Cisco Security Services for Connected Health

Protecting Healthcare Infrastructure
To provide a secure healthcare environment, it is critical to have a well-designed security architecture that contains controls and protects the infrastructure against ever-changing threats and vulnerabilities. The architecture must also support alignment with evolving healthcare security policies and compliance requirements. Building a comprehensive security system for a healthcare network begins with a clear understanding of the current security state of the organization's network architecture.

Cisco® healthcare security experts help to prioritize limited security resources, improve the security posture, simplify management, improve compliance, and optimize security investments. Cisco provides expertise on healthcare frameworks and standards, such as HIPAA, ISO 27001, FISMA, PCI, and ISO 80001, to address compliance needs so that healthcare organizations get the most value out of their security investments.

Assessing the Effectiveness of Security Controls
Cisco Security Services for Connected Health is provided by Cisco security consultants who draw on their extensive experience in the healthcare industry and related agencies. This expertise is supported by a combination of advanced tools, methodologies, and access to Cisco product development engineers.

Cisco security experts begin by conducting a detailed review of the security goals, identifying critical assets, and gathering business and technical requirements. Based on this information, they complete an in-depth analysis of your security infrastructure, including the network topology, network devices, and security devices, and the processes related to them.

Cisco Security Design Assessment for Connected Health
This service provides a comprehensive vendor-independent assessment of the healthcare network infrastructure, based on healthcare industry best practices and the Cisco Security Control Framework (SCF). The framework is consistent with international standards for healthcare security, including the ISO 27000 series (27799), NIST 800-66, and ISO 800001. This assessment evaluates the capabilities of the network infrastructure to protect an identified business-critical asset and provides a set of recommendations to remediate the risk to the identified asset. The recommendation includes improvements to topology, protocols, device configurations, and security controls.

The Cisco Security Design Assessment for Connected Health addresses the compliance requirements of healthcare customers by incorporating the relevant compliance requirements into the Cisco security control framework.

Cisco Security Posture Assessment for Connected Health
Security posture assessment is a requirement under many healthcare and government regulations to maintain the current state of the organization’s vulnerabilities, allowing it to prioritize remediation activities based on available resources and risks to healthcare infrastructure.

The Cisco Security Posture Assessment Service for Connected Health provides a point-in-time validation of how effectively the organization’s security controls have been implemented and are being operated. By emulating typical malicious activities using nondestructive means, Cisco identifies the presence of vulnerabilities in the healthcare IT network, wireless, and physical infrastructure.

Cisco will assess, prioritize, and make recommendations regarding the identified vulnerabilities and the risks they present to the healthcare infrastructure and business. A final report documenting the assessment results will be delivered.

Cisco security experts begin by conducting a detailed review of the security goals and requirements. Based on this information, Cisco probes the IT infrastructure from the interior and perimeter, surveys and maps the wireless network, and attempts to engineer its way into the facility. This analysis is done in a safe and controlled manner simulating activities typical of malicious attackers.

Cisco Network Device Security Assessment for Connected Health
Cisco Network Device Security Assessment Service for Connected Health helps implement and maintain a hardened network device environment by identifying gaps in your Cisco network device security. The rules-based assessment includes device configurations and access policies. These are compared with the leading security practices and the organization is provided with prioritized and actionable recommendations to mitigate the identified gaps in device configurations and policies.

Cisco Compliance Support Service for Connected Health
The Cisco Compliance Support Service for Connected Health provides analysis and evaluation of the organization’s readiness to meet healthcare industry and regulatory compliance requirements. Cisco will identify gaps that must be addressed and make recommendations for fixing problems and building the controls and documentation necessary for the auditors.

Cisco also supports ongoing help to maintain compliance after the completion of the audit.
Service Benefits and Value Proposition

- Create a comprehensive and scalable security architecture using a business-focused, risk-averse approach
- More effectively protect the infrastructure by identifying architectural, network device, and system vulnerabilities, and deviations from security best practices
- Safeguard employee productivity, healthcare data, and sensitive patient data by mitigating security risks
- Strengthen the staff’s ability to prevent, detect, and respond to future threats
- Protect the network investment by extending the security capabilities of the existing infrastructure
- Reduce the risk of intentional or accidental access to IT assets and information
- Test current infrastructure security safeguards to help ensure that malicious activity does not successfully penetrate or disrupt service
- Correlate vulnerability data with network topology information and identify risks posed to critical healthcare networks and assets
- Improve the overall security state of healthcare network infrastructure by following recommended actions to mitigate identified vulnerabilities
- Achieve improved compliance with regulations and industry mandates that require security assessments by identifying improved internal controls needed to better protect sensitive healthcare data

How to Order

To order the Cisco Security Services for Connected Health, please contact your Client Service Executive.

Additional Resources

For more information on Cisco in healthcare, visit http://www.cisco.com/web/strategy/healthcare/index.html.

For information about Cisco Medical Grade Network, a set of Cisco recommended guidelines for building an optimal in-hospital network, visit http://www.cisco.com/web/strategy/healthcare/cisco_medical-grade_network.html.

Portfolio for Cisco Services for Connected Health

Figure 1 shows the Cisco Services for Connected Health.