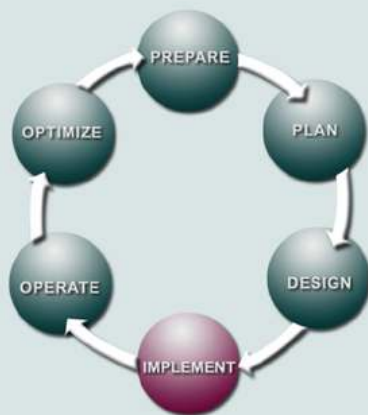


Cisco Security Agent Implementation Service

Expert Assistance to Proactively Protect Networks from Worm and Virus Attacks

THE CISCO LIFECYCLE SERVICES APPROACH



The unique Cisco lifecycle approach to services defines the requisite activities at each phase of the network lifecycle to help ensure service excellence. With a collaborative delivery methodology that joins the forces of Cisco, our skilled network of partners, and our customers, we achieve the best results.

Network Lifecycle Phases

- **Prepare**—Develop a business case for a technology investment
- **Plan**—Assess readiness to support proposed solution
- **Design**—Create a detailed design to address business and technical requirements
- **Implement**—Deploy new technology
- **Operate**—Maintain network health through day-to-day operations
- **Optimize**—Achieve operational excellence through ongoing improvements

Service Overview

High-visibility attacks that target servers and desktops are becoming more common and more sophisticated. As the number of attacks grows and propagation times shrink, your organization needs new strategies to defend critical network endpoints. Although antivirus and spyware removal applications provide important protection, they rely on signatures from known attacks. Cisco® Security Agent goes beyond conventional host-based security by analyzing actual operating system behavior instead of matching virus signatures. As a result, the solution can help protect against both known and unknown (“day-zero”) attacks and can defend against vulnerabilities that have not yet been published or even discovered.

However, to function effectively, the Cisco Security Agent solution must be carefully deployed, configured, tuned, and integrated into your network infrastructure. In addition, Cisco Security Agent uses a policy-based approach to blocking security attacks, so your organization’s business and security policies must be integrated into the solution from the beginning.

The Cisco Security Agent Implementation Service, designed for large enterprises, provides the expert security analysis, planning, design, and implementation assistance that your organization needs to design and deploy an effective Cisco Security Agent solution. Applying extensive practical experience, knowledge of the latest risk mitigation techniques, and specialized tools and methodologies, Cisco security consultants can help your organization deploy effective host-based network defenses and better manage evolving security threats.

Proactively Defend Against Known and Unknown Attacks

Through the Cisco Security Agent Implementation Service, Cisco security consultants help your organization deploy a Cisco Security Agent solution that integrates with existing network infrastructure, software operations procedures, and security management (Table 1). Employing a consistent and proven methodology for implementing Cisco Security Agent, Cisco experts provide the following services to help ensure the Cisco Security Agent deployment is a success:

- **Cisco Security Agent readiness assessment**—Cisco network engineers analyze Cisco Security Agent deployment requirements and assess the readiness of your network devices, operations, and architecture to support the solution. In addition to identifying components that do not support Cisco Security Agent capabilities, security engineers determine if your network topology supports a scaled deployment and deliver an impact analysis detailing requirements for redundancy, scalability, and hardware and software upgrades.
- **Cisco Security Agent limited deployment**—Cisco network security engineers install and configure a limited deployment solution, allowing your IT staff to test and gain experience with the Cisco Security Agent solution. This limited deployment can be deployed in a lab or in a production environment such as a branch office, and includes configuration, maintenance, and support documentation for the solution.
- **Cisco Security Agent design development**—Cisco consultants assist in developing a detailed design for integrating Cisco Security Agent into your network infrastructure. Working with your IT staff, design engineers develop the overall strategy and plan for the Cisco Security Agent solution, providing an in-depth analysis of the technical, procedural, and resource requirements for a corporatewide deployment. Cisco consultants also provide you with a design specification that defines your network topology and functional requirements, including configuration recommendations for Cisco Security Agent protocols, policies, and features.
- **Cisco Security Agent implementation engineering**—The Cisco Security Agent solution must be carefully deployed, configured, and integrated into the network infrastructure, so Cisco security engineers support your team through a full-scale implementation. Cisco consultants work with your IT staff to develop detailed deployment plans, including installation, configuration, integration, and management. After the plans are completed, Cisco security engineers deliver onsite support for installation, configuration, testing, and tuning to help ensure the deployment integrates smoothly into your production environment. Once in production deployment, Cisco engineers assist in optimizing custom policies and document all Cisco Security Agent policy rules.

Table 1. Cisco Security Agent Implementation Activities, Methodology, and Deliverables

Activities	Methodology and Deliverables
<ul style="list-style-type: none"> • Analyze Cisco Security Agent deployment goals, objectives, and requirements, including security policy and technical requirements for endpoints, applications, and devices • Analyze the impact of integrating Cisco Security Agent with existing IT infrastructure, software operations, and security management procedures • Assess your network's readiness to support the solution, including the readiness of the current IT infrastructure, security device configurations, software operations, and security management procedures • Define the architectural, topological, and functional requirements for the solution • Develop a detailed design of the solution, including network diagrams, network topology, and sample configurations for Cisco Security Agent protocols, policies, and features • Specify hardware and software requirements, including security management tools • Develop an implementation strategy and plan detailing the requirements for solution deployment, integration, and management • Develop the solution testing, installation, integration, management, and maintenance plans • Define the systems and application groups to be protected and define policies for each application group • Build and distribute the solution to end-user workstations in a controlled environment • Test the solution and analyze system performance and network impact • Perform detailed policy tuning and retuning, as needed • Develop the network staging plan detailing installation and service requirements tasks • Develop the acceptance test plan • Provide custom installation, configuration, testing, tuning, and integration of the solution in a production environment • Perform an acceptance test on the solution and analyze system performance and network impact • Provide practical knowledge transfer with staff on the operation and management of the solution 	<p>Methodology</p> <ul style="list-style-type: none"> • Conduct a kickoff meeting to identify the business objectives for the project, introduce the implementation team, and review major implementation tasks and milestones • Conduct a design workshop to gather business, technical, and operational requirements • Assess the readiness of the network to support Cisco Security Agent • Develop a Cisco Security Agent deployment plan • Develop a Cisco Security Agent design specification • Perform custom installation, configuration, tuning, and integration of the Cisco Security Agent solution • Document Cisco Security Agent policies, tuning, and operational procedures • Deliver maintenance and support documentation • Present an executive summary of the Cisco Security Agent implementation methodology and production deployment <p>Deliverables</p> <ul style="list-style-type: none"> • A Cisco Security Agent Design Specification detailing the Cisco Security Agent design topology, feature configuration, and policy implementation • A Cisco Security Agent Rules Reference Guide documenting the deployed Cisco Security Agent policy rules • An optimized Cisco Security Agent installation in a production environment

Benefits

With the Cisco Security Agent Implementation Service, your organization can:

- More effectively mitigate security threats by using a sound design and implementation process to deploy the Cisco Security Agent solution
- Obtain expert assistance to plan the most strategic and effective placement and configuration for the Cisco Security Agent solution
- Speed Cisco Security Agent integration by anticipating resource and technical requirements and more effectively planning for required infrastructure changes
- Reduce your operating costs and total cost of network ownership by helping to ensure consistent deployment of security policy
- Enhance Cisco Security Agent performance, resiliency, and availability by using the correct set of hardware, software releases, features, and functionality
- Improve staff proficiency managing and operating Cisco Security Agent through continuous knowledge exchange with Cisco experts throughout the design and deployment process

Why Cisco

The Cisco Security Agent Implementation Service helps you rapidly deploy a solution to mitigate the risk of worms, viruses, and spyware. The service strengthens your team's ability to meet aggressive deployment schedules while decreasing costly disruptions to the network. By helping to ensure the consistent deployment of Cisco Security Agent policies and procedures, as well as efficient management and maintenance of the solution, Cisco Services can support your efforts to reduce the total cost of ownership of your security infrastructure.

Availability and Ordering

The Cisco Security Agent Implementation Service is available through Cisco and Cisco partners globally. Details may vary by region.

For More Information

For more information about the Cisco Security Agent Implementation Service or the Cisco Lifecycle Services approach, contact your Cisco representative.



Americas 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: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
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
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.

©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)