

## Cisco Security Agent Version 5.0

Cisco® Security Agent endpoint security software provides a critical line of defense to protect systems against new and unknown attacks. Through market-leading endpoint and network integration, Cisco Systems® offers its customers the most comprehensive security threat protection solution for securing corporate networks.

Cisco Security Agent security software provides threat protection for server and desktop computing systems, also known as endpoints. The Cisco Security Agent goes beyond conventional endpoint security solutions by identifying and preventing malicious behavior before it can occur, thereby removing potential known and unknown security risks that threaten enterprise networks and applications. Because the Cisco Security Agent analyzes behavior rather than relying on signature matching, its solution provides robust protection with reduced operational costs.

### Benefits

The Cisco Security Agent provides numerous benefits, including:

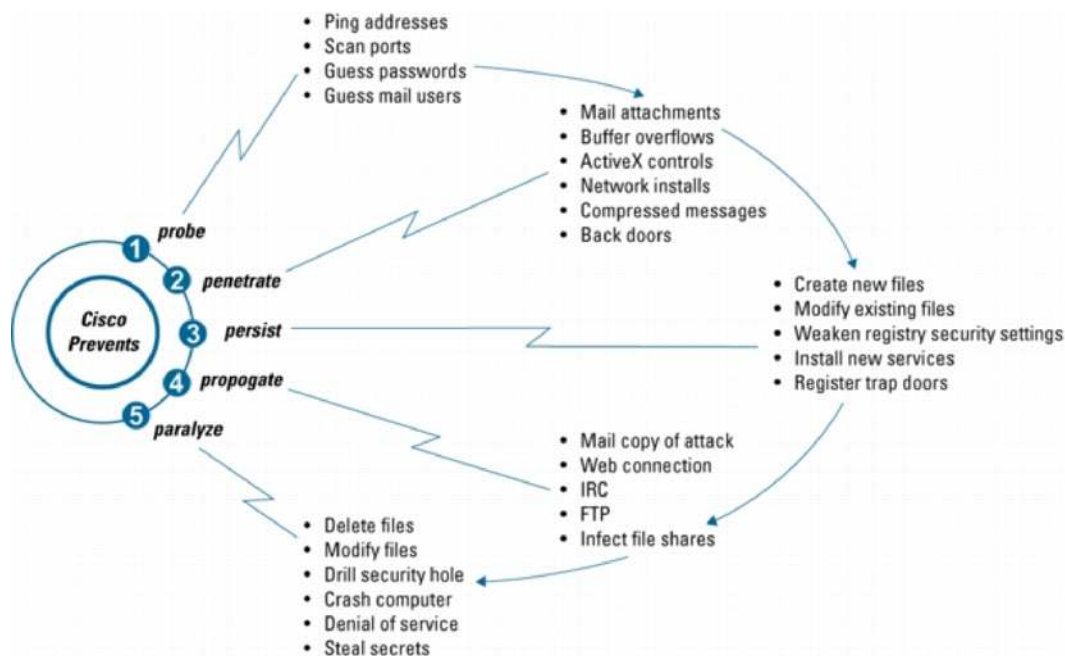
- The ability to aggregate and extend multiple endpoint security functions—the Cisco Security Agent provides host intrusion prevention, distributed firewall, malicious mobile code protection, operating system integrity assurance, and audit log consolidation, all within a single agent
- Integrates with Cisco network IPS devices to increase the effectiveness of identifying attacks within the network
- Preventive protection against entire classes of attacks, including port scans, buffer overflows, Trojan horses, malformed packets, malicious HTML requests, and e-mail worms
- “Zero update” prevention for known and unknown attacks
- Industry-leading protection for servers and desktops, Unix and Windows
- Application-specific protection for web servers and databases
- An open and extensible architecture with the ability to define and enforce security according to corporate policy
- An enterprise scalable architecture—the Cisco Security Agent is scalable to 100,000 agents per manager
- Integrated solution architecture with Cisco Network Admission Control (NAC)
- Integration with Cisco VPN via the “Are You There” (AYT) feature

### Combating New and Unknown Attacks

High-visibility threats like Zotob and the Windows WMF vulnerability have shown that traditional technologies are limited in their ability to combat the effects of new and evolving attacks. Customers require host security that protects throughout all stages of an attack and that provides important protection against new and unknown threats.

Because assaults on network systems typically go through stages, a layered approach is the only effective strategy against these attacks, which can occur beyond the perimeter, at the server, or at the file level. The Cisco Security Agent proactively defends against damage to a host throughout all stages of an attack, whereas other technologies provide early stage protection—and only when a signature is known. The Cisco Security Agent is specifically designed to protect against new attacks where there is no known signature.

**Figure 1.** Lifecycle of an Attack



## The Cisco Security Agent Solution

The Cisco Security Agent consists of host-based agents, deployed on mission-critical desktops and servers, that report to the Management Center for Cisco Security Agents. The Management Center runs on the CiscoWorks VPN and Security Management System (VMS). The agents use HTTP and 128-bit Secure Sockets Layer (SSL) for the management interface, and for communication between agents and the Management Center. Configuration is performed via CiscoWorks VMS, and alerts can be integrated with alerts from other Cisco security products via the Cisco Security Monitoring, Analysis, and Response System.

## Agent Architecture

The Cisco Security Agent resides between the applications and the kernel, enabling maximum application visibility with minimal impact to the stability and performance of the underlying operating system. The software's unique architecture intercepts all operating system calls to file, network, and registry sources, as well as to dynamic run-time resources such as memory pages, shared library modules, and COM objects. The agent applies unique intelligence to correlate the behaviors of these system calls, based on rules that define inappropriate or unacceptable behavior for a specific application or for all applications. This correlation and subsequent understanding of an application's behavior is what allows the software—as directed by the security staff—to prevent new intrusions.

When an application attempts an operation, the Cisco Security Agent checks the operation against the application's security policy, making a real-time allow or deny decision on its continuation and determining if logging the request is appropriate. Security policies are collections of rules that IT and/or security administrators assign to protected servers and desktops individually or across an enterprise. These rules provide safe application access to required resources. By combining security policies implementing distributed firewall, operating system lockdown and integrity assurance, malicious mobile code protection, and audit event collection capabilities in default policies for servers and desktops, the Cisco Security Agent provides defense-in-depth protection for exposed corporate systems.

Because protection is based on blocking malicious behavior, the default policies stop both known and unknown attacks without needing updates. Correlation is performed both on the agent and the Management Center console. Agent-based correlation results in dramatically increased accuracy, identifying actual attacks or misuse without blocking legitimate activity; correlation on the Management Center identifies global attacks such as network worms or distributed scans.

### **Centralized Management**

The Management Center for Cisco Security Agents provides all management functions for all agents in a centralized manner, from the CiscoWorks VMS platform. Its role-based, web browser, "manage from anywhere" access makes it easy for administrators to create agent software distribution packages, create or modify security policies, monitor alerts, or generate reports. The Management Center ships with more than 20 fully configured default policies, making it easy for administrators to deploy thousands of agents across the enterprise. It also allows customers to deploy agents in "IDS mode", where activity is alerted but not blocked.

The Management Center offers simple but powerful customization capabilities such as a tuning wizard, allowing administrators to quickly fit default policies to their environments. Administrators can easily modify rules or create entirely new rules to meet custom needs and requirements. To aid audit compliance requirements, the Explain Rules feature allows the administrator to print out a human-language description of the function of specified rules or policies.

Agents are deployed to servers and desktops directly from the Management Center, and are controlled and updated from this manager. Each agent operates autonomously—if communication with the manager is not possible (for example, if a remote laptop user has not yet connected via the VPN), the agent continues to enforce the security policy. All security alerts are cached by the agent and uploaded to the manager when communication is restored.

Cisco also offers a suite of analysis reporting tools from the Management Center. The Deployment Analysis feature provides details on which applications are installed across all agents, as well as information about usage of those applications. The Behavior Analysis feature is a comprehensive data analysis tool for custom or unknown applications and environments. It provides detailed reports of application behavior, allowing customers to understand any application, even extremely complex ones that have been highly customized to an individual customer's environment.

### **End-To-End Security Solutions**

Cisco Security Agent is a key component for customers building a Self-Defending Network solution. By investing in endpoint and network components that collaborate with each other, customers can enable new critical security services that are not possible with disparate systems.

Trusted QoS is a new security service that allows customer to protect the data flows of mission-critical applications. With Trusted QoS, Cisco Security Agent can identify and classify critical traffic at the endpoint, before it gets on the network. In collaboration with the network infrastructure, the mission-critical data is given a higher service level as it crosses through the network. This end-to-end application awareness and protection is only possible with an adaptive, collaborative, and integrated solution that incorporates the network and its endpoints.

### System Requirements

The Cisco Security Server Agent supports:

- Windows 2003
- Windows 2000 Server and Advanced Server
- Windows NT v4.0 Server and Enterprise Server (SP 6a)
- Solaris 8 SPARC architecture (64-bit kernel)
- Solaris 9 SPARC architecture (64-bit kernel)
- Red Hat Enterprise Linux 3.0 ES and AS

The Cisco Security Desktop Agent supports:

- Windows NT 4 Workstation (SP 6a)
- Windows 2000 Professional
- Windows XP Professional
- Windows XP Tablet Edition
- Red Hat Enterprise Linux 3.0 WS

The Management Center for Cisco Security Agents on CiscoWorks VMS is available for:

- Windows 2000 Server and Advanced Server (SP 4), English (United States) only

Internationalization (Cisco Security Desktop and Server Agents):

- Support for English (United States) and international (except Arabic and Hebrew) Windows operating systems
- Localized user interface for Windows operating systems running English (United States), Chinese (Simplified), French, German, Italian, Japanese, Korean, and Spanish,
- Support for English (United States) Linux and Solaris operating systems only

Additional details for Cisco Security Agent system requirements can be found in the product release notes.

[http://www.cisco.com/en/US/products/sw/secursw/ps5057/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/sw/secursw/ps5057/prod_release_notes_list.html).

## Ordering Information

The Cisco Security Agent solution consists of two main components: the Cisco Security Agents (desktop and server agents) and the Management Center. A management center is required to run agents, and agents cannot be licensed to an unlicensed console. The Management Center for Cisco Security Agents is provided at no charge with the separately licensed CiscoWorks VMS restricted or unrestricted product, or in the Cisco Security Agent starter bundle.

Tables 1 and 2 provide Cisco Security Agent product and maintenance part numbers, respectively.

**Table 1.** Cisco Security Agent Part Numbers

Part Numbers	Product Description
CSA-SRVR-K9	Cisco Security Server Agent (Windows, Linux, and Solaris), one agent
CSA-B10-SRVR-K9	Cisco Security Server Agent (Windows, Linux, and Solaris), 10-agent bundle
CSA-B25-SRVR-K9	Cisco Security Server Agent (Windows, Linux, and Solaris), 25-agent bundle
CSA-B50-SRVR-K9	Cisco Security Server Agent (Windows, Linux, and Solaris), 50-agent bundle
CSA-B100-SRVR-K9	Cisco Security Server Agent (Windows, Linux, and Solaris), 100-agent bundle
CSA-B500-SRVR-K9	Cisco Security Server Agent (Windows, Linux, and Solaris), 500-agent bundle
CSA-B1000-SRVR-K9	Cisco Security Server Agent (Windows, Linux, and Solaris), 1000-agent bundle
CSA-B2500-SRVR-K9	Cisco Security Server Agent (Windows, Linux, and Solaris), 2500-agent bundle
CSA-B5000-SRVR-K9	Cisco Security Server Agent (Windows, Linux, and Solaris), 5000-agent bundle
CSA-B10000-SRVR-K9	Cisco Security Server Agent (Windows, Linux, and Solaris), 10,000-agent bundle
CSA-B25-DTOP-K9	Cisco Security Desktop Agent (Windows and Linux), 25-agent bundle
CSA-B100-DTOP-K9	Cisco Security Desktop Agent (Windows and Linux), 100-agent bundle
CSA-B250-DTOP-K9	Cisco Security Desktop Agent (Windows and Linux), 250-agent bundle
CSA-B500-DTOP-K9	Cisco Security Desktop Agent (Windows and Linux), 500-agent bundle
CSA-B1000-DTOP-K9	Cisco Security Desktop Agent (Windows and Linux), 1000-agent bundle
CSA-B5000-DTOP-K9	Cisco Security Desktop Agent (Windows and Linux), 5000-agent bundle
CSA-B10000-DTOP-K9	Cisco Security Desktop Agent (Windows and Linux), 10,000-agent bundle
CSA-B50000-DTOP-K9	Cisco Security Desktop Agent (Windows and Linux), 50,000-agent bundle
CSA-B75000-DTOP-K9	Cisco Security Desktop Agent (Windows and Linux), 75,000-agent bundle
CSA-B100K-DTOP-K9	Cisco Security Desktop Agent (Windows and Linux), 100,000-agent bundle
CSA-B200K-DTOP-K9	Cisco Security Desktop Agent (Windows and Linux), 200,000-agent bundle
CSA-B300K-DTOP-K9	Cisco Security Desktop Agent (Windows and Linux), 300,000-agent bundle
CSA-STARTER-K9	Cisco Security Agent starter bundle (Includes 1 server agent and 10 desktop agents)

**Table 2.** Cisco Security Agent Maintenance Part Numbers

Maintenance Part Number	Maintenance Product Description
CON-SAU-CSA-STRT	Software Application Support plus Upgrades (SASU) for the Cisco Security Agent starter bundle
CON-SAU-CSA-SRVR	SASU for 1 server agent (Windows, Linux, and Solaris)
CON-SAU-CSA-B10S	SASU for 10-server agent bundle (Windows, Linux, and Solaris)
CON-SAU-CSA-B25S	SASU for 25-server agent bundle (Windows, Linux, and Solaris)
CON-SAU-CSA-B50S	SASU for 50-server agent bundle (Windows, Linux, and Solaris)
CON-SAU-CSA-B100S	SASU for 100-server agent bundle (Windows, Linux, and Solaris)
CON-SAU-CSA-B500S	SASU for 500-server agent bundle (Windows, Linux, and Solaris)
CON-SAU-CSA-B25D	SASU for 25-desktop agent bundle (Windows and Linux)
CON-SAU-CSA-B100D	SASU for 100-desktop agent bundle (Windows and Linux)

Maintenance Part Number	Maintenance Product Description
CON-SAU-CSA-B250D	SASU for 250-desktop agent bundle (Windows and Linux)
CON-SAU-CSA-B500D	SASU for 500-desktop agent bundle (Windows and Linux)
CON-SAU-CSA-1000D	SASU for 1000-desktop agent bundle (Windows and Linux)
CON-SAU-CSA-5000D	SASU for 5000-desktop agent bundle (Windows and Linux)
CON-SAU-CSA-10KD	SASU for 10,000-desktop agent bundle (Windows and Linux)

### For More Information

For more information on Cisco Security Agent, please visit <http://www.cisco.com/go/csa>.



**Americas Headquarters**  
 Cisco Systems, Inc.  
 170 West Tasman Drive  
 San Jose, CA 95134-1706  
 USA  
[www.cisco.com](http://www.cisco.com)  
 Tel: 408 526-4000  
 800 553-NETS (6387)  
 Fax: 408 527-0883

**Asia Pacific Headquarters**  
 Cisco Systems, Inc.  
 168 Robinson Road  
 #28-01 Capital Tower  
 Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
 Tel: +65 6317 7777  
 Fax: +65 6317 7799

**Europe Headquarters**  
 Cisco Systems International BV  
 Haarlerbergpark  
 Haarlerbergweg 13-19  
 1101 CH Amsterdam  
 The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
 Tel: +31 0 800 020 0791  
 Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

©2006 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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 Website 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. (0609R)