



Achieving Proactive Risk Management

As a strategic asset enabling business processes and relationships, the network is a target for ever-changing attack modes. Day-zero protection against security threats is a top priority among Cisco® enterprise customers, which need to maintain business continuity, comply with government regulations, preserve customer confidence, and effectively compete in an increasingly global economy.

The Cisco Lifecycle Services approach helps Cisco enterprise customers to realize optimal value from their Cisco networks. As part of the optimization phase, the Cisco defense-in-depth approach to network security integrates proactive security response capabilities throughout the network infrastructure. Cisco Security Optimization Services help enterprises to be prepared against constantly changing threats and attacks from within and without the organization.

Optimizing the Network

Through expertise, tools, and proven methodologies, Cisco Security Optimization Services help your organization to proactively evaluate and strengthen the network's ability to prevent, detect, and mitigate against threats. Cisco service experts help you create a trusted, resilient security network. Cisco service experts guide you as you invest in strategic, system-level solutions that help you continually optimize your network security posture, so as threats emerge, the network is prepared to respond.

This eight-part service includes the following components:

- Security technology planning support: proactively manage security risk with expert planning, analysis, and decision making
- Security architecture review: strengthen your network by identifying vulnerabilities and deviations from best practices and policy

- Security technology readiness assessment: speed deployment and reduce costly mistakes with expert analysis of your network's ability to support and scale a new solution
- Security posture assessment: reduce the risk of intentional or accidental access to IT assets and information
- Security performance tuning: proactively optimize advanced solutions with ongoing analysis of system configuration and policy implementation
- Security design support: improve the reliability, maintainability, and performance of your solution design
- Security change support: mitigate costly delays and problems during critical changes to the security infrastructure
- Security knowledge transfer: continuously improve the skills of your staff with ongoing interactive continuous learning and training sessions.

Service Benefits

Along with improving the security posture and responsiveness of your organization's network, Cisco Security Optimization Services enable the following business benefits:

- Reduce operating costs by improving your ability to identify and mitigate vulnerabilities, anticipate resource and technical requirements, and effectively plan for infrastructure changes
- Improve decision making and augment IT skill sets by using Cisco expertise to proactively identify and mitigate against vulnerabilities, protect against emerging threats, and plan enhancements to your security infrastructure
- Achieve compliance through consistent security policy enforcement, improved procedures, and up-to-date assessments
- Extend your investment by optimizing the features and capabilities of your existing security solutions

Why Cisco Services?

Cisco and its certified security services partners maintain high standards for expertise and experience, delivering consistently excellent results based on best practices and good communication. These experts deliver security optimization services that allow organizations to quickly, accurately, and cost-effectively protect their networks.

Cisco Security Optimization Services are delivered by highly trained Cisco experts, typically with one or more Cisco CCIE® designations. These experts develop in-depth knowledge of your security environment and how it supports your business objectives. They act as liaisons between your organization and the wealth of security expertise and resources available at Cisco.

If you are interested in Cisco Security Optimization Services, you might also want to consider the Cisco Network Optimization Service.

For more information about the Cisco Network Optimization Service, visit www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html.



Table 1 summarizes the Cisco Security Optimization Service

Table 1. Cisco Security Optimization Service Summary

Activities	Deliverables
Security Technology Planning Support	<ul style="list-style-type: none"> • Ongoing support for strategic planning and roadmap development • Technology migration planning • Analysis and recommendations for network security decision making • Quarterly security technology planning report
Security Architecture Review	<ul style="list-style-type: none"> • Security architecture workshop • Security architecture analysis • Gap analysis with recommendations • Security architecture review report
External Security Posture Assessment	<ul style="list-style-type: none"> • Discovery to identify systems and services visible to the Internet • Penetration testing to confirm the presence of vulnerabilities • Detailed analysis to identify critical vulnerabilities • Prioritized list of discovered risks with recommended actions • External security posture assessment report
Security Technology Readiness Assessment	<ul style="list-style-type: none"> • Security discovery workshop • Effect analysis of proposed solution deployment • Security technology readiness assessment report
Security Design Support	<ul style="list-style-type: none"> • Security design and discovery workshop • Security design review, including gap analysis and recommendations • Detailed security design report
Security Performance Tuning	<ul style="list-style-type: none"> • Security device discovery • Analysis of baseline configuration template • Device configuration analysis, including tuning requirements • Iterative performance tuning • Security performance tuning report
Security Change Support	<ul style="list-style-type: none"> • Implementation plan review • Test plan review • Rollback plan review • Remote engineering support • Scheduled security system change support • Unscheduled security system change support
Security Knowledge Transfer and Mentoring	<ul style="list-style-type: none"> • Knowledge transfer evaluation workshop • Knowledge transfer requirements report • Quarterly "chalk talks" and/or technical presentations • Instructor-led and remote knowledge transfer sessions • Ongoing conference calls and e-mail communication