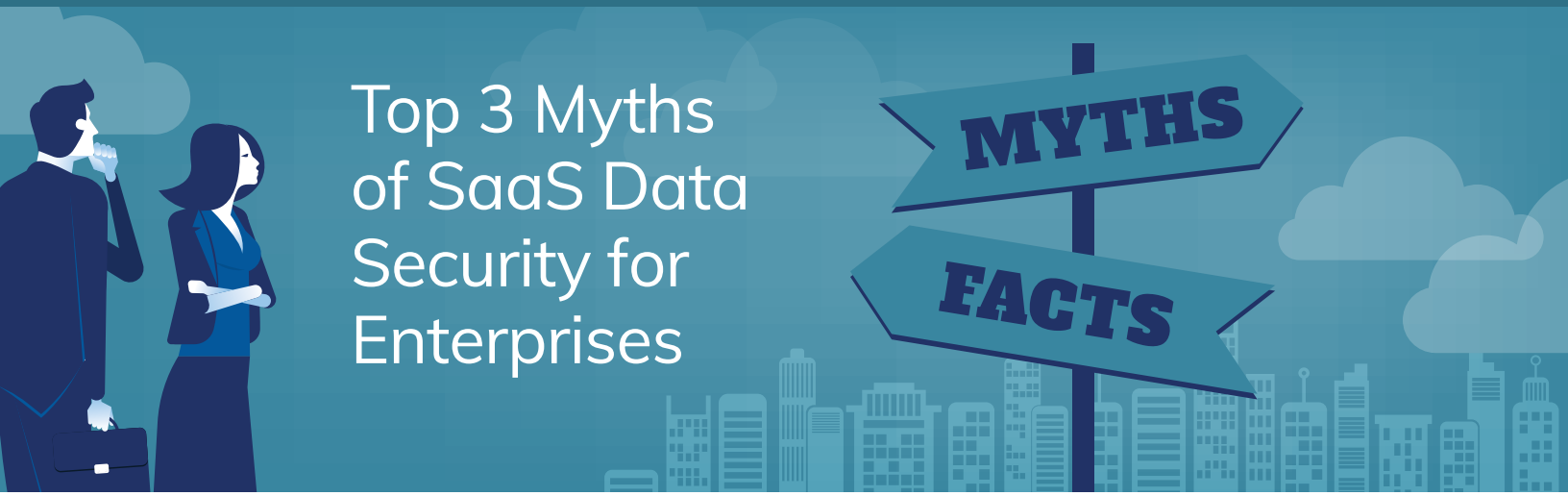
AppOmni



Top 3 Myths of SaaS Data Security for Enterprises

Recent news of data privacy violations, data exposures, and preconceived notions of cloud security have all contributed to incorrect and often confusing assumptions regarding SaaS data security. Here are the top 3 most common myths regarding SaaS data security and what you should be focusing on instead.

MYTH #1 Application vulnerabilities are the top cause of SaaS data loss/theft.

Application and system vulnerabilities consistently rank as one of the top reasons for cloud data breaches by IT professionals. Recent high profile reports of vulnerabilities found in mobile consumer apps and the resulting data breaches have reinforced this perception. These apps are cloud-based, and the impacted number of users is often very significant. One such high profile cloud app is Facebook. During much of 2018 and 2019, Facebook was in the news for a wide range of data and privacy-related issues. The vulnerabilities identified include, among others, exposure of user data and account takeover. The number of impacted users from these incidents range from hundreds of thoughts to tens of millions.

Despite the high profile incidents, Facebook is not an accurate representation of the state of security in SaaS applications used by enterprises. SaaS applications many enterprises rely on today for their day-to-day operations are designed and maintained with a very different rigor in comparison to social media consumer applications. These cloud apps are regularly updated with the latest security capabilities as well as supported by rapid response to any vulnerabilities.

An example of SaaS relied on by many enterprises is Salesforce. As the leading CRM solution, Salesforce has more than 150,000 enterprise customers with revenue over $13 billion. The security measure taken by Salesforce includes stateful inspection firewalls, bastion hosts between the perimeter and core firewalls, and data encryption. Salesforce also employs in-house penetration testing teams who continuously simulate and defend against attacks. There have been no recorded breaches of Salesforce in the past decade.

If application vulnerabilities are not the leading cause of SaaS data loss or theft for enterprises, then what is? It is, in fact, the enterprise. More specifically, it's the enterprise's misconfiguration of SaaS that leads to many data exposures. With the increasing sophistication of features as well as security capabilities, many organizations lack the manual resources and expertise to configure security features and monitor for deviation accurately. As an example, Salesforce issues new security guides approximately 3 times a year. To be fully versed in all the new capabilities, administrators must read the entire guide spanning more than 300 pages.

MYTH #2 Shared Responsibility model does not apply to SaaS data security.

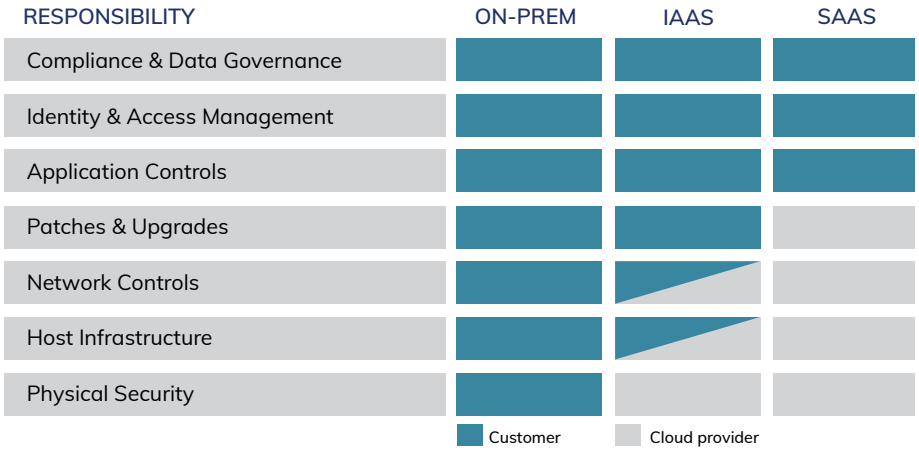
Many recognize the shared responsibility model by its use in Infrastructure-as-a-Service (IaaS), such as Amazon Web Services. In this model, the cloud service provider is responsible for the security OF the cloud, including the underlying hardware, global infrastructure, and software. Customers, in turn, are responsible for security IN the cloud, such as the encryption and data integrity, Operating System (OS), firewall configuration, applications, and customer data. It's a simple concept that delineates responsibilities to ensure the safe and secure use of cloud services. It also clarifies liabilities in case of service disruption due to a wide range of issues, including cyberattacks.

With SaaS, cloud service providers assume an increasing portion of the shared responsibility model. In addition to the underlying hardware and infrastructure, cloud service providers manage the network, OS, and the application. In comparison to IaaS, this level of coverage seems rather comprehensive, leading to the perception that the shared responsibility model does not apply to SaaS. If this were indeed accurate, the cloud service providers would assume practically all responsibilities and liabilities, leaving very little to the customer.

Despite the cloud service provider's increased responsibilities, the customer is responsible for the security of data housed in SaaS as well as access to the SaaS applications. Security of the data, including the use of encryption as well as managing the level of user access to match the appropriate types of data all, fall squarely on the enterprises' shoulders.

Data exposure related to the city of Denver 311 non-emergency system is an example of a failure in the organization's part of the shared responsibility model. An auditor found personal information of city employees and their dependents were accessible by over 10,000 people. The data exposure was due to incorrect Salesforce configuration put in place to increase efficiency. The administrator did not account for the exposure of sensitive data due to the configuration change. Incidents such as this have prompted many enterprises to deploy solutions to manage their SaaS instances better.

> *"Through 2025, 99% of all cloud security failures will be the customer's fault."*
> – Gartner



Shared Responsibility Model

MYTH #3 CASB is the ideal solution to secure SaaS data

As more and more enterprises adopt cloud services, they wanted to recreate the familiar security perimeter model of on-premise deployments in the cloud. Cloud Access Security Broker (CASB) promised to fill that role by acting as an in-line access broker overseeing user access to particular cloud services. Different CASB solutions focused on different features, including detection of shadow IT, securing sanctioned apps, encryption of cloud data, and cloud-based Data Loss Prevention (DLP). Similar to how firewalls are considered a must-have for traditional networks, CASB vendors were positioning the solution as standard security for cloud services.

In practice, however, enterprises quickly realized that CASB solutions did not address all of their needs. These solutions traded off granular insight and controls over SaaS solutions to support an increasing number of SaaS applications. By design, policies had to be high level and general to support different SaaS solutions ranging from CRMs and storage to collaboration tools. One particular deficiency of CASB solutions stem from the reactive nature of the solution. Similar to other perimeter security architecture, enterprises are only alerted when incidents occur at the perimeter, such as an attempt to download sensitive data. Unfortunately, such incidents are the only gauge of the enterprise's security posture or the state of their data exposure when using CASB solutions.

Many enterprises are now turning to SaaS monitoring solutions such as Cloud Security Posture Management (CSPM). These solutions address vital capabilities not found in CASB solutions. They provide deep integration with SaaS solutions allowing them to analyze specific settings and configurations that are relevant to the SaaS in question. The level of policy granularity surpasses the CASB's one-size-fits-all policy approach. Granular policies ensure that the configurations accurately represent the business intent. Continuous monitoring ensures the SaaS configurations always remain accurate, alerting on deviations, and in some cases, reverting changes to approved settings.

Some CSPM solutions for SaaS are also proactive solutions providing enterprises real-time security posture. Enterprises can identify the SaaS data exposure in real-time, enabling them to take necessary measures before an incident can occur. Many enterprises that use sandbox environments to verify new rollouts of SaaS updates also leverage CSPM solutions to verify data security before going live in the production environment.

> *"Through 2024, implementing CSPM offering...will reduce cloud-related incidents due to misconfiguration by 80%"* – Gartner

Debunking the Myths

What do all these myths have in common? They are all based on outdated information. Despite the flurry of news regarding vulnerabilities of mobile consumer apps, SaaS solutions designed for the enterprise are very secure. But, it is the responsibility of the enterprise to ensure the services are configured correctly and continue to be maintained.

Enterprise cannot address and manage these responsibilities without the right tools in place. While traditional cloud security solutions offer some benefit, enterprises must employ a proactive solution. One that continuously monitors the SaaS environment and can take necessary actions without requiring significant in-house resources or SaaS/Cybersecurity expertise.

ABOUT APPOMNI AppOmni is the leading software as a service (SaaS) data security and management platform for the enterprise. AppOmni provides unprecedented data access visibility, management, and security of SaaS solutions, enabling organizations to secure mission-critical and sensitive data. AppOmni's patent-pending technology comprehensively scans APIs, security controls, and configuration settings to evaluate the current state of SaaS deployments and compare against best practices and business intent. With AppOmni, organizations can establish rules for data access, data sharing, and third party applications that will be continuously and automatically validated. The company's leadership team brings expertise and innovation from leading SaaS providers, high tech companies, and cybersecurity vendors.