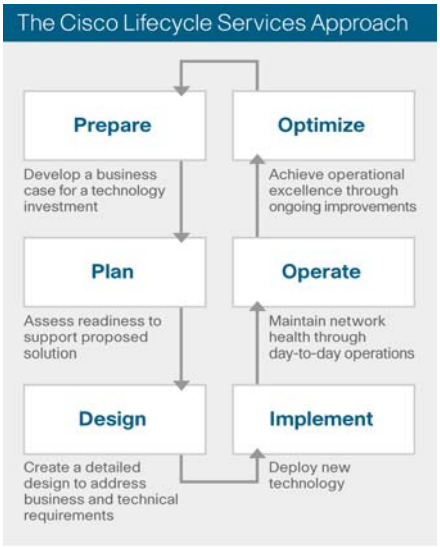
Cisco Security Optimization Service

Proactively strengthen your network to better respond to evolving security threats and planned and unplanned events.

Service Overview



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.

Maintaining strong defenses to protect your business applications and assets is a constant challenge. From viruses to phishing to Trojans to intrusions, the evolution and complexity of threats must be addressed with proactive IT risk management and security strategies that minimize downtime, loss, and damage to corporate systems. By taking a proactive approach to security, you can gain confidence that your security infrastructure is providing a robust, comprehensive defense in the face of evolving business requirements.

Experts no longer view security as a single product or solution, but rather as an in-depth system that must be integrated throughout the network. The best way to manage network security risk is through a systematic, architectural approach that addresses the entire network lifecycle and is built upon a standards-based infrastructure. Your organization can reduce the likelihood of severe service disruptions or compromised business assets and applications through continuous evaluation and strengthening of network security.

The Cisco Security Optimization Service supports you as you continually evolve your security system to meet ever-changing threats and compliance requirements. The Cisco Security Optimization Service employs a range of expertise, tools, and methodologies to proactively evaluate and strengthen the network's ability to prevent, detect, and mitigate threats. With this service, your organization can work with Cisco security experts to:

- Create a trusted, resilient security infrastructure
- Optimize your network security to evolve as your business changes
- Invest strategically in system-level solutions

The Cisco Security Optimization Service is an integrated service offering designed to assess, develop, and optimize your security infrastructure on an ongoing basis. With the help of expert planning, specialized tools, quarterly site visits, and continual analysis and tuning, the Cisco security team builds an in-depth knowledge of your security infrastructure. Aided by this knowledge, the Cisco engineering team becomes a highly effective trusted advisor supporting your organization with deep security technical expertise and intellectual property.

Through a combination of strategic planning, architectural reviews, and ongoing 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. With assistance from Cisco security experts, this service enables your IT staff to perform analysis of strategic initiatives to proactively provide long-term business security and risk management, as well as near-term tactical solutions to evolving security threats and intrusions.

Whether your focus is on rolling out a new security solution, fine-tuning the existing security infrastructure, or creating an enterprisewide security architecture, Cisco security experts can guide your decisions to better protect your business. With the Cisco Security Optimization Service, Cisco security experts regularly evaluate your solution design, security policy implementations, and critical device configurations and make recommendations to help you optimize your security infrastructure cost-effectively. This level of support assists your organization in prioritizing areas of improvement and reducing risk when making changes to the security infrastructure.

The Cisco Security Optimization Service includes eight deliverables:

- Security technology planning support
- Security architecture review
- Security posture assessment (external)
- Security technology readiness assessment
- Security design support
- Security performance tuning
- Security change support
- Security knowledge transfer

Security Technology Planning Support

Evolving applications, solutions, services, and security threats require your organization to constantly reevaluate the effectiveness of the defenses in place. Even with a skilled network security staff and well-developed policies, staying abreast of emerging vulnerabilities and security best practices can be extremely difficult.

With Cisco’s help, your organization can meet these challenges by taking a proactive approach to security risk management and implementing a comprehensive security plan. With ongoing decision-making assistance from Cisco security experts, your organization can better mitigate risks, allow for more effective protection in the short term and long term, and increase the return on your network security investment.

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.

Security Architecture Review

Your security architecture must provide a robust, comprehensive defense to protect your critical business services and assets. As the network architecture evolves over time, network security technologies must remain aligned with security policy and compliance requirements.

The security architecture review provides a detailed evaluation of your organization's network security architecture, technology policy, and management practices. This analysis allows your organization to strengthen its network security infrastructure by providing multilayer "defense-in-depth" network protection, avoid unexpected costs, and reduce compliance exposures. The service identifies vulnerabilities and recommends improvements to better align the security architecture with the International Organization for Standardization (ISO) 17799 security model, industry best practices, and your organization's security policy.

With the security architecture review, your organization can:

- More effectively protect your network by identifying vulnerabilities and deviations from security best practices and policy
- Help achieve compliance requirements by identifying internal controls and procedures needed to better protect data from unauthorized access
- Extend your network investment by expanding the security capabilities of the existing infrastructure
- Lower your operating costs through the consistent deployment of security policy and procedures

During the course of the review, Cisco network security experts examine your network security goals and requirements and your security technology policy in detail. We provide an in-depth analysis of your network security architecture, including the network topology, solution components, device features, and configurations. We evaluate your security technology policies for remote access, network segmentation, server protection, authentication, and firewall design. In addition, we evaluate your overall security architecture for scalability, performance, and manageability.

Based on this analysis, our engineers provide you with a detailed analysis of network security architecture vulnerabilities and operational risks, and evaluate how closely your security architecture aligns with proven industry network security best practices. The team then provides prioritized recommendations to mitigate the identified operational risks, including improvements to topology, protocols, policy, device configurations, and network and security management tools.

Taking a systematic and detailed approach to assessing network security helps your organization manage risk; satisfy compliance requirements; and reduce threats to the confidentiality, integrity, and availability of business processes and information.

Security Posture Assessment (External)

Your organization's critical business applications and data need protection from external security

intrusions. Building robust security defenses requires a clear understanding of the current vulnerabilities of your network, applications, and systems.

The external security posture assessment identifies the security risk associated with your organization's Internet-connected systems and services. These vulnerabilities can allow outside, untrusted networks to gain access to your internal, trusted networks, applications, and systems.

With the external security posture assessment, your organization can:

- Proactively identify Internet vulnerabilities that pose a risk to your networks, systems, and information
- Improve the overall security state of your network by acting on prioritized recommendations to protect devices, systems, and applications
- Improve compliance with federal and state regulations that require security assessments
- Reduce the time and resources it takes to stay current with new and emerging vulnerabilities

We begin by conducting a remote vulnerability scan of your organization's Internet presence using specialized, automated tools with capabilities that extend beyond those of standard commercial tools. After confirming registration of Internet devices, Cisco experts scan for externally visible services. We carefully search for inherent and well-known vulnerabilities in network services that can lead to security breaches. The assessment simulates typical attack activities but in a safe, controlled manner.

The assessment provides you with a detailed analysis of simulated attacks used. It identifies critical vulnerabilities and compares the results with recommended industry best practices and policies, as well as with your operational requirements. Cisco then prioritizes the discovered risks and provides you with recommended actions, which can both improve the security state of your network and meet your organizational security goals.

Security Technology Readiness Assessment

As you prepare for implementing 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 may be required to smoothly and readily integrate a new solution with your existing network.

With the security technology readiness assessment, your organization can:

- Reduce solution implementation and migration times by anticipating resource and technical requirements and more effectively planning for required infrastructure changes
- Increase overall network administration and IT staff productivity by enabling the deployment of an integrated, consistent solution
- Enhance solution performance, resiliency, and availability by using the correct set of hardware, software releases, features, and functions

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 impact 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 technologies 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

It has never been more important to protect your corporate network. 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 against directed attacks from hackers or indiscriminate attacks from viruses and worms.

With security design support, your organization can:

- Develop a customized network security design that provides a multilayer defense
- Improve the reliability, maintainability, and performance of security solution
- Mitigate costly delays and problems during design, implementation, and deployment of new technology

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 best 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. Many advanced technologies such as intrusion prevention, network admission control, and automated monitoring and response systems use a policy-based approach to blocking security attacks, so your organization's business goals and security policies must be tightly integrated into the solution from the beginning.

Because technologies, business processes, and network threats are always changing, your organization's security posture never remains static. 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.

Security performance tuning support can help your organization:

- Optimize your security system through ongoing analysis of configuration best practices and policy implementation
- Better align network performance with corporate security policy and procedures
- Improve system performance by recommending improved policy configuration and tuning

Cisco security performance tuning support provides ongoing analysis and tuning of policy-based solutions such as Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS), Cisco Network Admission Control (NAC), and Cisco Security Agent, and recommends changes to help you use your equipment in the most cost-effective way that is consistent with your organization's security policy. By analyzing device configurations and policy implementation and comparing them against Cisco best 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 planned and unplanned changes to your security solution. As part of this service, 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.

Security change support can help your organization:

- Mitigate costly delays and problems during critical changes to the security infrastructure
- Review implementation, test, and rollback plans to help solution deployment changes occur smoothly
- Quickly diagnose any problems that may occur during a change window, providing expert assistance to rapidly resolve unforeseen network service disruption

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

The skills and technologies needed to effectively secure your network are constantly changing. 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. To help reduce your ongoing operational expenses, you need to continually improve the skills of your network support organization.

Security knowledge transfer and mentoring support 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.

Topics, training methodologies, and delivery times are determined in a collaborative manner and may include the following:

- Technology updates
- Detailed product and technology information
- Engineering white papers
- Operational guidance
- Technical tips for performance tuning

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

Table 1. Cisco Security Optimization Service Summary

Activities	Deliverables
Security Technology Planning Support	• 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	• Security architecture workshop • Security architecture analysis • Gap analysis with recommendations • Security architecture review report
External Security Posture Assessment	• 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	• Security discovery workshop • Impact analysis of proposed solution deployment • Security technology readiness assessment report

Activities	Deliverables
Security Design Support	• Security design and discovery workshop • Security design review including gap analysis and recommendations • Detailed security design report
Security Performance Tuning	• Security device discovery • Analysis of baseline configuration template • Device configuration analysis, including tuning requirements • Iterative performance tuning • Security performance tuning report
Security Change Support	• 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	• 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

Benefits

Cisco engineers are experts in securing networks. Each engineer possesses an intimate knowledge of Cisco advanced security technologies such as intrusion detection, admission control, remote access, endpoint protection, threat mitigation, perimeter control, and virtual private 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. Our engineers also possess a deep understanding of the types of threats facing today’s networks.

The Cisco Security Optimization Service can help you to respond to evolving security threats and planned and unplanned events by proactively strengthening your network infrastructure through strategic planning, architectural assessments, design, performance tuning, and ongoing optimization support.

In summary, these services provide:

- **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.

Why Cisco Services

Cisco Services make networks, applications, and the people who use them work better together.

Today, the network is a strategic platform in a world that demands better integration between people, information, and ideas. The network works better when services, together with products, create solutions aligned with business needs and opportunities.

The unique Cisco Lifecycle Services approach 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.

For More Information

For more information about Cisco Security Optimization Services, visit http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html or contact your local account 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.**

Printed in USA C78-413039-00 6/07

