# Cisco Security Assessment

## Address critical security challenges with clarity and confidence

### Business challenge

Many organisations struggle with limited visibility into the security gaps that exist across their network environments—whether on campus, in data centres, in the cloud, or within IoT ecosystems. This lack of insight can result in unidentified vulnerabilities that leave the organisation exposed to cyber threats, ineffective or outdated security controls that fall short of compliance and operational standards, and missed opportunities to modernise and consolidate their security architecture.

### How we help

Insight's Cisco Security Assessment delivers a comprehensive evaluation tailored to your organisation's unique environment, covering critical areas such as campus networks, data centres, cloud infrastructure, and IoT ecosystems.

The assessment provides a clear view of your current security posture, identifies vulnerabilities, and evaluates the effectiveness of existing controls. Whether it's uncovering risks in virtualised environments, assessing cloud configurations, or securing connected devices, the deliverables are designed to help you understand where improvements are needed and how to address them with confidence. Key deliverables include:

- **Risk Discovery:** The assessment uncovers hidden vulnerabilities and evaluates the effectiveness of current security measures.
- **Tailored Recommendations:** It provides a roadmap for improvement, aligned with Cisco's security solutions.
- **Strategic Planning:** The output includes a project plan and readout that helps customers visualise their ideal security state and next steps.
- **Specialised Focus Areas:** Assessments are tailored to specific domains—Campus & Edge, Data Centre & Virtual Infrastructure, Cloud, and IoT—making them relevant to a wide range of customer environments.

**Duration:**

2-4 Weeks
(based on size and complexity of your network environment)

**Benefits:**

- Strengthen security posture by identifying and addressing vulnerabilities
- Receive tailored recommendations for improvement
- Financial incentives for partners
- Strategic planning and visualisation of ideal security state