SaaSAssure℠

TECHNICAL BRIEF

Top 12 SaaS Security Best Practices to Implement Now

Index

Top 12 SaaS Security Best Practices to Implement Now

With data breaches and ransomware at an all-time high, security professionals are working diligently to lock down their infrastructure to stop attackers. Naturally, attackers are shifting their attention toward data where the organization's security posture is less robust — their Software-as-a-Service (SaaS) environments.

Businesses are storing more business-critical and sensitive customer data in more SaaS services, often under the assumption that their SaaS provider fully safeguards this data. However, given the nature of the shared responsibility model, IT leaders must play a crucial role in ensuring SaaS data is secure.

SaaSAssure℠

Understanding Security Risks in the SaaS Environment

Like any IT architecture, SaaS applications have a number of risks security professionals must be vigilant about. Key among these risks include:

- **Data breaches:** SaaS providers are at risk of large-scale attacks that can compromise user data.
- **Account hijacking:** Phishing attacks, social engineering, credential breaches and other common attacks can open up user accounts for take over.
- **Weak authentication:** Default settings on many SaaS services may not include any form of multifactor authentication or additional access controls.
- **Fragmented platforms:** The average number of SaaS services used by a mid-market organization is 100+, leading to overly fragmented data structures and workflows.
- **Custom configurations and misconfigurations:** SaaS services can offer configurations to users that can inadvertently expose data. Misconfigured API connections can also introduce security vulnerabilities.
- **Evolving environments:** SaaS services are under constant development with new features and code rolled out that can easily introduce new security bugs.
- **Shadow IT and personal devices:** Users are notorious for accessing unauthorized services to perform their jobs, putting company data at risk.

Impact of SaaS Security Breaches on Organizations

Several high-priority security breaches at SaaS companies have had huge impacts for customers, and by extension their users' customers. Big names like Slack, GitHub, Salesforce, Jira, Box, Dropbox and Zoom have all been victim to attacks or misconfigurations leading to the exposure of sensitive data.

One of the most critical incidents involved LastPass, which posed a significant threat due to storing credentials for various other SaaS services and applications. Attackers managed to breach systems containing vault data as well as source code. Although vault data is encrypted, access to the data is possible if an individual user's master password is compromised, a risk heightened by the common practice of re-using passwords.

The gravity of security vulnerabilities involving SaaS data cannot be overstated. These threats can lead to data breaches, incurring substantial fines and penalties, legal repercussions, and damaged brand reputation. Security breaches can also lead to data loss, which can disrupt business operations and lead to downtime that can cost the average large enterprise $9000 per minute.

Obviously, some SaaS services are more critical than others when it comes to business continuity, but these services are often overlooked in business continuity planning. It's critical that organizations develop a strong SaaS security posture to reduce the potential for incidents and minimize their impact.

Developing a Comprehensive Security Strategy for SaaS Applications

Security professionals looking to improve their overall SaaS security posture need to develop a strategy and include both an overarching approach to SaaS in general and best practices for managing each supplier that they use.

General SaaS Security Best Practices

1 Adopt a security-first mindset

A good approach to SaaS security is to assume that attacks are going to happen and all measures to ensure security should be implemented, including awareness by all users about why they need to comply with security measures.

2 Provide ongoing training

Training should be provided so that users are hyper-aware of the most frequent attacks, like phishing attempts, to new approaches that use generative AI to fool them.

3 Document SaaS footprint

IT leaders should maintain an up-to-date inventory of their organization's entire SaaS footprint and enforce policies requiring employees and contractors to use only approved applications.

4 Maintain visibility

Technology leaders should also maintain awareness of news regarding updated security features, recent attacks, vendor breaches and new security vulnerabilities that could impact their security posture.

5 Use a Cloud Access Security Broker (CASB)

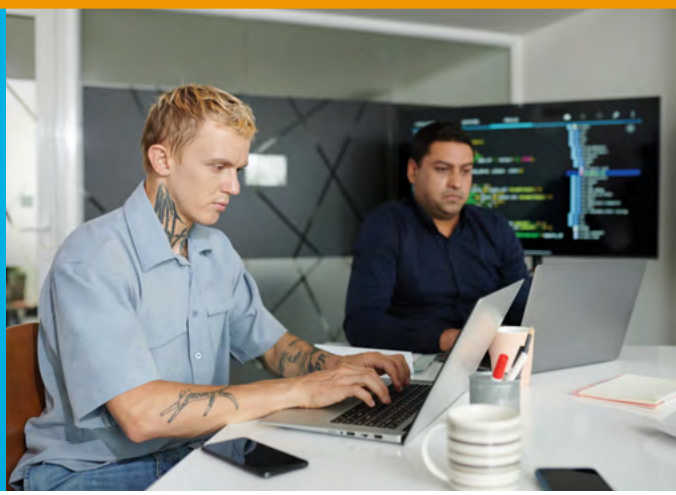
A cloud access security broker is a third-party service provider capable of managing the bulk of the work in enforcing security policies across a broad range of cloud services. For larger enterprises with hundreds of apps and thousands of users, a CASB can simplify the effort required to ensure compliance.

6 Prevent shadow IT with centralized procurement

All employees and contractors must understand that SaaS service charges will only be paid or approved if managed through a centralized procurement process

SaaSAssure℠

Vendor-Specific SaaS Security Best Practices



1 Implement strong access controls

Default login/password combinations should be accompanied by multi-factor authentication at a minimum, with single-sign-on being the preferred method. Biometric based access authenticators are also effective.

2 Use role-based access control

Ideally, SaaS applications should enable role-based access to restrict user privileges, cross-platform data access, and functionality like data deletion or third-party app integration, pending oversight and approval.

3 Ensure secure API connections

The default API connection most SaaS services offer are simple API keys, which are often tied to admin accounts and can open full administrative access to data. These should be used sparingly, and only for momentary connections. More secure Oath2 can limit the scope of access. Some applications have “enterprise” tiers that allow admins to make more specific API calls.

4 Make sure data is encrypted at-rest and in-transit

SaaS services often allow admins to export data. But this data is usually provided as unencrypted .csv files, which are not typically encrypted during download. Depending on the download target this can result in data left on a device without encryption. It’s safer to use a backup service that ensures data encryption both in-transit and at-rest.

5 Backup SaaS data

And on that note, administrators should have an automated backup service with strong security that provides coverage for the most business-critical SaaS services to ensure data is available in the event of accidental or malicious deletion.

6 Ensure vendors are compliant with security and privacy regulations

When evaluating and selecting SaaS vendors, IT leaders should mandate common security certifications like SOCII while also requiring vendors to support data privacy standards such as HIPAA and GDPR. (A guide to evaluating SaaS vendors' level of security and SaaS security checklists can be found here.)

Conclusion

With the increasing reliance on SaaS services, it's imperative for businesses to strengthen their SaaS security posture. These security practices include adopting a security-first mindset, providing ongoing training against sophisticated attacks, maintaining an inventory of all SaaS services, ensuring visibility and compliance, and using CASBs for managing cloud services. Additionally, strong access controls, role-based access, secure API connections, data encryption, regular backups, and vendor compliance with security and privacy regulations are essential practices. Implementing these best practices will significantly reduce security challenges and protect sensitive data, maintaining business continuity and safeguarding against potential financial and reputational damage.

About SaaSAssure

Total control over data, or data sovereignty, solves many problems. However, backing up the fast-growing mountain of data from SaaS apps is a daunting task. Partial solutions only paper over the need for future work. What's needed is a way to close data gaps, keep up with data growth, and even make comprehensive backups stable and secure not just now but in the future. SaaSAssure helps businesses of all sizes accomplish that.

Find out more about our secure SaaS backup platform, SaaSAssure.

Join the forefront of SaaS data protection with SaaSAssure.