ATLASSIAN

Understanding shared responsibility in the cloud

As many organizations are prioritizing cloud transformation or embarking on a Cloud-first journey, there can be lingering questions and doubts. Cloud offers increased flexibility, scalability, and performance. However, moving away from a traditional on-premises environment can cause uncertainty about the perceived loss of control. One of the most common concerns is data protection and security.

While data protection is a top priority, the majority of organizations feel understaffed when it comes to security. Teams that fail to execute on an effective security and compliance strategy run the risk of compromised data, damaged customer reputation, and hefty fines. The good news is that moving to the cloud introduces a shared responsibility model, which means cloud vendors can help shoulder the load. This resource will help you understand how to implement successful joint strategies to make your migration to the cloud secure.

Common challenges organizations are facing:

94%

of organizations surveyed in the US are using **at least one type of cloud deployment.**

80%

of organizations reported they **lack a dedicated cloud security** team responsible for protecting cloud resources from threats.

62%

of organizations feel they are **understaffed** in terms of cybersecurity professionals.

Understanding the Shared Responsibility Model

Moving to the cloud can offer increased control and visibility to help meet stringent security and compliance requirements. On-premises, implementing new security tools can be time-consuming and complex. With cloud provisioning, a wide array of resources and tools are instantly available to constrained teams, empowering them to take action.

Additionally, in traditional on-premises environments small internal teams of IT professionals must secure every aspect of the company's infrastructure, data, and users. In the cloud, internal teams can collaborate with the vendor's security experts, who specialize in securing cloud environments, making the vendor's security team an extension of their own.

In a successful shared responsibility model, some aspects of security and data protection can be offloaded to the cloud vendor entirely, others can be managed collaboratively, and some remain the full responsibility of the organization.

Shared Responsibility in Atlassian Cloud

Let's break down which aspects of security are owned by Atlassian and which are owned by our customers. We can think of shared responsibility as a layered approach across three main categories - infrastructure, data, and administration.

As a cloud provider, Atlassian takes full responsibility for the system and underlying infrastructure. Protecting data requires a collaborative approach, while administering products is the customer's responsibility. It's important to remember that although your organization shares in this responsibility, Atlassian provides tools, controls, and best practice guidelines to help your organization defend against threats and malicious activity.

RESILIENCE AT SCALE

In the Atlassian Cloud organizations can remove the operational burden of managing infrastructure, including maintaining physical data center locations and hardware, configuration monitoring, penetration testing, and more.

You benefit from a cloud platform designed to deliver scalability, performance, and reliability. The **infrastructure layer is the sole responsibility of Atlassian** as your cloud service provider.

COMPREHENSIVE DATA PROTECTION

In today's digital world, data is your most valuable asset and a **shared layer of responsibility in the cloud.**

To meet our portion of the shared responsibility, we undergo rigorous audits to ensure we handle data securely and continually expand the list of geographic and industry compliance regulations we've attained.

To support your portion of the shared responsibility, we offer robust controls for data protection, identity and access management, and data privacy.

CENTRALIZED VISIBILITY AND CONTROL

Another critical aspect of data protection is the ability to effectively administer products while maintaining visibility and control. **This layer of shared responsibility is owned by you as the customer, but that doesn't mean Atlassian isn't here to help.**

Our team is focused on creating solutions that make it easier for your organization to gain centralized visibility across all your Atlassian environments, as well as successfully manage any size and number of teams.

Partner with Atlassian in the cloud

As your organization may be moving to the cloud with a variety of cloud service providers, understanding the core principles of the shared responsibility model is key. Apart from increased scalability, resilience, and performance; enhanced security and compliance can be substantial benefits of cloud transformation. Atlassian wants to partner with you to help empower your organization to unlock the potential of every team.

Learn more about **Atlassian's approach to security and data protection in the Cloud**

ATLASSIAN