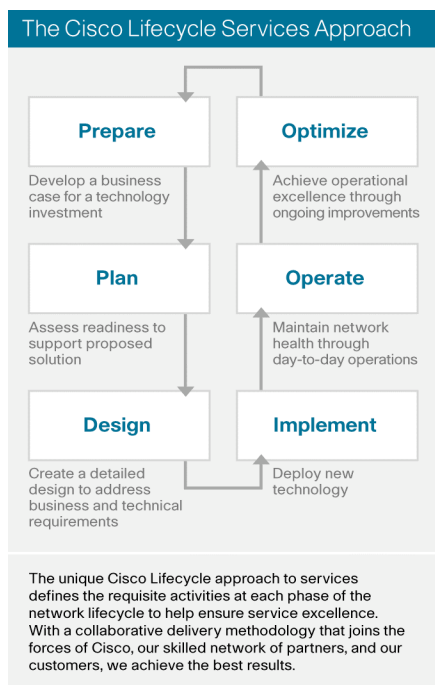


# Cisco Security Posture Assessment Service

Protect Your Organization's Infrastructure Security Through Active Testing



## Service Overview

To protect your critical business applications and data from security intrusions, your organization needs comprehensive, in-depth infrastructure security. Building a robust security defense requires a clear understanding of the current vulnerability state of your network, applications, systems, and network-connected devices.

Because technologies, business processes, and threats are always changing, your organization's security posture never remains 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 Service provides a point-in-time validation of how well the security architecture and designs have been implemented and are being operated. This service provides a detailed assessment of network devices, servers, desktops, web applications, and the related IT infrastructure. This assessment compares discovered vulnerabilities with industry best practices and up-to-date intelligence from the industry and Cisco; delivering a prioritized report based on risk to the organization with recommended actions for remediation.

## Service Solution

The assessments are performed by Cisco consultants, who draw on their extensive security experience in a variety of vertical industries and government agencies. This expertise is supported by a combination of best-in-class tools, methodologies, and superior access to Cisco product development engineers to help you make the most of the sophisticated security features included in your Cisco products. Exploitable vulnerabilities are evaluated using data from the Cisco Security Intelligence Operations, which is composed of more than 500 research analysts dedicated to the round-the-clock collection and analysis of threat intelligence.

By gathering data from upward of one million security devices and 10 million desktop clients, Cisco Security Intelligence Operations are uniquely positioned to provide the global reach and security expertise necessary for successful global threat correlation. Using the gathered data, Cisco maintains an up-to-date threat database by analyzing information from more than two million URLs per day, 30 percent of the world's web and email traffic, 40,000 security alerts, and 3300 vulnerability signatures.

Cisco security experts begin by conducting a detailed review of your security goals and requirements. Based on this information, they scan and probe the IT infrastructure from the interior and perimeter, survey and map your wireless network, and attempt to socially engineer their way into your facility. This analysis is done in a safe and controlled manner by simulating activities typical of malicious attackers. The engineers then analyze the discovered vulnerabilities and compare them with industry best practices and up-to-date information from Security Intelligence Operations to remove false positives. Based on the confirmed vulnerabilities, the engineers analyze the results to

determine which critical assets and data are exposed. The prioritized and actionable results of the analysis are then delivered to your organization in a formal report and executive presentation.

By taking this comprehensive approach to assessing the current state of your security infrastructure, this service provides your organization with the information it needs to understand and improve its security posture. (See Table 1.)

**Table 1.** Cisco Security Posture Assessment Service Activities and Benefits Summary

Activities and Deliverables Summary	Benefits Summary
<ul style="list-style-type: none"> <li>• Identify and confirm the presence of security vulnerabilities in your IT infrastructure through expertise, tools, and the data from Cisco Security Intelligence Operations</li> <li>• Emulate typical malicious activities through nondestructive means to confirm the presence of vulnerabilities and the level of unauthorized access that they can expose</li> <li>• Provide a security posture assessment report containing:               <ul style="list-style-type: none"> <li>◦ A detailed analysis of simulated attacks to identify critical vulnerabilities</li> <li>◦ Comparison of assessment results with recommended industry best practices and your organization's operational requirements</li> <li>◦ Recommended prioritization of the vulnerabilities based on risk to the organization</li> <li>◦ Recommended actions to remediate the vulnerabilities and improve your organization's security posture</li> </ul> </li> <li>• Deliver onsite executive presentation of findings and recommendations</li> </ul>	<p>With the Cisco Security Posture Assessment Service, your organization can:</p> <ul style="list-style-type: none"> <li>• Reduce the risk of intentional or accidental access to IT assets and information</li> <li>• Test current infrastructure security safeguards to help ensure that malicious activity does not successfully penetrate or disrupt service</li> <li>• Proactively identify security vulnerabilities that pose a risk to your IT infrastructure</li> <li>• Prioritize resources to address vulnerabilities based on business risk</li> <li>• Improve the overall security state of your infrastructure by following recommended actions to mitigate identified vulnerabilities</li> <li>• Achieve improved compliance with regulations and industry mandates that require security assessments</li> <li>• Reduce the time and resources needed to stay current with new and emerging vulnerabilities</li> </ul>

In order to provide flexibility in matching your unique business, infrastructure, and budget requirements, the Cisco Security Posture Assessment Service can be customized to focus on various functional domains in your infrastructure.

There are four assessments that address different functional domains. They can be delivered independently or together based on your specific business objectives:

- Cisco Internal Security Posture Assessment
- Cisco Perimeter Security Posture Assessment
- Cisco Wireless Security Posture Assessment
- Cisco Physical Security Posture Assessment

### **Cisco 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 or sophisticated client-side attacks. 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 to your infrastructure and business needs. The first step is to discover the internal systems and services that are exposed on the internal network. This is typically done through ping sweeps and scanning of commonly exploited TCP and User Datagram Protocol (UDP) ports on identified devices. After the systems and services have been identified, they are scanned for known vulnerabilities using a combination of commercial and Cisco proprietary tools.

Using controlled attack simulation; your internal vulnerabilities are exposed, validated, and assessed. During the simulation, attempts are made to gain access including secondary exploitation of systems and services through compromised hosts. This secondary exploitation can include targeting trusted relationships between hosts, gathering infrastructure data from compromised systems, revealing password weaknesses, and attempting to crack password files to gain administrative access to your systems.

### **Cisco Perimeter Security Posture Assessment**

This assessment identifies the security risk associated with your organization's Internet, partner, 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.

### **Cisco Wireless Security Posture Assessment**

In order for 802.11 wireless technology and services to provide the same level of privacy and protection as the wired infrastructure, they must be fully integrated into your organization's security framework. If not properly secured, wireless networks can be one of the easiest ways for unauthorized users to access critical systems and information. This assessment helps you to prevent such security breaches by identifying points of exposure, including unauthorized access points, weak access control, and wireless data leakage vectors inside and outside your physical facilities.

Cisco experts begin by surveying your premises to discover and map all available access points. By comparing the discovered data against a list of authorized devices, Cisco engineers can identify possible rogue access points that might provide an entryway to your internal wired networks. Outside your organization's facilities, the assessment uses sophisticated wireless antennas to seek wireless LAN (WLAN) traffic that might be leaking from buildings. With your permission, Cisco engineers can enter controlled areas of your building to further identify unauthorized WLAN traffic. If such traffic is discovered, engineers determine the encryption and authentication method used and attempt to gain access to the LAN segment.

### **Cisco Physical Security Posture Assessment**

Controlling physical access to your network infrastructure is a critical component in the overall security of your infrastructure and critical data. The value of a secure network architecture and deployment is compromised if intruders can gain access to physical devices or other areas where sensitive data is stored. Gaining physical access to your facility, intruders might install network back doors, keystroke loggers, software to call home, and rogue access points or remove other sensitive data.

This assessment consists of a combination of onsite techniques where, with your permission, engineers attempt to gain access to your location to determine vulnerabilities. Multiple techniques help engineers understand the physical security posture of your locations, providing invaluable insight into lapses or security procedures that are missing altogether. Social engineering, impersonation, and tailgating are a few of the techniques utilized during a given engagement.

## Why Cisco Services

Cisco Services make networks, applications, and the people who use them work better together. The IT infrastructure works better when services, together with products, create solutions aligned with business needs and opportunities. The unique Cisco Lifecycle approach to services defines the requisite activities at each phase of the IT lifecycle to help ensure service excellence. With a collaborative delivery methodology that joins the forces of Cisco, our skilled partners, and our customers, we achieve the best results.

## Availability and Ordering

The Cisco Security Posture Assessment Service is available through Cisco and Cisco partners globally. Details might vary by region.

## For More Information

For more information about Cisco Security Services, visit [www.cisco.com/go/services/security](http://www.cisco.com/go/services/security) or contact your local account representative.

**Cisco Services.**  
**Making Networks Work.**  
**Better Together.**



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](http://www.cisco.com/go/offices).

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0903R)