Solution Brief

SaaS Security Checklist–Best Practices for CISOs

Implementing SaaS is a core component of digital transformation, the integration of digital technologies into how a company operates to help them become more agile, respond to the market faster, and reduce costs. The transformation touches nearly every aspect of IT, from the network infrastructure to the applications used by employees on a daily basis. One notable difference from technology transformations of the past is that much of the transformation is business-led and not dictated by IT or security teams.

Business-led IT has many similarities to the bring your own device (BYOD) movement, which was initially resisted by IT/security but eventually embraced as security tools and products came on the market to help solve the problem. Employees are now used to using the device of their choice to get their work done, largely enabled by SaaS. It helps them get their work done faster and increases job satisfaction.

BYOD became possible as consumer IT products became more powerful and able to support enterprise features. The same is happening in software, and the consumerization of SaaS is driving the growth of bring your own application (BYOA) in the enterprise. Employees are now able to purchase an app on their own without IT/security approval or going through the vendor procurement process.

Though this is great from a productivity perspective, it does not diminish the risks it presents to the business. The nature of the risks are different, which is why security is a significant focus of digital transformation initiatives. For SaaS in particular, there are a set of best practices CISOs can implement that can help companies embrace digital transformation and balance their risk management policies with the business objectives.

Implement Proactive New SaaS Discovery

Employees today want to use the best app to get their job done, and that means they will acquire SaaS apps on their own. The monitoring must occur across all of the devices employees use for their work regardless of whether they are using a VPN or ZTNA access method. Traditional security products fall short in SaaS discovery because they require network traffic analysis or endpoint agents. Newer SaaS security platforms do a far better job of constant discovery by using discovery methods that work no matter what device the employee is using or what access network they are connected to.

Automate SaaS Business Justification

Once SaaS is discovered, a process to evaluate the risk is needed. The first step in this process is for the user to inform IT/security of the business need for the SaaS app and the type of data that is going to be used in the app. This can be achieved through an automated survey that is sent out to the user. The sheer volume of SaaS usage in an enterprise makes this impossible without automation. Once the risk level is assessed, IT/security can then enforce the appropriate policies. The efficacy of this process depends on comprehensive detection.

Enforce Identity and Access Management (IAM)

Most companies use an IdP or an SSO solution and officially have a policy that when a SaaS app supports one of those two, the employee should be using them to access the app. Having employees use IdP to create accounts provide IT/security teams centralized visibility and access control. Despite the official policy, many employees use logins and passwords. Knowing and enforcing the IAM method is important because this allows IT/security teams to centralize SaaS risk control. Traditional SaaS security products are not able to provide this type of data, whereas newer SaaS security platforms are. Furthermore, not all SaaS apps support an IdP or SSO integration, so IAM enforcement using traditional SaaS security products is just not possible.

Require Multi-Factor Authentication

Multi-factor authentication (MFA) enhances SaaS security by requiring users to identify themselves with more than just a username and password. Most SaaS apps support at least two-factor authentication, and this should be a requirement. The challenge for security teams is to identify SaaS apps that do not support MFA and stop users from using them. SaaS security platforms are able to do this, and automate the reporting of this capability.

Prioritize Single Sign On Integration

Single Sign On (SSO) helps employees be more productive and reduces the number of usernames and passwords that could be compromised. It also provides an audit trail of SaaS app access, which is required for compliance and security certifications. Adding an app to SSO does not happen automatically and can be expensive due to SSO licensing costs. IT/security teams benefit greatly by knowing which SaaS apps are used by the most employees and have the greatest risk. This information cannot be obtained using traditional SaaS security products.

Monitor Sharing of Accounts

Sharing SaaS accounts among multiple users is one of the greatest risks. If one employee were to leave the company, the remaining employees would need to change the password, and this is an inconvenience, which means there is a good chance that this will not happen. Sometimes sharing does make business sense though, and a process is required to ensure that the account is secured with any changes in personnel. SaaS security platforms can monitor the sharing of accounts and even reset the passwords for everybody if needed.

Remove Dormant (Zombie) Accounts

The ease with which SaaS accounts can be created means that employees likely have more accounts than they are aware of. In many cases, they may be testing something out with a free trial or stopped using an app once they discovered a better one. Each of these dormant accounts is a potential attack vector or could store sensitive, confidential company information. Newer SaaS security platforms are designed to discover and secure dormant SaaS accounts, and this is something that should be done on a regular basis.

Enforce Password Policies

When a SaaS app does not support a company's IdP or SSO the only option is a username and password. The problem is that most users will reuse passwords across multiple apps, and they do not regularly change them. Using password managers is viewed as an option, but employees often do not follow the password strength and change guidelines. A better approach is to remove the need for usernames and passwords and handle them using a SaaS security platform. This helps extend IdP or SSO policies to all SaaS apps and implements a consistent risk management strategy.

There are no silver bullets when it comes to SaaS security. Many of these items are things that are commonly known. Detecting SaaS applications is the critical first step. After that the challenge is being consistent and implementing automation to reduce the chance of human error. Newer SaaS security products were designed specifically for the SaaS environment and can help companies achieve their SaaS security objectives.

SaaS Security Checklist With Grip

When going through a SaaS security checklist, it is vital to understand the security implications and possibilities. It's important to start with locating and securing shadow SaaS. Grip can help with our SaaS Security Control Plane (SSCP) solution. This modern approach enables your business to discover, prioritize, protect, and organize SaaS security for authorized and unauthorized applications and managed and unmanaged devices.

Grip's SSCP requires fewer personnel and resources than competitors and takes less time to install. Our innovation allows your business an immediate return on investment and save money on SSO. To learn more about SaaS security with Grip, download the datasheet today. Interested in a demo to see how an SSCP can help your SaaS security program? Learn more about SaaS Security or get a free SaaS security risk assessment from Grip today!