How to Build your 2025 SaaS Security Strategy

Best Practices for CISOs

SaaS is reshaping how businesses operate, boosting agility, improving productivity, and cutting costs. And, it's reaching every corner of IT, from network infrastructure to the tools employees rely on daily. What sets this transformation apart from past changes is the fact that it's increasingly led by business units, not IT or security teams.

The SaaS shift mirrors the early days of the BYOD (bring your own device) movement, where IT/security initially resisted, but eventually adapted as new security solutions emerged. Today, employees expect the flexibility to use the devices and tools that suit them best—thanks in large part to SaaS. SaaS accelerates workflows and enhances job satisfaction.

As personal tech advanced to meet enterprise demands, so too has software.

The rise of bring your own application (BYOA) means employees can now choose and purchase apps without waiting for IT/security approval or following lengthy procurement processes.

While this freedom can supercharge productivity, it also introduces new risks. These risks, while different from traditional IT challenges, remain critical to address. Security must keep pace with business objectives, and SaaS security best practices help CISOs strike that balance, ensuring digital transformation efforts remain both agile and secure.

This SaaS security checklist is designed to help CISOs build a proactive SaaS security strategy and put the necessary controls in place to manage the growing risks from independent SaaS and AI adoption.

grip

SaaS Security Best Practices Checklist

Implement Proactive New SaaS Discovery

Because employees are acquiring SaaS apps independently, monitoring needs to cover every device they use, regardless of whether they're connected via VPN or ZTNA. Traditional security tools struggle with SaaS discovery because they rely on network traffic analysis or endpoint agents, which are limited by device or access type. Newer SaaS security platforms, however, offer continuous discovery, effectively tracking apps across all devices and networks without those restrictions.

Automate SaaS Business Justification

After discovering a SaaS app, assessing its risk is the next step. Users need to inform IT/security about the app's business purpose and the type of data it will handle. Automating this with a survey streamlines the process, especially given the sheer volume of SaaS apps in an organization. Without automation, managing this at scale would be impossible. Once the risk level is identified, IT/security can enforce the necessary policies. The success of this process hinges on thorough and continuous SaaS detection.

Enforce Identity and Access Management (IAM)

Most companies use an IdP or an SSO solution and have a policy that when a SaaS app supports one of those two, the employee should be using them to access the app. Using IdP to create accounts gives IT/security teams centralized visibility and control. However, many employees still resort to traditional logins and passwords despite the policy. Enforcing the proper IAM methods is important for centralizing SaaS risk management. Traditional SaaS security tools often fall short in tracking this, while modern platforms offer the necessary insights. Additionally, not all SaaS apps support IdP or SSO integration, making IAM enforcement challenging (if not impossible) with older security solutions.

Require Multi-Factor Authentication

Multi-factor authentication (MFA) strengthens SaaS security by requiring more than just a username and password for access. Since most SaaS apps offer at least two-factor authentication, it should be mandatory. The challenge for security teams is identifying apps that don't support MFA and then preventing their use. Modern SaaS security platforms can automate this process, flagging apps without MFA and reporting them efficiently.

Prioritize Single Sign-On Integration

Single Sign-On (SSO) boosts employee productivity by reducing the number of usernames and passwords that could be compromised, while also providing an audit trail for SaaS app access—essential for compliance and security certifications. However, adding apps to SSO isn't automatic and can be costly due to licensing fees. IT/security teams need insight into which SaaS apps are most widely used and pose the highest risk. Traditional SaaS security tools don't offer this level of visibility, but modern platforms do.

Monitor Sharing of Accounts

Sharing SaaS accounts among multiple users poses significant risks. When an employee leaves, the password should be changed, but this often gets overlooked due to the inconvenience. In some cases, account sharing may be necessary for business reasons, but a process must be in place to secure accounts when personnel changes occur. SaaS security platforms can monitor account sharing and even automate password resets for all users if needed.

Remove Dormant (Zombie) Accounts

The simplicity of creating SaaS accounts means employees often have more accounts than they realize. Many may have signed up for a free trial or abandoned an app after finding a better alternative. Each of these dormant accounts becomes a potential security risk, possibly storing sensitive company data. Modern SaaS security platforms can regularly discover and secure these unused accounts, reducing the chances of them becoming attack vectors.

Enforce Password Policies

When a SaaS app doesn't support a company's IdP or SSO, the only option is a username and password. The problem is that many employees reuse passwords across apps and rarely change them. While password managers are an option, employees often ignore password strength and update guidelines. A more effective solution is to eliminate the need for usernames and passwords altogether by using a SaaS security platform. This extends IdP or SSO policies to all SaaS apps, ensuring a consistent and secure risk management approach.

Remember, there are no silver bullets when it comes to SaaS security. While many of the steps are well known, the key lies in consistent execution. Detecting SaaS applications is the crucial first step, followed by automating processes to minimize human error. Modern SaaS security platforms, built specifically for the SaaS ecosystem, provide the tools needed to help organizations meet their security goals effectively. Grip is here to help; we encourage you to take advantage of our free SaaS identity risk assessment to understand the SaaS risks in your unique environment.

grip

Grip Security is a pioneer in SaaS identity risk management, providing innovative solutions to help enterprises address the security risks associated with widespread SaaS adoption.

Contact Us

info@grip.security

@GripSecurity

grip.security

SOC 2 Type II Certified

ISO 27001 Certified