Cisco Security Advisory Services

Network Architecture Assessment

Today's dynamic threat landscape

Organizations are under attack everywhere. The global average cost of a data breach is $3.62 million, according to a 2017 report by Ponemon Institute.[1] Gartner predicts that by 2021, more than 1M IoT devices will come online every hour of every day. As a result, attack surfaces will increase, giving attackers more space to operate. The use of collaboration and rich media applications along with the transition to cloud services also introduces new points of network vulnerability. Meanwhile the global cybersecurity workforce will have more than 1.8 million unfilled positions by 2022 according to 2017 report from Frost & Sullivan.[2]

This talent shortage, along with the increasingly complex threat landscape, has led to a weaker security posture amongst most organizations. In such a dynamic threat environment, you need dependable security you can trust. Cisco recognizes these challenges and helps you identify security weaknesses within your system, and provides you with an actionable roadmap, using which you can significantly improve your security posture.

Benefits

- **Identify architectural and systemic weaknesses** within your networks
- **Measure** effectiveness of network segmentation
- **Gauge maturity** of technical and operational security controls
- **Measure security** coverage within the network across key security domains
- **Reduce risk** by following expert remediation roadmap to better utilize security technologies and improve security operations

1 https://www.ibm.com/security/infographics/data-breach/
2 https://iamcybersafe.org/wp-content/uploads/2017/07/N-America-GISWS-Report.pdf

Case Study

Global Enterprise Customer

Challenges

- Extremely complex networking environment
- Global requirements across a diverse landscape
- Lack of confidence in the coverage provided by current configuration of defense
- Unsure how to best spend the security budget to optimally protect the network
- Difficulty identifying business justification for security purchases

Solution

- Cisco worked with customer teams to discover gaps in the existing security architecture
- Cisco provided an actionable remediation roadmap to achieve an optimal level of security

Outcome

- Avoided high costs of purchasing new security products by updating existing product configurations
- Replaced ineffective security defenses with more effective, modern security technologies
- Reduced risk associated with many assets by implementing strategically placed defenses

A Roadmap for a more secure network

Managing risk requires wise investments in modern security technologies. The decision to implement a new security control must respect existing security capabilities and their configuration. The decision must also respect time of purchase. Early adoption risks being a poor investment if the decision lacks expert guidance. Late adoption yields sub-standard security defenses.

A network architecture assessment provides an evaluation that concentrates on the security of your network from both an operational and architectural perspective. We consider your existing network technical requirements including technical specifications, high-level design documents, and technologies in use, as well as your network business requirements to identify the business drivers, service capabilities, and specific areas of security-related concern.

In addition, we review your existing architecture to gain an understanding of systems, controls, and requirements. Based on the findings, we assess the security measures currently in place compared with industry good practice, including analysis of security issues identified, estimated business impact, if possible, and a prioritized list of recommendations to eliminate security weaknesses in your network's design.

Next Steps

Visit www.cisco.com/go/securityservices to connect with our advisors and protect your business today.

OCTOBER 2018