

Cisco Security Agent Version 5.2

Product Overview

Cisco® Security Agent security software provides threat protection for server, desktop, and Point-of-Service (POS) computing systems. Cisco Security Agent goes beyond conventional endpoint security solutions, providing an industry-leading defense against targeted attacks, spyware, rootkits, and day-zero attacks. Proactive protection is offered against unknown, never-seen-before threats, brand new exploits, and variants trying to take advantage of recently announced vulnerabilities. Cisco Security Agent provides “zero update” system integrity protection for critical servers that cannot be taken out of service to apply operating system or application-specific vulnerability patches. It helps reduce emergency patching of systems to respond to vulnerability announcements, minimizing patch-related downtime and IT manhour expenses. Organizations can now patch on their own schedule, not in crisis mode.

Robust policy compliance controls offer protection for sensitive data files and critical servers. Access to key files, applications, and servers can be monitored or controls enforced to stop inadvertent or malicious data loss. Removable media usage controls reduce risk and ensure workplace compliance. Granular controls may be put in place as needed to manage policy compliance for users, applications, systems, locations, and network addresses.

Cisco Security Agent offers more than a standalone endpoint security solution. It collaborates with network security devices to increase the effectiveness of the overall network deployment. Cisco VPN devices can leverage Cisco Security Agent's personal firewall and host intrusion prevention (HIPS) features to provide robust endpoint security for IP Security (IPSec) and Secure Sockets Layer (SSL) VPN remote-access users. Host information collected by Cisco Security Agent can be shared with Cisco network IPS devices to enhance the overall awareness and relevancy of the IPS actions taken in the network. The firewall and application inspection capabilities of Cisco ASA and Cisco PIX® security appliances can be enhanced by Cisco Security Agent to examine particular applications based on Cisco Security Agent traffic markings.

Network Integrated Features Table

Table 1 lists the network integration features of Cisco Security Agent.

Table 1. Network Integration Features

Feature	Description
Wireless Policy Controls	Cisco Security Agent provides wireless policy controls to enhance the overall security and optimize the bandwidth of a wireless deployment. Policies can restrict wireless connections to specific parameters, such as requiring a VPN connection for wireless traffic when a user is out of the office. Critical applications can be prioritized to minimize latency over the wireless LAN infrastructure. Cisco Security Agent's location-based policy controls offer an additional layer of protection when users are out of the office.
Traffic Marking	Cisco Security Agent can classify traffic on a per-application basis on wireless and wired networks to provide quality of service for critical applications, such as Oracle financials or voice/video. Less-critical applications such as Web browsing or e-mail can be classified as a lower priority, to optimize available network bandwidth. Cisco Security Agent traffic markings can also be used to enhance the firewall inspection capabilities of Cisco ASA 5500 Series and Cisco PIX security appliances to apply specific application inspection policies.

Feature	Description
IPS Integration	Cisco Security Agent integrates with Cisco network IPS devices to increase the effectiveness of identifying attacks within the network. Cisco Security Agent provides crucial endpoint security information to Cisco IPS 4200 Series appliances and the IPS modules for the Cisco ASA 5500 Series and the Cisco Catalyst® 6500/7600 Series to provide a complete, end-to-end security solution.
Network Admission Control (NAC) Integration	In a Cisco NAC Appliance or NAC Framework deployment, hosts that are running Cisco Security Agent can be identified and trusted to have full network access. Nonconforming hosts can be quarantined until remediation is performed and they are brought into compliance. Cisco Security Agent will protect the integrity of the NAC agent on the endpoint, preventing unwanted modifications. This enhances the self-defending nature of the enterprise network by providing mitigation against denial of service (DoS) and malware attacks.
Cisco Security MARS Event Integration	Cisco Security Agent provides important endpoint information to the Cisco Security Monitoring, Analysis, and Response System (MARS), enhancing the Cisco Security MARS capabilities of threat identification and investigation across the network.

Features and Benefits

Cisco Security Agent provides numerous benefits, including:

- Regulatory policy compliance enforcement
- Preventive protection against targeted attacks
- The ability to identify and quarantine rootkits
- Industry-leading host intrusion prevention, personal firewall, and day-zero attack protection
- Optimized Wi-Fi bandwidth
- Ensure availability of critical client-server applications and transactions
- Protects retail point of service (POS) terminals, as well as servers & desktops

Product Architecture

The Cisco Security Agent Solution

Cisco Security Agent consists of host-based agents, deployed on mission-critical desktops and servers that report to the Cisco Management Center for Cisco Security Agents. The Management Center runs as a standalone application performing configuration of Cisco Security Agent deployments. The agents use HTTP and 128-bit SSL for the management interface, and for communication between agents and the Management Center. Alerts can be integrated with alerts from other Cisco security products using Cisco Security MARS.

Agent Architecture

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, 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. Its role-based, Web browser 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 that allow 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 the applications that 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.

Summary/Conclusion

Cisco Security Agent is a core component of a Cisco 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.

Product Specifications

Table 2 lists product specifications for Cisco Security Agent Version 5.2.

Table 2. Product Specifications

Description	Specification
Software Compatibility for Cisco Security Server Agents	<ul style="list-style-type: none"> • Windows Embedded for Point of Service (WEPOS) • Windows 2003 (Standard, Enterprise, Web, or Small Business Editions) • Windows 2000 Server and Advanced Server • Windows NT 4.0 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 • Red Hat Enterprise Linux 4.0 ES and AS
Software Compatibility for Cisco Security Desktop Agents	<ul style="list-style-type: none"> • Windows XP Professional • Windows XP Tablet Edition • Windows 2000 Professional • Windows NT 4.0 Workstation (SP 6a) • Red Hat Enterprise Linux 3.0 WS • Red Hat Enterprise Linux 4.0 WS
Hardware Compatibility for Cisco Security Agents (Windows OS Minimum Requirements)	<ul style="list-style-type: none"> • 200-MHz x86 processor • 25 MB hard drive space • 128 MB RAM • Ethernet or dialup network connection
Hardware Compatibility for Cisco Security Agents (Solaris OS Minimum Requirements)	<ul style="list-style-type: none"> • UltraSPARC 400-MHz processor • 25 MB hard drive space • 256 MB RAM • Ethernet network connection
Hardware Compatibility for Cisco Security Agents (Linux OS Minimum Requirements)	<ul style="list-style-type: none"> • 500-MHz x86 processor • 25 MB hard drive space • 256 MB RAM • Ethernet network connection
Software compatibility for Management Center for Cisco Security Agents	<ul style="list-style-type: none"> • Windows 2003 R2 Server
Hardware Compatibility for Management Center for Cisco Security Agents (Minimum Requirements)	<ul style="list-style-type: none"> • 1-GHz x86 processor • 1 GB RAM • 2 GB virtual memory
Internationalization	<ul style="list-style-type: none"> • 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, Polish, Portugese and Spanish • Support for English (United States) Linux and Solaris operating systems only

Ordering Information

The Cisco Security Agent solution consists of two main components: 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 in the Cisco Security Agent starter bundle.

Tables 3 and 4 provide Cisco Security Agent product and maintenance part numbers, respectively. To place an order, visit the [Cisco Ordering Home Page](#).

Table 3. Ordering Information for Cisco Security Agents

Product Name	Part Number
--------------	-------------

Product Name	Part Number
Cisco Security Agent starter bundle for Version 5.2 (includes Management Center for Cisco Security Agents, 1 server agent, and 10 desktop agents)	CSA-START-5.2-K9
Cisco Security Server Agent (Windows, Linux, and Solaris), 1 agent	CSA-SRVR-K9
Cisco Security Server Agent (Windows, Linux, and Solaris), 10-agent bundle	CSA-B10-SRVR-K9
Cisco Security Server Agent (Windows, Linux, and Solaris), 25-agent bundle	CSA-B25-SRVR-K9
Cisco Security Server Agent (Windows, Linux, and Solaris), 50-agent bundle	CSA-B50-SRVR-K9
Cisco Security Server Agent (Windows, Linux, and Solaris), 100-agent bundle	CSA-B100-SRVR-K9
Cisco Security Server Agent (Windows, Linux, and Solaris), 500-agent bundle	CSA-B500-SRVR-K9
Cisco Security Server Agent (Windows, Linux, and Solaris), 1000-agent bundle	CSA-B1000-SRVR-K9
Cisco Security Server Agent (Windows, Linux, and Solaris), 2500-agent bundle	CSA-B2500-SRVR-K9
Cisco Security Server Agent (Windows, Linux, and Solaris), 5000-agent bundle	CSA-B5000-SRVR-K9
Cisco Security Server Agent (Windows, Linux, and Solaris), 10,000-agent bundle	CSA-B10000-SRVR-K9
Cisco Security Desktop Agent (Windows and Linux), 25-agent bundle	CSA-B25-DTOP-K9
Cisco Security Desktop Agent (Windows and Linux), 100-agent bundle	CSA-B100-DTOP-K9
Cisco Security Desktop Agent (Windows and Linux), 250-agent bundle	CSA-B250-DTOP-K9
Cisco Security Desktop Agent (Windows and Linux), 500-agent bundle	CSA-B500-DTOP-K9
Cisco Security Desktop Agent (Windows and Linux), 1000-agent bundle	CSA-B1000-DTOP-K9
Cisco Security Desktop Agent (Windows and Linux), 2500-agent bundle	CSA-B2500-DTOP-K9
Cisco Security Desktop Agent (Windows and Linux), 5000-agent bundle	CSA-B5000-DTOP-K9
Cisco Security Desktop Agent (Windows and Linux), 10,000-agent bundle	CSA-B10000-DTOP-K9
Cisco Security Desktop Agent (Windows and Linux), 25,000-agent bundle	CSA-B25000-DTOP-K9
Cisco Security Desktop Agent (Windows and Linux), 50,000-agent bundle	CSA-B50000-DTOP-K9
Cisco Security Desktop Agent (Windows and Linux), 75,000-agent bundle	CSA-B75000-DTOP-K9
Cisco Security Desktop Agent (Windows and Linux), 100,000-agent bundle	CSA-B100000-DTOP-K9
Cisco Security Desktop Agent (Windows and Linux), 200,000-agent bundle	CSA-B200000-DTOP-K9
Cisco Security Desktop Agent (Windows and Linux), 300,000-agent bundle	CSA-B300000-DTOP-K9

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, see [Cisco Technical Support Services](#) or [Cisco Advanced Services](#).

Table 4. Ordering Information for Cisco Security Agent Maintenance

Product Name	Part Number
Software Application Support plus Upgrades (SASU) for the Cisco Security Agent starter bundle	CON-SAU-CONSAS5K
SASU for 1 server agent (Windows, Linux, and Solaris)	CON-SAU-CSA-SRVR
SASU for 10 server agents (Windows, Linux, and Solaris)	CON-SAU-CSA-B10S
SASU for 25 server agents (Windows, Linux, and Solaris)	CON-SAU-CSA-B25S
SASU for 50 server agents (Windows, Linux, and Solaris)	CON-SAU-CSA-B50S
SASU for 100 server agents (Windows, Linux, and Solaris)	CON-SAU-CSA-B100S
SASU for 250 server agents (Windows, Linux, and Solaris)	CON-SAU-CSA-B250S
SASU for 500 server agents (Windows, Linux, and Solaris)	CON-SAU-CSA-B500S

Product Name	Part Number
SASU for 1000 server agents (Windows, Linux, and Solaris)	CON-SAU-CSA-B1000S
SASU for 2500 server agents (Windows, Linux, and Solaris)	CON-SAU-CSA-B2500S
SASU for 5000 server agents (Windows, Linux, and Solaris)	CON-SAU-CSA-B5000S
SASU for 10,000 server agents (Windows, Linux, and Solaris)	CON-SAU-CSA-B10000S
SASU for 25-desktop agent bundle (Windows and Linux)	CON-SAU-CSA-B25D
SASU for 100-desktop agent bundle (Windows and Linux)	CON-SAU-CSA-B100D
SASU for 250-desktop agent bundle (Windows and Linux)	CON-SAU-CSA-B250D
SASU for 500-desktop agent bundle (Windows and Linux)	CON-SAU-CSA-B500D
SASU for 1000-desktop agent bundle (Windows and Linux)	CON-SAU-CSA-B1000D
SASU for 2500-desktop agent bundle (Windows and Linux)	CON-SAU-CSA-B2500D
SASU for 5000-desktop agent bundle (Windows and Linux)	CON-SAU-CSA-B5000D
SASU for 10,000-desktop agent bundle (Windows and Linux)	CON-SAU-CSA-B10KD
SASU for 25,000-desktop agent bundle (Windows and Linux)	CON-SAU-CSA-B25KD
SASU for 50,000-desktop agent bundle (Windows and Linux)	CON-SAU-CSA-B50KD
SASU for 75,000-desktop agent bundle (Windows and Linux)	CON-SAU-CSA-B75KD
SASU for 100,000-desktop agent bundle (Windows and Linux)	CON-SAU-CSA-B100KD
SASU for 200,000-desktop agent bundle (Windows and Linux)	CON-SAU-CSA-B200KD
SASU for 300,000-desktop agent bundle (Windows and Linux)	CON-SAU-CSA-B300KD



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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.

CCDE, CCVP, Cisco, Cisco StadiumField, the Cisco logo, CPE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play and Learn is a service mark; and Access Registrar, Altran, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCS, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS IPsec, IPTV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuickStudy, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MIM, NetWorkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx 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 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. ©2007