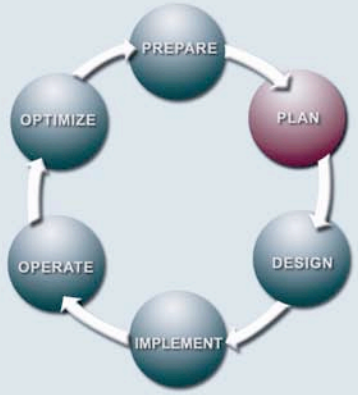
# Cisco Security Posture Assessment Services

**Identify, analyze, and validate network security vulnerabilities that can threaten your business**

## 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

To protect your critical business applications and data from security intrusions, your organization needs comprehensive, in-depth network security. However, building robust security defenses requires a clear understanding of the current vulnerability state of your network, applications and systems. As part of the plan phase of the Cisco® Lifecycle Services approach, Cisco Security Posture Assessment Services, designed for large enterprises, provide a detailed vulnerability assessment of network devices, servers, desktops, web applications, and databases in the network.

Cisco Security Posture Assessment services consist of the following three services:

- **Cisco External Security Posture Assessment Service -** Identifies vulnerabilities that allow outside, untrusted networks to gain access to internal, trusted networks and systems and recommends solutions for improvements
- **Cisco Internal Security Posture Assessment Service** - Identifies the steps you must take to thwart intentional attacks or unintentional mistakes from trusted internal users and systems
- **Cisco Wireless Security Posture Assessment Service** - Identifies risks and points of exposure in your wireless infrastructure and recommends solutions to address them

Together, these services provide proactive protection of your IT infrastructure by identifying vulnerabilities in the network, web applications, and Internet perimeter and prioritizing corrective actions to protect the confidentiality, integrity, and availability of your organization's assets and information.

Because technologies, business processes, and network threats are always changing, your organization's security posture never remains static. Many organizations perform periodic security posture assessments to assess the evolving state of your business's network security. Ongoing assessments can help you maintain a more up-to-date picture of their current network security posture.

With Cisco Security Posture Assessment services, your organization can:

- Reduce the risk of intentional or accidental access to IT assets and information
- Identify security vulnerabilities in your network infrastructure
- Develop a prioritized list of steps required to fix identified vulnerabilities
- Improve compliance with federal and state regulations that require security assessments
- Reduceg the time and resources trying to stay current with new and emerging vulnerabilities
- Validate current security policies and practices against industry best practices and verifying areas that require security budget or staffing

- Receive an independent, third-party security assessment that strengthens your organization's security policy and compliance efforts

## CISCO EXTERNAL SECURITY POSTURE ASSESSMENT SERVICE

### Identifying Vulnerabilities in Internet-Connected Networks and Services

The Cisco External Security Posture Assessment identifies the security risk associated with your organization's Internet-connected systems and services by identifying vulnerabilities that can allow outside, untrusted networks to gain access to your internal, trusted networks, applications, and systems.

Cisco Systems® experts 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. Because most services have inherent and well-known vulnerabilities, Cisco engineers determine if these services are at risk by manually confirming vulnerabilities that can lead to security breaches. The service simulates activities typical of malicious attackers in a safe, controlled manner in an attempt to compromise perimeter devices and Internet security controls providing the in-depth analysis needed to identify and validate vulnerabilities. (See Table 1.)

**Table 1.** Cisco External Security Posture Assessment Activities, Methodology and Deliverables

| Activities | Methodology and Deliverables |
|---|---|
| • Identify and confirm the presence of systems and services visible to the Internet by:<br>– Identifying the number of active systems and devices, including hosts behind filtering devices such as firewalls<br>– Scanning TCP ports and User Datagram Protocol (UDP) ports to determine if any services are externally visible<br>– Researching and confirming potential target systems, services, devices, and applications<br>• Emulate typical hacker activities through nondestructive means, to confirm the presence of vulnerabilities and the level of unauthorized access<br>• Provide a detailed analysis of simulated attacks to identify critical vulnerabilities and compare assessment results with recommended industry best practices and policies, as well as the operational requirements of the organization<br>• Prioritize the discovered risks and provide recommended actions to improve the security state of your network and meet your organizational security goals | **Methodology**<br>• Gather and review your network documentation<br>• Identify target systems and services visible to the Internet<br>• Conduct automated vulnerability testing against the targets<br>• Analyze vulnerability data and validate the presence of the vulnerabilities<br>• Provide vulnerability analysis and recommendations<br>• Provide an onsite executive presentation of findings and recommendations<br>**Deliverables**<br>The External Security Posture Assessment Report. This deliverable typically:<br>• Prioritizes the discovered vulnerabilities and identifies the most critical findings<br>• Provides vulnerability analysis and statistics for individual systems and services<br>• Provides recommended actions to improve the security state of the network to meet the your security goals |

### Benefits

With the Cisco External Security Posture Assessment, your organization can:

- Proactively identify Internet security vulnerabilities that pose a risk to your networks, systems, and information
- Act on prioritized recommendations to protect devices, systems, and applications from unauthorized access
- Effectively simulate an external attacker to confirm the risks posed by hackers or malicious Internet users
- Test current Internet security safeguards to help ensure that malicious activity is not successful at penetrating or disrupting service
- Improve the overall security state of your network by providing recommended actions to mitigate identified vulnerabilities

## CISCO INTERNAL SECURITY POSTURE ASSESSMENT SERVICE

**Exposing Security Weaknesses in Internal Networks, Applications, and Processes**

Although external network security incidents occur more frequently, 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.

The Cisco Internal Security Posture Assessment is a controlled attack simulation to gauge the exposure of systems, applications, and network devices within the internal, trusted network. Through the course of the assessment, Cisco engineers take an in-depth approach to gaining unauthorized access to your internal resources. (See Table 2.) This approach includes both automated vulnerability identification and secondary exploitation through simulation of a real intruder's attack in a controlled, safe manner to manually confirm vulnerabilities. This secondary exploitation can include targeting trusted relationships between hosts, revealing password weaknesses, and gaining administrative access to your systems – providing a structured approach to identifying vulnerabilities that otherwise might go undetected.

Cisco experts then provide a report describing the strengths and weaknesses found in the test scenarios, with recommendations for improvements. By identifying the steps needed to thwart intentional attacks or unintentional mistakes from trusted insiders, the Cisco Internal Security Posture Assessment helps you better secure valuable information assets.

**Table 2.** Cisco Internal Security Posture Assessment Activities, Methodology and Deliverables

| Activities | Methodology and Deliverables |
|---|---|
| Identify the presence of vulnerabilities on the internal network by:<br>● Performing a ping sweep on the network to identify devices, operating systems, and applications<br>● Scanning critical and well-known TCP and UDP ports on identified hosts<br>● Confirming the existence of identified vulnerabilities<br>Exploit system, application, and network device vulnerabilities by simulating a controlled network attack by:<br>● Performing secondary exploitation of trust relationships between hosts<br>● Exploiting user-caused problems such as use of the same password in Windows, Novell, and UNIX<br>● Exploiting information gathered from penetrated systems, applications, and devices<br>● Attempting to crack password files and gain administrator (Windows), root (UNIX), or supervisor (Novell) access<br>Analyze the test data to identify critical vulnerabilities and compare assessment results with recommended security practices you're your organizational security policies | **Methodology**<br>● Gather and review your network documentation<br>● Identify and confirm all vulnerabilities<br>● Conduct primary and secondary vulnerability testing<br>● Analyze vulnerability data and validate the presence of vulnerabilities<br>● Provide vulnerability analysis and recommendations<br>● Provide an onsite executive presentation of findings and recommendations<br>**Deliverables**<br>The Internal Security Posture Assessment Report. This deliverable typically:<br>● Prioritizes the discovered vulnerabilities and identifies the most critical findings<br>● Provides vulnerability analysis and statistics for individual systems and services<br>● Provides recommended actions to improve the security state of the network to meet your organization's security goals |

### Benefits

With the Cisco Internal Security Posture Assessment, your organization can:

- Acquire a cost-effective, unbiased assessment of your internal information security risk
- Identify critical security threats that pose a risk to your devices, systems, and applications within your corporate "trusted" network
- Effectively simulate an internal attacker to quantify the risks posed by a disgruntled employee or contractor
- Validate internal security policies and practices against industry best practices
- Improve the overall security state of your network by taking recommended actions to mitigate vulnerabilities

## CISCO WIRELESS SECURITY POSTURE ASSESSMENT SERVICE

**Quantifying Security Risks and Vulnerabilities in Wireless Networks**

Wireless technology and services must be fully integrated into your organization's security framework and provide the same level of privacy and protection as the wired infrastructure. The Cisco Wireless Security Posture Assessment evaluates your wireless architecture and configurations to identify points of exposure, locate unauthorized access points, and recommend solutions to strengthen the security state of your wireless infrastructure.

Cisco experts begin by surveying your premises to discover and map all available access points. (See Table 3.) By comparing the access points found as well as data gathered during the site survey against a list of authorized devices, Cisco engineers can identify possible rogue devices. Cisco engineers then compare your wireless network architecture and configuration to industry best practices, documenting known vulnerabilities and threats.

Moving outside your organization's facilities, the assessment also uses sophisticated wireless antennas to seek wireless LAN (WLAN) traffic leaking from buildings. If necessary, Cisco engineers move into controlled areas of your building to continue seeking WLAN traffic. After such traffic is discovered, engineers determine the encryption and authentication method used and attempt to gain access to the LAN segment.

**Table 3.** Cisco Wireless Security Posture Assessment Activities, Methodology, and Deliverables

| Activities | Methodology an Deliverables |
|---|---|
| Identify, validate, and confirm the presence of vulnerabilities on the WLAN network. Activities typically include:<br>• Examine the wireless access point configurations and compare them against recommended security practices<br>• Locate WLAN traffic leaking from customer buildings by deploying sophisticated wireless antennas<br>• Map signal coverage with Global Positioning System (GPS) technology to plot areas where WLAN traffic is detected<br>• Check for signal visibility and strength in public areas inside buildings, and in controlled areas of buildings if necessary, if no WLAN traffic is detected outside the buildings<br>• Determine if Wired Equivalent Privacy (WEP) encryption is enabled or if wireless traffic is being transmitted without encryption<br>Confirm vulnerabilities on identified security weaknesses to more effectively determine the level of unauthorized access. Activities typically include:<br>• Attempts to decipher WEP<br>• Attempts to obtain customer IP addresses and evaluate the security of the access points<br>Analyze the test data to identify critical vulnerabilities and compare wireless assessment results with recommended security practices and organizational security policies | **Methodology**<br>• Gather and review customer network documentation<br>• Identify and confirm all vulnerabilities<br>• Conduct primary and secondary vulnerability testing<br>• Analyze vulnerability data and validate the presence of vulnerabilities<br>• Provide vulnerability analysis and recommendations<br>• Provide an onsite executive presentation of findings and recommendations<br>**Deliverables**<br>The Wireless Security Posture Assessment Report. This deliverable typically summarizes:<br>• Prioritizes the discovered vulnerabilities and identifies the most critical findings<br>• Provides vulnerability analysis and statistics for individual systems and services<br>• Provides recommended actions to improve the security state of the network to meet your organization's security goals |

### Benefits

With the Cisco Wireless Security Posture Assessment, your organization can:

- Identify critical wireless security risks such as information leakage, unauthorized access points, and misconfiguration of WLAN devices
- Effectively simulate a wireless attacker to quantify the risks posed by a malicious drive-by scanner
- Protect proprietary information by identifying the potential for unauthorized access and identifying fixes to reduce vulnerabilities
- Prioritize specific recommendations for strengthening security configurations of WLAN devices

- Validate internal security policies and practices against industry best practices for your wireless network infrastructure
- Strengthen the overall security state of your wireless network through the development of a roadmap that prioritizes recommended improvements

With the Wireless Security Posture Assessment, management and network administrators are demonstrating a commitment to improving overall wireless infrastructure security. This continued commitment to enhancing the security state of the wireless network will increase your confidence in the security of your systems and data.

## WHY CISCO

Hackers, malicious Internet users, and internal threats to your network and business assets never rest. Likewise, the security posture of your network, systems and applications never remains static. In order to preserve critical business services, safeguard customer trust and loyalty, and decrease the costs of potential network attacks, you must continually assess the evolving security state your business's security with ongoing assessments that keep you up-to-date on your current security posture.

As part of the Cisco Lifecycle Services approach, Cisco Security Posture Assessment services provide a critical first step in helping to ensure pervasive network protection. With a detailed evaluation of the current state of network security, your organization can achieve a clear picture of its security strengths and vulnerabilities and develop a detailed plan for more effectively protecting your business.

## AVAILABILITY AND ORDERING

Cisco Security Posture Assessment services are available through Cisco and Cisco partners globally. Details may vary by region.

## FOR MORE INFORMATION

For more information about Cisco Security Posture Assessment services or the Cisco Lifecycle Services approach, contact your Cisco representative.


**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.
168 Robinson Road
#28-01 Capital Tower
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 Website at** www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica Croatia • Cyprus • 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




Printed in the USA C78-332592-00 02/06