

## Cisco Security Agent Version 6.0

### **Always Vigilant Endpoint Security**

Cisco® Security Agent 6.0 is the first endpoint security solution that combines zero-update attack defense, policy-driven data loss prevention, and signature-based antivirus detection in a single agent. This unique blend of capabilities defends servers and desktops against sophisticated day-zero attacks, and enforces acceptable-use and compliance policies within a simple management infrastructure.

### **Zero Update Protection**

Cisco Security Agent is the industry leader in defending endpoints against targeted attacks, malicious mobile code, rootkits, worms, and day-zero attacks. Zero-update protection is critical when addressing brand new exploits or variants that take advantage of published and unpublished system and application vulnerabilities. Cisco Security Agent continuously defends critical servers that cannot be taken out of service to apply operating system or application-specific vulnerability patches. This reduces emergency patching of systems in response to vulnerability announcements and minimizes patch-related downtime and IT person-hour expenses.

### **Data Loss Prevention**

Cisco Security Agent provides visibility and control of sensitive data across all endpoints; protecting against data loss from both end-user actions and targeted malware. Newly added content scanning capabilities detect credit card numbers, Social Security numbers, and customer-defined sensitive data in local files. Access to these sensitive files is audited and policy controls can be implemented to stop malicious data transfers to removable devices or through insecure network applications. Cisco Security Agent offers customizable feedback queries for end-user education and reinforcement of company security policies. Justification options provide an audit trail without sacrificing employee productivity and timely access to critical data. Additionally, the end-user interface is localized in 11 different languages to facilitate worldwide deployments.

### **Signature-Based Antivirus**

Although behavior-based controls are the primary and most reliable means of stopping malware attacks on endpoints, signature-based anti-virus protection plays a key role in identifying known malware. Newly added signature-based anti-virus increases the confidence that malware can be removed from the endpoint, since it has been identified by name. Additionally, antivirus signatures enable you to comply with regulations that still require this technology.

### **Compliance and Acceptable-Use Policy Auditing and Enforcement**

Cisco Security Agent's robust policy engine offers compliance auditing and control. Predefined and customized policies are centrally managed for efficient reporting and auditing of activities. Many predefined compliance and acceptable-use policies are available from Cisco. Some examples include:

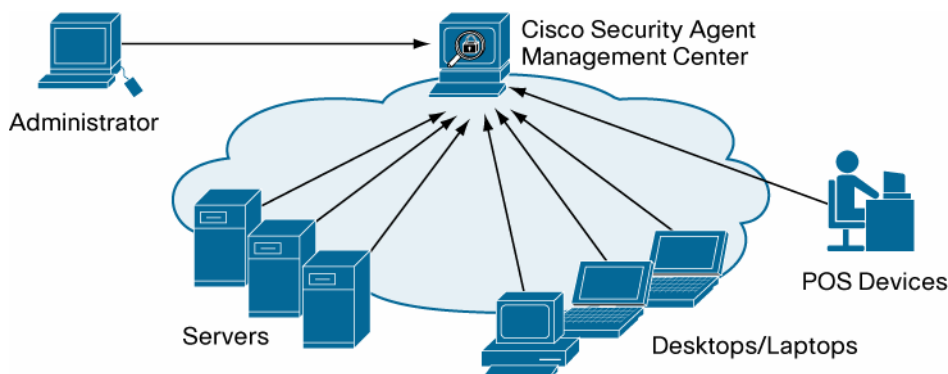
- **Payment Card Industry Data Security Standard (PCI DSS) policies**, which enable control and auditing for compliance to the standard, including requirements that vendors typically fail during audit
- **Application of location-based policies** that require the user to have a VPN connection when out of the office
- **Disabling reading and writing to USB drives**
- **Wireless communication** is restricted when the endpoint is also connected to the wired network

## Network Security Integration

The industry-leading network and endpoint security integration offered by Cisco Security Agent increases the effectiveness of Self-Defending Network deployments.

- **Cisco Network Admission Control** can use the status of Cisco Security Agent as part of the posture check assessed before allowing a connection to the network.
- **Cisco network IPS devices** receive host information collected by Cisco Security Agent, which enhances overall awareness and relevancy of the IPS actions taken in the network.
- **Cisco Security Monitoring, Analysis, and Response System (MARS)** collects security information from Cisco Security Agents, which enhances the Cisco Security MARS ability to identify and investigate threats across the network.
- **Cisco VPN remote-access clients** are protected by the personal firewall and host intrusion prevention features of Cisco Security Agent.
- **Cisco's IronPort®** network inspection coverage can be enhanced with Cisco Security Agent policies that require roaming users to establish VPN connections back to the corporate network.
- **Cisco Security Agent network traffic marking policies** are based on the source application, which enables more granular and manageable network differentiation. This can be used in conjunction with the firewall and application inspection capabilities of Cisco ASA 5500 Series and Cisco PIX® security appliances to examine traffic from specific applications.
- **Cisco Unified Communications servers** ship with Cisco Security Agent already installed to protect against attacks.

Figure 1.



## Centralized Management

The Management Center for Cisco Security Agents provides management functions for all agents in a centralized manner. Behavioral policies, data loss prevention, and antivirus protection are fully integrated into a single configuration and reporting interface. 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. Each agent operates autonomously and enforces the security policy even if communication with the manager is not possible (for example, if a remote laptop user has not yet connected through the VPN).

Table 1 lists specifications for Cisco Security Agent Version 6.0.

**Table 1.** Agent Specifications

Specification	Details
<b>Server Agent</b>	<ul style="list-style-type: none"> <li>• Windows 2003 Server</li> <li>• Windows 2000 Server and Advanced Server</li> <li>• Solaris 9 SPARC architecture (64-bit kernel)</li> <li>• Solaris 8 SPARC architecture (64-bit kernel)</li> <li>• Red Hat Enterprise Linux 4.0 ES and AS</li> <li>• Red Hat Enterprise Linux 3.0 ES and AS</li> <li>• VMware GSX 3.2</li> <li>• VMware ESX 3.0 and 2.5</li> <li>• (free) VMware Server</li> </ul>
<b>Desktop Agent</b>	<ul style="list-style-type: none"> <li>• Windows Vista</li> <li>• Windows Embedded Point of Service (WEPOS)</li> <li>• Windows XP Professional</li> <li>• Windows XP Tablet Edition</li> <li>• Windows 2000 Professional</li> <li>• Red Hat Enterprise Linux 4.0 WS</li> <li>• Red Hat Enterprise Linux 3.0 WS</li> <li>• VMware WS 5.x</li> <li>• (free) VMware Player</li> </ul>
<b>Localization</b>	<ul style="list-style-type: none"> <li>• Chinese</li> <li>• English</li> <li>• French</li> <li>• German</li> <li>• Italian</li> <li>• Japanese</li> <li>• Korean</li> <li>• Polish</li> <li>• Portuguese</li> <li>• Russian</li> <li>• Spanish</li> </ul>

## Cisco Service and Support

Cisco takes a lifecycle approach to services and, with its partners, provides a broad portfolio of security services so enterprises can design, implement, operate, and optimize network platforms that defend critical business processes against attack and disruption, protect privacy, and support policy and regulatory compliance controls.

Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. Cisco services include:

- The Cisco Security Center provides one-stop shopping for early warning threat intelligence threat and vulnerability analysis, Cisco IPS signatures, and mitigation techniques. Visit and bookmark the Cisco Security Center at <http://www.cisco.com/security>.
- The Cisco Security Intellishield Alert Manager Service provides a customizable, Web-based threat and vulnerability alert service that allows organizations to easily access timely, accurate, and credible information about potential vulnerabilities in their environment.
- Cisco Security Optimization Service: Increasingly, the network infrastructure is the foundation of the agile and adaptive business. The Cisco Security Optimization Service supports the continuously evolving security system to meet ever-changing security threats through a combination of planning and assessments, design, performance tuning, and ongoing support for system changes. This service helps integrate security into the core network infrastructure.
- Cisco Software Application Support Services, plus Upgrades [SASU] ensures Cisco Security Agent availability, functionality, and reliability with around-the-clock access to technical support, software updates, and major upgrades.
- Cisco Security Agent Implementation Service provides expert security analysis, planning, design, and implementation assistance to help organizations integrate Cisco Security Agent into their environments.

### For More Information

The Cisco Security Agent product bulletin describes the licensing options and ordering details. To access the product bulletin or other information about Cisco Security Agent visit <http://www.cisco.com/go/csa>.

For more information about Cisco Security Services visit [http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv\\_group\\_home.html](http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html).



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](http://www.cisco.com/go/offices).

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, 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, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, 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. (0809R)