Cisco IOS Software Cybersecurity Assessment and Enablement Service

Service Overview

Turn it on: Enable embedded Cisco IOS® Software cybersecurity features with the Cisco IOS Software Cybersecurity Assessment and Enablement Service. Take full advantage of Cisco's powerful core networking solutions to maximize productivity, efficiency, and reduce risk.

Cisco wants you to get the most out of equipment already deployed by enabling key Cisco IOS Software features to enhance your network protection. Understanding the existing capabilities in your routers and switches and enabling them can help to reduce your security risk. The Cisco IOS Software Cybersecurity Assessment and Enablement Service provides expertise to take full advantage of powerful Cisco® core networking solutions to maximize your productivity, efficiency, and technology investment. An assessment will be conducted to recommend and provide guidance on enabling one or all of the following existing feature sets:

- Cisco IOS Software IP service level agreements (SLAs) enable customers to assure mission-critical IP applications and IP services that utilize data, voice, and video in an IP network. Cisco has augmented traditional service level monitoring and reinvented the IP infrastructure to become IP application-aware by measuring both end-to-end SLAs and at the IP layer.
- The Control Plane Policing feature allows you to configure a QoS filter that manages the traffic flow of control plane packets to protect Cisco IOS Software routers and switches against reconnaissance and denial-of-service (DoS) attacks. By turning on this feature, you can maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.
- NetFlow is embedded within Cisco IOS Software to characterize network operation. This creates an environment where administrators have the tools to understand who, what, when, where, and how network traffic is flowing. When network behavior is understood, processes will improve, and an audit trail of how the network is utilized is available. This increased awareness reduces risk and vulnerability in the network.
- Cisco's Network-Based Application Recognition (NBAR) is a powerful classification engine that recognizes and classifies a wide variety of applications. NBAR works with QoS features to help ensure network bandwidth is best used to fulfill agency objectives. Utilize NBAR to guarantee bandwidth for critical applications, limit bandwidth to other applications, drop selective packets to avoid congestion, and mark packets appropriately to provide end-to-end QoS. NBAR ensures performance of mission-critical applications. When NBAR is turned on, an attack is mitigated because critical applications have priority over the traffic generated by the attack. Critical applications continue to send traffic, while NBAR drops selective packets to avoid congestion. This limits the amount of traffic your network will allow for the attacker's request for data. By setting up NBAR, you further mitigate the ability of a DoS/distributed DoS (DDoS) attack to be successful on day 0.

The Cisco IOS Software Cybersecurity Assessment and Enablement Service allows you to deploy a more secure network. When these features are turned on, they make your network more robust and provide better cybersecurity. They provide insight into how traffic flows on your network and how an attack can occur. Organizations are increasingly looking for ways to reduce their security risks, stay informed about security incidents, and maintain visibility into situations, while reducing costs and protecting their critical mission systems and data necessary to fulfill business objectives. Through consolidation of older environments, virtualization, expanding endpoint presences, and addressing wireless needs and multivendor technology sprawl, a larger awareness of risks and gaps may be identified and addressed across the enterprise. The use of cybersecurity technology, processes, and best practices can enhance the security, resilience, and manageability of the data and its infrastructure.

The Cisco IOS Software Cybersecurity Assessment and Enablement Service assesses security impact and necessary steps to enable the additional Cisco IOS Software features that reduce security risk and enable more visibility into your networks. Whether you are experiencing cyberattacks and data loss, identity and access problems, or are trying to understand where the go-forward security gaps will be, the Cisco Cybersecurity IOS Assessment and Enablement Service can provide risk reduction steps that help protect your network against changing threats.

To reduce risk and provide clarity to your existing network, Cisco will assess and recommend features to be enabled based on:

- Existing architectural design
- Environments and topologies
- Operations and procedures
- Interoperability
- Compliance

Cisco and Partner Expertise

Cisco will provide a Cisco IOS Software routing and switching expert with cybersecurity knowledge to conduct the assessment, helping to reduce your security risk.

Our Cisco IOS Software and cybersecurity experts apply Cisco's deep expertise in routing and switching, security planning, design, and implementation as well as in operating and optimizing for risk reduction and adherence to compliance requirements. Cisco's expertise and knowledge with cybersecurity enables us to provide you with the best solution to meet your needs. Cisco expertise is continually enhanced by hands-on experience with real life security networks and broad exposure to the latest security technology and implementations.

Follow-On Services

Cisco has several in-depth follow-on assessment, enablement, and operational services that address security architecture, risk, and compliance. Whether you are planning future programs, consolidating or modifying existing systems, or simply need to reduce security exposure, Cisco can help guide you through the security complexities.

Why Cisco Cybersecurity Services?

In today's complex and ever-changing threat landscape, gaps in a security solution can place data integrity, information confidentiality, business-critical applications, and mission objectives at risk. You need visibility into those risks with actionable steps to remediate. Your infrastructure needs integrated security controls that provide protection in a dynamic threat and vulnerability environment, while at the same time remaining aligned with security policy and compliance requirements as your organization evolves. Cisco and our industry-leading partners deliver intelligent, personalized services that identify, address, and help to mitigate security gaps.

Cisco takes an enterprisewide approach to help you reduce the risk and costs associated with achieving your mission objectives by helping you plan, build, run, and measure the effectiveness of your security solutions.

Availability

The Cisco IOS Software Cybersecurity Assessment and Enablement Service is widely available. Contact your local Cisco account manager about availability in your area.

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.**