

Cisco **Security** Agent Profiler

The next-generation Cisco® Security Agent network 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.

The Cisco Security Agent Profiler extends these security capabilities by automating analysis of the activities performed by particular applications and by building custom protective policies for these applications.

Benefits

- Simplifies forensic investigation of unknown applications by automatically observing all file, network, registry, and COM access requests made by the application
- Builds protective policies based on observed application behavior
- Protects all new and legacy corporate applications

- Integrated with the Management Center for Cisco Security Agents; hot-linked directly from alerts to start monitoring applications on any system protected by a Cisco Security Agent
- Reduces the cost of administering security by providing automated, centralized analysis of security-related activity
- Offers an enterprise-scalable architecture; scalable to thousands of agents per profiler

Automating Security Investigation

One of the most difficult aspects of managing security is deciding what to do after an alert is received. Alerts often contain only a portion of the information needed by the security operator to make an informed decision about what action to take. Should the current security policy be modified? Should the incident be escalated to system administrators? Is policy being violated, or is this event normal and expected? The sometimes-incomplete information contained in alerts makes this decision difficult or impossible.

The Cisco Security Agent Profiler provides a centralized ability to investigate alerts received from any Cisco Security Agent. It can centrally configure an agent to monitor a particular application, observing all



behavioral requests made by the application. Each request for file system, network, registry, and COM object access is logged and uploaded from the agent to the Management Center, where the profiler analyzes the data and provides a series of reports to the operator.

This silent, centralized monitoring of application behavior provides a rich set of information about all activities performed by an application, not just behaviors that violate security policy. This rich information environment allows easy identification of malicious activity, and helps identify benign activity that may have been identified as suspect. Using the Cisco Security Agent Profiler, the operator moves from an environment where decisions must be made based on anecdotal data to one where decisions are made based on a complete view of the suspect application. Decision-making factors include:

- What are all the network connections that this application makes? Which remote systems are communicating with the application? Is the application acting as a network client? As a server? Both? Increasingly, many applications are using Secure Sockets Layer (SSL) encrypted connections to hide what they are doing. The Cisco Security Agent Profiler will show what these applications are.
- What are all the files being accessed by the application? Are any of them sensitive data files, or files that may be prohibited (for example, a network application serving MP3 files to remote systems)? Are the files being read or written?
- What registry keys are being read or written? Very often this will identify the application and vendor by name.
- Are any COM objects being loaded? Many applications make their functions available as loadable objects (for example, Microsoft Office or e-mail programs). The use of these objects can help to identify what an unknown application is trying to do.

By observing this activity and presenting a centralized, consolidated view to the security operator, security decisions can be made more quickly and with a much higher level of confidence.

Integrates with the Management Center for Cisco Security Agents

The Cisco Security Agent Profiler is installed on the Management Center for Cisco Security Agents, and can be used to monitor the behavior of any application on any system with a Cisco Security Agent. The Management Center provides a hot link directly from alerts displayed in the event log, which cause the profiler to investigate the specific application on the agent that generated the alert. An analysis job can also be created for an application that has not caused any alerts to be generated. For example, if an alert is observed from a Cisco Secure IDS sensor, a profiler job could help investigate that as well.

Builds Custom Protective Policies

Many organizations have custom applications performing mission-critical business functions. While many organizations would like to have increased security protection for these applications, there has traditionally been no way to provide this, other than modifying the application's source code. Even if there had been a way to externally overlay security onto the application, there has been no way to know whether these security measures would block necessary functions. In other words, there has traditionally been a significant risk that the security measures themselves will cause application failure.

The Cisco Security Agent Profiler's ability to monitor all application behavior provides a unique capability to customize security to the needs of the application, rather than limit application activity to meet the needs of security. The same process that is used to investigate unknown application behavior can be used to monitor an application



for all resource access made in the normal course of that application's execution. This data is collected by the agent, and then the profiler automatically builds a Cisco Security Agent protective policy for that application. Since the policy reflects the actual observed behavior of the application, the security protection automatically adapts to the needs of the application.

The Cisco Security Agent Profiler can create a protective policy for any application. No knowledge of how the application works—or access to the application's source code—is required. Profiler-created protective policies can be used on any agent managed from that Management Center, or can be exported and used by a different Management Center entirely.

Technical Specifications

Language availability: English (United States) only for all agents.

Installation Requirements

A license key must be installed on the Management Center for the profiler to function.

Ordering Information

The Cisco Security Agent Profiler is enabled by the installation of a license key on a Management Center for Cisco Security Agents. Table 1 lists part numbers for the Cisco Security Agent Profiler.

Table 1 Cisco Security Agent Part Numbers

Part Numbers	Product Description
CSA-PROFILER-K9	Cisco Security Agent Profiler
Maintenance Part Number	Maintenance Product Description
CON-SAS-CSA-PRO	Software Application Support Services for Cisco Security Agent Profiler



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe