

Cisco Security Optimization Service

Proactively strengthen your network to better respond to evolving security threats and unexpected incidents.



Optimize Your Network for Borderless Business Evolution

The borderless network is the new foundational network. Business innovation demands that employees, customers, and partners can access mission-critical applications with any device from anywhere, any time – securely, reliably, transparently. Cisco and our partners offer services to support the Borderless Network Architecture and the business solutions that run on it.

The Cisco Security Optimization Service strengthens your security infrastructure.

Our team of professionals complements your team and the Cisco partners you work with as we help you to:

- Strengthen your infrastructure
- Adopt new security solutions and smoothly integrate them into your network
- Prepare your network environment to support new technologies and applications and help ensure alignment of your business and technical requirements

Service Overview

The evolution and complexity of security threats pose an ongoing challenge to your business. Proactive IT risk management and security strategies help minimize downtime, asset loss, and damage to corporate systems. The Cisco® Security Optimization Service helps businesses with high security and compliance requirements by providing ongoing expertise, tools, and methodologies to evaluate and strengthen the network’s ability to prevent, detect, and mitigate threats.

Through a combination of strategic planning, architectural reviews, quarterly site visits, and periodic assessments, your IT staff can proactively anticipate changing security requirements, identify vulnerabilities at the system and network level, and more efficiently integrate advanced technology into the core infrastructure. This level of support assists your organization in prioritizing areas of improvement and reducing risk when making changes to the security infrastructure. These activities enable long-term business security and risk management, as well as near-term tactical solutions to immediate security threats and intrusions.

The Cisco Security Optimization Service includes nine components:

- Security technology planning support
- Network device security assessment
- Security posture assessment
- Security architecture assessment
- Security technology readiness assessment
- Security design support
- Security performance tuning
- Security change support
- Security knowledge transfer

Security Technology Planning Support

The security technology planning support provides you with access to a Cisco security advisor for ongoing expert advice and technical guidance, helping to support your security strategy, technology choices, and architectural decision making. This trusted advisor can help your organization:

- Augment the skills of your IT staff with ongoing advice and guidance
- Develop near- or long-term security solution plans to improve your security defenses and deploy new solutions

- Keep you up-to-date on the security posture of your network through analysis of ongoing vulnerability assessments and change support updates
- Improve the effectiveness of security decision making through an ongoing relationship with security experts familiar with your network environment

Your security adviser participates in periodic security technical planning meetings for the purpose of advising technical leadership and strategic planning organizations. The security topics covered in consultative meetings are determined by your organization and can range from active input about your company's current security projects to advising you about long-term technology planning initiatives.

Network Device Security Assessment

In today's complex and ever-changing threat landscape, gaps in network and security devices hardening can place data integrity, information confidentiality, and business-critical applications at risk. Vulnerable devices provide attack vectors to valuable data and resources. Also, new deployments bring new devices and new vulnerabilities. Secure network devices are a critical foundational step to securing business and customer data.

The Cisco Network Device Security Assessment allows you to implement a hardened network device environment by identifying gaps in your Cisco network infrastructure security and providing a prioritized set of actionable steps to remediate them. The assessments are appropriate for Cisco infrastructures for the core routing and switching network, wireless network, and firewalls connected to the network.

Cisco security experts begin by conducting a detailed review of your Cisco network and firewall devices. Based on this information, they complete an in-depth analysis of your network, firewall, and wireless devices. Additionally, they perform high-level analysis of access lists deployed in your network against best practices.

Cisco engineers identify gaps by performing a thorough analysis of your organization's alignment with industry security best practices. Engineers then provide prioritized and actionable recommendations to mitigate the identified gaps in device configurations. By taking this comprehensive approach to assessing the Cisco infrastructure, this service helps your organization improve risk management and satisfy compliance needs by reducing threats to the confidentiality, integrity, and availability of business processes and information.

Security Posture Assessment

Because technologies, business processes, and security threats are always changing, your organization's security posture is never static. Many organizations perform periodic security posture assessments to maintain a current picture of their vulnerabilities, allowing them to prioritize remediation activities based on available resources and business risk.

The Cisco Security Posture Assessment provides a point-in-time validation of how well the security architecture and designs have been implemented and are being operated. These services measure the extent to which identified vulnerabilities can be utilized to achieve unexpected or unauthorized access to the OS or applications on IP-connected endpoints (UNIX/Windows/network and security devices). This assessment compares discovered vulnerabilities with industry leading practices and up-to-date intelligence from the industry. Cisco delivers a prioritized report based on risk to the organization with recommended remediation actions.

Internal Security Posture Assessment

Although external network security incidents often get more attention, your organization cannot afford to overlook the threat from internal, trusted sources. Whether an event is caused by intentional malicious behavior or a simple mistake, internal threats can be more disruptive and more costly than an external security breach.

This assessment focuses on vulnerabilities in your internal network and is conducted from within your trusted network with detailed procedures customized based on the infrastructure and environment. The first step is to conduct a workshop in order to identify critical networks and assets. This information is used to qualify risk and prioritize recommendations. The next step is to discover the internal systems and services that are exposed on the internal network. After the systems and services have been identified, they are scanned for known vulnerabilities. Using controlled attack simulation, your internal vulnerabilities are exposed, validated, and assessed.

Perimeter Security Posture Assessment

The Perimeter Security Posture Assessment identifies the security risk associated with your organization's Internet, partners, customer, and remote worker connectivity and services. It identifies vulnerabilities that can allow inappropriate access to your internal IT infrastructure from the outside.

Cisco experts begin by remotely scanning for the presence of systems and services accessible through the external connections. They identify the number of active systems and devices (including hosts behind filtering devices such as firewalls) and scan TCP and UDP ports to determine if any services are externally visible. They also research and confirm potential target systems, services, devices, and applications.

Following the identification of externally accessible systems and services, Cisco consultants conduct a remote vulnerability scan of your organization's Internet and extranet presence using specialized tools with capabilities that extend beyond those of standard commercial tools. The engineers analyze the results to remove false positives and determine which critical assets are at risk.

Security Architecture Assessment

Security infrastructures and architectures may be deployed in many different configurations in order to achieve the same security goal. This flexibility makes it difficult to assess the effectiveness of the security infrastructure by focusing on individual controls. The metrics-based assessment methodology of this service focuses on assessing the security business goal directly, independent of the supporting technical and operational controls.

Focusing on your critical business assets, the Cisco Security Control Framework is used to evaluate the network architecture from the foundational security objectives of visibility and control. Through the lenses of the supporting security actions for identify, monitor, correlate, harden, isolate, and enforce, the collected data and information are presented in the form of security metrics that measure the capabilities and effectiveness of the currently deployed technical and operational controls.

The Cisco Security Architecture Assessment allows you to implement a comprehensive security architecture by:

- Identifying the critical business assets and network infrastructure that supports those assets
- Highlighting security gaps and risks in your infrastructure
- Providing a prioritized set of actionable steps to remediate risks

This assessment is appropriate for Cisco and multivendor infrastructures supporting the core routing, switching, and wireless network infrastructure and the primary functional domains such as the perimeter and edge networks.

Cisco security experts begin by conducting a detailed review of your security goals, identifying critical assets and gathering business and technical requirements. Based on this information, they complete an in-depth analysis of your security infrastructure, including the network topology, network devices, security devices, and the processes around them. Additionally they provide an evaluation of your overall security architecture for scalability, performance, and manageability.

Working from carefully gathered data about your infrastructure, Cisco engineers are able to identify vulnerabilities and operational risks in your architecture by performing a thorough analysis of its alignment with industry best practices. Engineers then provide prioritized and actionable recommendations to mitigate the identified operational risks, including improvements to topology, protocols, policy, device configurations, and management tools. By taking this comprehensive approach to assessing the security infrastructure, these services help your organization improve risk management and satisfy compliance needs by reducing threats to the confidentiality, integrity, and availability of business processes and information.

Security Technology Readiness Assessment

As you prepare to implement a new Cisco security solution, it is important to determine if your existing network, operations, and management tools are capable of supporting the solution requirements. The security technology readiness assessment helps you understand any changes that might be required to smoothly integrate a new solution with your existing network.

Network engineers analyze deployment requirements and assess the readiness of your network devices, operations, and architecture to support the proposed solution. In addition to identifying components that do not support the systems capabilities, security engineers determine if your network topology supports a scaled deployment and deliver an effect analysis detailing requirements for redundancy, scalability, and hardware and software upgrades.

The readiness assessment recommendations provide you with the necessary information to design your Cisco security solution to work within your existing network. By identifying gaps in your existing infrastructure and developing a design that can fill those gaps, you can accelerate deployment time, avoid costly mistakes, and decrease the need for expensive rework of your network infrastructure.

Security Design Support

Even when your organization understands the threats facing your network, adapting a network security design to deal with them can be difficult. A flawed design can reduce the effectiveness of new security solutions, delay deployment, and increase integration costs.

Cisco consultants can work with your organization to develop a strong security design. The Cisco design methodology considers all aspects of your network security and its integration with your core network infrastructure. Using an in-depth, architectural approach based on industry standards, we can help develop a multilayer defense that's right for your organization.

Taking an architectural approach, we design and build your security infrastructure to last and to evolve over time, supporting the deployment of new business applications. We specify a common set of security design principles, policies, and practices that can be replicated across your organization. This helps you save time and money on network security administration, lowering your network's total cost of ownership.

Cisco network security experts collaborate with you to review your organization's business strategy and related security goals, requirements, and standards. We analyze your network security design in depth to determine its potential for meeting your business and IT strategies. Based on analysis of the network information gathered, Cisco engineers review your network vulnerabilities in detail, helping evaluate the security design against proven industry network security design leading practices.

After evaluating the existing network design for vulnerabilities, our engineers identify and prioritize security requirements for security solutions, including intrusion detection, admission control, remote access, endpoint protection, threat mitigation, perimeter control, and VPNs. Cisco recommendations may include improvements to your security infrastructure design, such as network topology, device placement, and connectivity. Taking into consideration all the aspects of your network security, including scalability, performance, and manageability, Cisco can recommend improvements to protocols, policies, and features for individual security components.

Security Performance Tuning

Today's advanced security solutions must be carefully deployed, configured, tuned, and integrated into the network infrastructure to perform effectively. Ongoing system analysis is important in maintaining consistent policy enforcement for solutions that are customized to your unique environment, consistent with your organization's security policy, and performing optimally.

The security performance tuning support provides periodic, ongoing system analysis design to maintain a secure, high-performance network that helps your IT staff more rapidly validate threats, subvert security incidents, and maintain compliance.

By analyzing device configurations and policy implementation and comparing them against Cisco leading practices, Cisco security experts will provide recommendations on how to get the most out of your security solution, resulting in a stronger alignment between your corporate security policies and procedures and the performance of your security devices.

Security Change Support

The ability to make changes to your security infrastructure quickly and efficiently is one of the keys to maintaining a secure network. Proactively identifying potential issues and rapidly resolving unforeseen events can result in a more effective and secure network.

Cisco security experts can support you as you make changes to your security solution. Cisco engineers can review proposed changes, implementation plans, test plans, and rollback plans for your advanced security technologies, helping you reduce risk while making changes that can improve your network security.

Because our security engineers are familiar with your security infrastructure and have experience with many security technology deployments, they can help you manage technical challenges and resolve deployment issues quickly and efficiently to reduce the potential effects on your network and business.

Security Knowledge Transfer

Keeping your network security staff up-to-date with new technologies and the state of network security can be the difference between a network that is secure from threats and one that is exposed to them. Security knowledge transfer is designed to help you increase your employees' self-sufficiency, giving them the knowledge they need to adapt to rapidly changing competencies required of today's network security professionals. Cisco security experts can transfer information through a series of customized sessions using a variety of media, including teleconferencing, video-on-demand presentations, virtual online classrooms, and instructor-led chalk talk and classroom sessions.

Our security engineers maintain regular communication with your staff through conference calls and email. This ongoing interaction augments the more structured training classes and facilitates general knowledge transfer through the lifecycle of your network.

Summary

The Cisco Security Optimization Service can help you to respond to evolving security threats and unexpected incidents by proactively strengthening your network infrastructure through strategic planning, architectural assessments, design, performance tuning, and ongoing optimization support. (See Table 1.)

Table 1. Cisco Security Optimization Service Summary

Service	Activities & Deliverables
Security Technology Planning Support Proactively manage security risk with expert planning, analysis, and decision making.	<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 Assessment Identify gaps in the network infrastructure and processes by focusing on the business goals, critical assets, and security objectives. Assess the actual business security goals using holistic metrics to understand the underlying architectural issues and gaps and make recommendations to remediate those gaps.	<ul style="list-style-type: none"> • Identify primary business assets • Network discovery • Interviews and metric collection • Security architecture analysis • Gap analysis with recommendations • Security architecture assessment report
Security Posture Assessment Identify vulnerabilities in your internal and perimeter network, and the effectiveness of your security controls. Measure the extent to which the identified vulnerabilities can be utilized to achieve unexpected or unauthorized access to the OS or applications on IP-connected endpoints (UNIX/Windows/network and security devices).	<ul style="list-style-type: none"> • Discovery to identify systems and services visible to the Internet • Scan TCP and UDP ports on identified devices. • Penetration testing to confirm the presence of vulnerabilities • Detailed analysis to identify critical vulnerabilities • Prioritized list of discovered risks with recommended actions • Security posture assessment report
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.	<ul style="list-style-type: none"> • Security discovery workshop • Effect analysis of proposed solution deployment • Security technology readiness assessment report
Security Design Support Improve the reliability, maintainability, and performance of your solution design.	<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 Proactively optimize advanced solutions with ongoing analysis of system configuration and policy implementation.	<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 Mitigate costly delays and problems during critical changes to the security infrastructure.	<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 Continuously improve the skills of your staff with ongoing interactive continuous learning and training sessions.	<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 email communication

Why Cisco Services

Cisco engineers are experts in securing networks and the types of threats facing today's networks. Cisco has developed proven methodologies for optimizing security system performance based on years of securing some of the most complex networks in the world.

Realize the full business value of your technology investments more quickly with intelligent, personalized services from Cisco and our partners. Backed by deep networking expertise and a broad ecosystem of partners, Cisco Services enable you to successfully plan, build, and run your network as a powerful business platform. Whether you are looking to quickly seize new opportunities to meet rising customer expectations, improve operational efficiency to lower costs, mitigate risk, or accelerate growth, we have a service that can help you.

For More Information

For more information about Cisco Security Services, visit www.cisco.com/go/services/security or contact your local account representative.

Cisco Services.

Making Your Business
Work Smarter.



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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)