Cisco Cloud Security Assessment Service

Benefits

- **Increase** awareness of your security posture
- **Develop** a repeatable process for evaluating new cloud service providers
- **Address** risk management, audit, and compliance issues
- **Enhance** governance and control for multicloud deployments
- **Define** robust identity and access management
Cloud strategy in a multicloud world

All companies want to reduce costs and focus their internal resources on core business functions. Many also want to build on-demand IT services. If you are among them, cloud service providers can help you gain a competitive edge with an array of services and capabilities. But these come with new, unique risks and exposures. You need to understand these security risks to manage those services effectively.

With the Cisco® Cloud Security Assessment Service, you can develop a holistic security strategy. We’ll help you improve network visibility, identify risks, and speed cloud adoption while improving security. We focus on long-term success with following components:

- **Cloud data protection assessment:** Understand the security posture of the data or activity taking place in your public cloud deployments.
- **User entity behavior assessment:** Detect potential anomalies in user behavior that suggest malicious behavior in a Software-as-a-Service (SaaS) application.
- **Cloud security strategy workshop:** Develop a cloud security strategy and roadmap aligned to your business priorities.
- **Cloud security architecture assessment:** Identify strengths and areas for improvement in your current security architecture as you onboard your multicloud environments.

Securing data to, from, and within the cloud

Many organizations lack the expertise they need to develop a security strategy and roadmap for their multicloud landscape. Cisco Services help organizations like yours navigate their multicloud security challenges. Our Cloud Security Assessment Service helps your organization deliver and consume cloud services with a high degree of security. We assess your data protection policies, user behaviors, and architecture. We can tailor a strategy that considers privacy, security, compliance, and business requirements.

**Cloud data protection assessment**

We help you prevent the unauthorized disclosure of sensitive data and maintain regulatory compliance. Together, we will:

- Review how a SaaS deployment is configured
- Examine where financial, Personally Identifiable Information (PII), or other sensitive information is stored and whether adequate access controls are in place
- Develop guidance on how users can properly share data within your organization, with another organization, or with the general public

**User entity behavior assessment**

We help you make sure that you have robust identity and access management in place. In this assessment we will:

- Create a baseline that shows you how users are behaving in a SaaS or Infrastructure-as-a-Service (IaaS) deployment
- Identify potentially malicious behavior
- Report anomalies along with recommendations for remediation

**Cloud security strategy workshop**

We help you understand your current security posture and collaboratively develop a desired future state. In this multiday workshop, we will:

- Analyze your security posture by looking at your security framework components in the context of the current environment (see Figure 1)
- Help you develop a cloud strategy and roadmap to reach your desired level of cloud security maturity within the next 1 to 3 years
- Consider staffing levels and business and technology strategies
- Recommend ways to improve IT governance in your multicloud environment
- Define a process for evaluating cloud service providers to help ensure they meet your business priorities, risk profile, and compliance requirements

**Cloud security architecture assessment**

We help you see how well prepared your organization is to absorb new cloud services. To strengthen your organization’s cloud security architecture, we will:

- Take a deeper look into your security tools, processes, and people and make recommendations for improvement
- Examine how new services can affect visibility and control and make sure that you have the right telemetry in place
- Identify the risks of introducing new cloud services into your multicloud environment
Develop a strategy to manage risk in your multicloud environment.

Do you:

• Feel confident that your organization is meeting its data protection and privacy compliance requirements?
• Know what cloud services are being used across your organization and how they are being used?
• Have a defined process for evaluating Cloud Services Providers (CSPs)?
• Know how public cloud services impact your organization’s efficiency and costs?
• Have a defined process to manage the SaaS applications, virtual machines and containers your organization is using today?
• Have trained personnel in place to define and implement your cloud security strategy?

The Cisco Cloud Security Assessment Service can help meet your privacy, security, compliance, and business requirements in your multicloud environment. Visit our Security Services page to connect with our advisors and protect your business today.

Use Case: Oil industry

Challenge

• The company’s leaders wanted to continue moving to the cloud, but there was a gap in their cloud strategy
• Lacked visibility into the cloud services they were consuming and what they needed in the future
• Needed to ensure that their data compliance requirements (PCI, PII) were met

Solution

• Cisco conducted a workshop to understand current information security strategies and processes

• Used the Cisco Cloud Security Framework to identify potential gaps in processes and controls for cloud security

Outcome

• Cisco delivered a SaaS cloud strategy for the customer to implement
• Identified gaps in existing tools and processes based on the recommended security controls
• Created a catalog with the current acceptable cloud applications, and the features that future ones must include