

# Symantec™ Control Compliance Suite for Internet Security

Maintain compliance with comprehensive identification of security risks on servers, workstations, and other enterprise devices throughout the entire environment

---

## Overview

Control Compliance Suite for Internet Security helps you maintain control of the shifting changes in your business network that can leave your organization exposed to both internal and external risks. Today, ensuring compliance in an organization is made more difficult by the variety of security issues and the need to comply with multiple external regulations. Recent research indicates that companies investing in one-off solutions for each regulatory challenge they face will spend significantly more on IT compliance than those that develop a single solution to manage multiple regulatory requirements.

With the complexity of today's business-critical infrastructure, it is difficult for administrators, security professionals and auditors to identify all the IP devices in their organization. Nor is it easy to locate rogue servers, verify all configurations, or identify which Web servers are vulnerable to CGI exploits. You want to be able to assess every device, track and monitor rogue machines, and to have the ability to patch systems at any given point. Furthermore, it's not enough to have tools that require credentials to check for vulnerabilities. To protect your infrastructure, it's important to be aware of what hackers may already know about your network.

Control Compliance Suite for Internet Security delivers these capabilities in a single product. Using high-speed, non-intrusive scanning, CCS for Internet Security looks

at every managed or unmanaged device connected to the network - from servers, desktops and workstations, to firewalls, hubs, routers - searching for potential problems, identifying possible at-risk devices and facilitating the remediation of non-compliant systems.

---

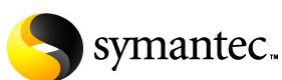
## Key features and benefits

### *Efficiently assess and secure multi-platform environments*

- Scans at every managed or unmanaged device connected to a network including servers, desktops, firewalls, hubs, and routers
- Uses non-credentialed vulnerability checks to offer an outside-in view of the network
- Customizes bandwidth usage to minimize network load
- Schedules scans to run at times that are optimal for your network

### *Provides rich, consolidated reports of vulnerabilities in an environment*

- Produces reports that detail existing vulnerabilities and required remediation
- Customizes reports to set exclusions and adjust risk levels



### **Key features and benefits - continued**

#### *Secures against the latest vulnerabilities*

- Provides 800 vulnerability checks defined by the elite Symantec RAZOR team of security experts
- Updates checks on a regularly scheduled basis through RapidFire Updates®
- Scans for vulnerabilities that could allow for debilitating Denial of Service (DoS) attacks
- Remediates common Microsoft vulnerabilities with auto-fix capability

#### *Helps manage and remediate rogue devices*

- Utilizes a Network Mapper and Nmap® Fingerprint Database, the most complete database of OS TCP/IP fingerprints available, to quickly discover and tag all devices
- Checks for available host, services of ports that are offered by the host, and operating systems that are running
- Checks for packet filters or firewalls that are operating

#### *Simplifies vulnerability checking*

- Ability to add comments to individual check details—from company specific vulnerability notes to verbiage describing a particular check in your environment
- Uses keyword search on any information included in the check details, such as CVE numbers or user annotations, to quickly find specific checks or information about a particular vulnerability

*Integrates with Symantec Bindview™ Policy Manager to provide proof of security configuration compliance with broader corporate policy*

- Provides a single compliance architecture for managing multiple regulations, by integrating with Symantec Bindview Policy Manager
- Reduces the cost of compliance by automating the assessment of IT policies against industry regulations and best practices

---

### **Endorsements**

Best Policy Monitor: 2004 Network Computing  
Well-Connect Awards

Best Policy Management Solution: 2004 SC Magazine  
Global Awards

2003 Network Computing Editor's Choice Award

IDC White Paper: "Optimizing Your IT Controls  
Environment for Compliance with Multiple Regulations,"  
by Charles Kolodgy, December 2005

## System requirements

### *Symantec Control Compliance Suite for Internet Security*

- Pentium® II 450 MHz
- 512 MB RAM and 300 MB of free disk space
- SVGA monitor that supports 256 colors with the display set to 800 x 600 pixels or greater
- Microsoft® Windows® 2000 SP3 (server or workstation), Windows XP® Professional SP1, or Windows Server™ 2003 or later
- Microsoft® Internet Explorer v5.5 SP1 or later
- Microsoft Outlook® 2000, Novell® GroupWise® v5.5, Lotus Notes® v5.0 or Lotus Domino® (only required for emailing export files)
- Microsoft® Excel (required for Excel, using OLE, export files)
- Client for Microsoft® Networks

## More information

### *Visit our web site*

<http://enterprise.symantec.com>

### *To speak with a Product Specialist in the US*

Call toll-free (800) 745-6054

### *To speak with a Product Specialist outside the US*

Symantec has operations in 40 countries. For specific country offices and contact numbers, visit our web site.

### *About Symantec*

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at [www.symantec.com](http://www.symantec.com).

### *Symantec World Headquarters*

20330 Stevens Creek Blvd.

Cupertino, CA 95014 USA

(408) 517-8000

(800) 721-3934

[www.symantec.com](http://www.symantec.com)

