB SERVERS**  
 Nimda infected systems scan for and compromise IIS web servers on the LAN or Internet by using a backdoor left by Code Red II.

- 6 **-----**  
**FILE SHARES**  
 Nimda infected systems scan for systems which have world writable network shares on the LAN. Vulnerable systems are then compromised.

- 7 **✕**  
**NEWLY INFECTED SYSTEMS**  
 Newly infected systems prepare and carry out all the attacks mentioned above against any targets visible to them on both the LAN and Internet. The process continues exponentially.

## **Symantec Client Security: Integrated antivirus, firewall, and intrusion detection for the client.**

THE COMPLEXITY OF THREATS AGAINST IT INFRASTRUCTURES IS GROWING. FOR EXAMPLE, BLENDED THREATS, SUCH AS NIMDA AND CODE RED, COMBINE THE CHARACTERISTICS OF VIRUSES, WORMS, TROJAN HORSES, AND/OR MALICIOUS CODE TO EXPLOIT VULNERABILITIES TO INITIATE ATTACKS. TO COMBAT THESE THREATS, NETWORK ADMINISTRATORS ARE DEPLOYING MULTIPLE SECURITY PRODUCTS SUCH AS ANTIVIRUS SOFTWARE AND FIREWALLS, TO NETWORK AND REMOTE CLIENTS. HOWEVER, THE STRATEGY OF SEPARATELY DEPLOYING, INSTALLING, MANAGING, AND UPDATING INDIVIDUAL SECURITY PRODUCTS CAN RAISE IT ADMINISTRATION AND SUPPORT COSTS. TO BETTER PROTECT AGAINST TODAY'S COMPLEX INTERNET THREATS, ENTERPRISES NEED A MANAGEABLE SOLUTION THAT INCLUDES A COMPREHENSIVE RANGE OF SECURITY TECHNOLOGIES, WITH INTEGRATED MANAGEMENT AND RESPONSE TO THREATS.

SYMANTEC CLIENT SECURITY DELIVERS INTEGRATED SECURITY PROTECTION FOR NETWORK AND REMOTE CLIENTS. IT PROVIDES BETTER PROTECTION AGAINST COMPLEX INTERNET THREATS THROUGH INTEGRATED MANAGEMENT AND RESPONSE OF FIREWALL, INTRUSION DETECTION, AND ANTIVIRUS TECHNOLOGIES. THIS APPROACH EASES THE ADMINISTRATIVE BURDEN, ENABLES QUICK RESPONSE TO THREATS AT THE CLIENT TIER, AND HELPS REDUCE OVERALL SECURITY COSTS.

# Integrated Security

## Comprehensive protection, integrated management, fast response.

Symantec Client Security brings multiple technologies together to enable more efficient management of client security across an enterprise, as well as updates of firewall rules, intrusion detection signatures, and virus definitions with a single update package. If an outbreak occurs, Symantec tests and verifies its solution across the integrated technologies – firewall, intrusion detection, and antivirus. Protection is comprehensive, and cross-vendor interoperability issues do not compromise security, since the IT staff is not required to resolve multiple vendor product issues.

### **Symantec Client Security combines integrated protection and management, client security policy enforcement, and proven technologies.**

INTEGRATED PROTECTION. Integrated firewall, intrusion detection, and antivirus protection help provide a significantly higher level of protection for the client by scanning all traffic for viruses, worms, Trojans, unauthorized intrusions, and firewall rule infractions.

#### **Symantec Client Security**

Firewall  
Intrusion Detection  
Antivirus

**CENTRALIZED MANAGEMENT AND RESPONSE**



INTEGRATED MANAGEMENT. Symantec Client Security includes Symantec's proven management infrastructure, Symantec System Center (SSC). With SSC, administrators can configure, deploy, manage policy, and update client firewall, intrusion detection, and antivirus functions from one management console.

CLIENT SECURITY POLICY ENFORCEMENT.

- Incoming and outgoing traffic is scanned against firewall rules. Firewall technology within Symantec Client Security works seamlessly with antivirus technology to protect the client from viruses, even if the administrator or user has configured real-time virus protection technology in the "off position."
- Through integration of client firewall and intrusion detection technologies, scanning and comparing all incoming and outgoing traffic with known intrusion threats enables an offending IP address to be blocked for up to 30 minutes if an intrusion attempt is detected.

INCORPORATION OF LEADING TECHNOLOGIES. Symantec Client Security is based on proven antivirus, firewall, and intrusion detection technologies.

- Digital Immune System™ automates the submission of virus threats and automatically delivers cures to the problem machine or the entire enterprise.
- Award-winning client firewall and intrusion detection technologies protects against unauthorized intrusions, unauthorized port scans, and limits the propagation of threats throughout the network by blocking suspect inbound and outbound traffic.

COMMON DEPLOYMENT AND UPDATING MECHANISM. The Symantec System Center enables the centralized deployment of virus definitions, firewall updates, and intrusion detection signatures to multi-platform workstations, significantly reducing the cost of deploying updates across the enterprise. Centralized distribution reduces deployment headaches, such as "sneaker nets," failed jobs, and bad installations.

# World-Class

## WORLD-CLASS SERVICE AND SUPPORT

Symantec Client Security achieves lower cost of ownership through single-vendor service and worldwide support for all integrated security functions. With around-the-clock vigilance from Symantec Security Response and Symantec's exclusive LiveUpdate™ technology, new threats can be identified and the latest virus definitions, firewall updates, and intrusion detection signatures can be made available within hours to prevent further security events. LiveUpdate ensures that each integrated security function is automatically updated – with no administrative intervention required.

## ADVANCED THREATS REQUIRE INTEGRATED PROTECTION

That's the thinking behind Symantec's integrated security products. For more information about Symantec Client Security please visit <http://enterprisesecurity.symantec.com>.

## **Enterprise-class protection at the client and beyond: That's the mission of Symantec Enterprise Security.**

# Service

Internet security doesn't stop at the client. Symantec Enterprise Security provides a complete set of technologies and services that can be configured in a variety of ways to meet the unique security requirements of any organization. Combining enterprise-class security products, world-class consulting and support, and rapid global response, Symantec Enterprise Security delivers the resources and flexibility you need to manage and minimize security risks in order to protect your business.

**SYMANTEC SECURITY SERVICES.** Symantec's complete service offering helps organizations develop strategies for managing and reducing risks. The consulting services group provides insights that enable organizations to implement best-practices security measures across the enterprise through comprehensive assessments, planning, and design. For turnkey, out-sourced solutions, Symantec Managed Security Services offers management, monitoring and response services that solve security challenges efficiently and cost-effectively.

**SYMANTEC SECURITY RESPONSE.** Through a global technical research and support organization, Symantec Security Response helps keep security systems optimized and effective in the face of the latest security threats. When new threats or vulnerabilities are discovered, Symantec Security Response experts provide rapid emergency response, delivering security updates and support to Symantec customers 24 hours a day.

**SYMANTEC, THE WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOFTWARE AND APPLIANCE SOLUTIONS TO INDIVIDUALS, ENTERPRISES, AND SERVICE PROVIDERS. THE COMPANY IS A LEADING PROVIDER OF CLIENT, GATEWAY AND SERVER SECURITY SOLUTIONS FOR VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY MANAGEMENT, INTRUSION DETECTION, INTERNET CONTENT AND E-MAIL FILTERING, REMOTE MANAGEMENT TECHNOLOGIES AND SECURITY SERVICES TO ENTERPRISES AND SERVICE PROVIDERS AROUND THE WORLD. HEADQUARTERED IN CUPERTINO, CALIFORNIA, SYMANTEC HAS WORLDWIDE OPERATIONS IN 38 COUNTRIES.**

Symantec Corporation  
World Headquarters  
20330 Stevens Creek Boulevard  
Cupertino, CA 95014 U.S.A.  
408 517-8000  
800 721-3934  
[www.symantec.com](http://www.symantec.com)

For Product Information in the U.S., call toll-free 800 745-6054.

Symantec has worldwide operations in 38 countries.

For specific country offices and contact numbers please visit our Web site.

