



Cisco Security Architecture Assessment Service

Understand and Strengthen Your Agency's Infrastructure Security Architecture

An Architectural Approach to Security

Gain a comprehensive view of your security infrastructure:

- **Align security goals with agency objectives:** Identify and prioritize risks and remediation opportunities.
- **Use standards-based methodologies:** Use the Cisco Security Control Framework to gain visibility and control.
- **Reduce regulatory compliance exposure:** Increase the confidentiality, integrity, and availability of your business processes and information.
- **Customize your approach:** Select the architectural assessments that address your security requirements.

Introduction

In today's complex and ever-changing threat landscape, gaps in a security solution can place data integrity, information confidentiality, and mission-critical applications at risk. Your infrastructure needs integrated security controls that provide protection in a dynamic threat and vulnerability environment, while remaining aligned with security policy and compliance requirements.

Cisco security architecture assessments are conducted using the Cisco® Security Control Framework. This vendor-independent control framework is built from industry standards, security architecture principles, and Cisco engineering experience in securing enterprise infrastructures.

Focusing on the technology controls that support the foundational security objectives of visibility and control, the Cisco Security Control Framework is used to evaluate the architecture that protects your extended network infrastructure, attached devices, and business data. This framework is consistent with common security regulatory and industry compliance standards as well as international standards, including the International Organization of Standardization (ISO) 27000 series, the Federal Information Security Management Act (FISMA) best practices and audit requirements, and National Institute of Standards and Technologies (NIST) 800-53.

The Cisco Security Architecture Assessment Service allows you to implement a comprehensive security architecture by identifying gaps in your security infrastructure and providing a prioritized set of actionable steps to remediate them. The assessments are appropriate for Cisco and multivendor infrastructures for the core routing, switching, and wireless network; primary functional domains, including data center and unified communications; and the endpoints connected to the network. These security assessments can also provide an independent, unbiased snapshot of your implementation of the Trusted Internet Connections (TIC) initiative and migration to EINSTEIN II and III, helping to quickly prioritize next steps.

Assessment Process

The security architecture assessments are performed by Cisco consultants and engineers who draw on their extensive security experience in a variety of 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 Cisco network devices.

Cisco security experts begin by conducting a detailed review of your security goals and requirements. Based on this information, they complete an in-depth analysis of your security infrastructure, including the network topology, network devices, security devices, application devices, and endpoints. 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 FISMA, TIC, and EINSTEIN implementation objectives and 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, 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. (See Table 1.)

Table 1. Cisco Security Architecture Assessment Service Activity and Benefits Summary

Activity Summary	Benefit Summary
<ul style="list-style-type: none"> • Review security goals, objectives, and requirements • Review existing security architecture and design documentation, including physical and logical designs, network topology diagrams, device configurations, and blueprints as needed • For each functional domain included in the scope of the engagement, evaluate whether each of the recommended controls in the Cisco Security Control Framework is present in the security infrastructure • Evaluate the effectiveness of each technical control at providing the designated security function • Evaluate the security architecture for scalability, performance, and manageability • Identify vulnerabilities in the security infrastructure • Provide a report that documents control gaps, security risk analysis, and suggested steps for remediation • Provide a presentation of findings and prioritized recommendations 	<ul style="list-style-type: none"> • Create a robust and scalable security architecture using a mission-focused, risk-avoidance approach • More effectively protect your infrastructure by identifying architectural vulnerabilities and deviations from federal goals and security best practices • Safeguard employee productivity, primary intellectual property, and sensitive customer data by mitigating security risks • Address compliance requirements by improving internal controls to better protect data • Strengthen your staff's ability to prevent, detect, and respond to future threats • Protect your investment by extending the security capabilities of the existing infrastructure

In order to provide flexibility in matching your unique organizational, infrastructure, and budget requirements, the Cisco Security Architecture Assessment Service and the underlying Cisco Security Control Framework can be customized to focus on various functional domains in your infrastructure. The Internal Security Architecture Assessment is required; this assessment looks at your internal network functional domain and common security infrastructure controls. There are seven additional functional domains that can be assessed independently. The following section describes each of the functional domains and their associated assessments.

The Cisco Security Architecture Assessment Service includes one required and seven optional assessments:

- Internal Security Architecture Assessment*
- Perimeter Security Architecture Assessment**
- Unified Communications Security Architecture Assessment
- Wireless Security Architecture Assessment
- Data Center Security Architecture Assessment
- Endpoint Security Architecture Assessment
- Firewall Rules Assessment**
- Physical Security Architecture Assessment

* Required.

** Includes comparison to TIC initiative goals and objectives, as well as migration to EINSTEIN II and/or III.

Internal Security Architecture Assessment (Required)

Sophisticated cross-protocol client-side attacks that are launched internally are potentially more disruptive and costly than external security breaches. This service examines the security architecture in the internal network required to protect against these threats, including WANs and LANs for core, campus, and individual sites. It also covers common security infrastructure controls that apply to access control, identity management, network management, intrusion detection and prevention, security event management, and logging. This assessment is required because it creates a baseline for the other assessments.

Perimeter Security Architecture Assessment

Connecting your internal network to the Internet, partners, citizens, and your mobile workforce is necessary, but exposes your infrastructure, intellectual property, citizen data, and the availability of your core operational services to significant threats. This assessment evaluates the security architecture that protects the boundary between the internal network and external networks, including perimeter firewalls, access control devices, guest networks, employee remote access, and e-commerce sites.

Unified Communications Security Architecture Assessment

Unified communications is a critical business application. Any underlying security weakness surrounding your unified communications application can put you at risk for a variety of security breaches, including toll fraud, eavesdropping, voice spam, and denial-of-service attacks. This assessment addresses the security used to protect not only your unified communications environment, but also the underlying data network that carries your communications traffic. This includes the routing and switching infrastructure, applications, servers, and endpoints required to make and process your communications.

Wireless Security Architecture Assessment

Interception, rogue access points, weak encryption keys, and denial-of-service attacks can target your wireless LAN (WLAN) infrastructure. While wireless LANs produce significant productivity gains, if not correctly configured

they can be one of the easier locations in the infrastructure to exploit. Properly deploying and configuring your WLAN secures your wireless infrastructure to protect your confidential data and increase availability. This assessment addresses the security architecture that protects the wireless and associated infrastructure, including local and guest controllers, access points, and WLAN clients.

Data Center Security Architecture Assessment

Internal servers and data center hosts contain mission-critical information resources that are generally accessed by trusted users, but internal security is still a serious concern. Properly securing your data center protects it from internal attacks and provides an additional layer of protection in case an external attacker gains entry to your infrastructure. This assessment evaluates the primary data center technologies and components, including the storage network, server farm, services aggregation, core, distribution, access control, and host virtualization, so you can fully utilize your data center equipment securely.

Endpoint Security Architecture Assessment

Application servers and end-user devices are exposed to highly sophisticated threats, from productivity-affecting spam to socially engineered attacks that exploit human nature. Securing endpoint devices is a critical piece of the overall security of your infrastructure. This assessment evaluates the security architecture that protects the hosts and endpoints outside the data center, including laptops, desktops, servers, and other devices connected to the infrastructure.

Firewall Rules Assessment

Correctly configuring your infrastructure to segregate traffic, control access, and detect anomalous behavior can be challenging. It can be even more challenging to keep the configuration up to date as the infrastructure evolves to defend against new threats and to support new applications, services, acquisitions, and infrastructure upgrades. This assessment includes a deep analysis of the rules on your access control devices. The analysis provides added value when combined with other assessments that address the security architectures of other functional domains.

Physical Security Architecture Assessment

Controlling physical access to your facility is a critical component in the overall security of your infrastructure and confidential information. If intruders gain access to your infrastructure, they are in a position to install network back doors, keystroke loggers, software to call home, and rogue access points or compromise other deployed security measures. This assessment covers the controls related to the perimeter and internals of the building or campus, monitoring devices, environmental sensors, communications, and lighting.

Why Cisco Services

Cisco Services make networks, applications, and the people who use them work better together. Today, the network and related infrastructure are a strategic platform in a world that demands better integration between people, information, and ideas. The IT infrastructure works better when services, together with products, create solutions aligned with business needs and opportunities. Cisco's unique 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 network of partners, and our customers, we achieve the best results.



Availability and Ordering

Cisco Security Architecture Assessment Service is available through Cisco and Cisco partners globally. Details may vary by region.

For More Information

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

For more information on Cisco Federal Security solutions visit: www.cisco.com/go/fedsecurity

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco.Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, 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 Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.