Solution Brief

5 SaaS Security Risks Every Company Needs to Address Immediately

More and more CIOs are beginning to embrace business-led IT, and this has serious implications for security. As SaaS democratizes the evaluation, deployment, and ownership of technology in companies, business leaders are taking on a do-it-yourself approach because it allows them to move more quickly and reduce project timelines. IT benefits because their project pipeline is reduced, and they can refocus their resources onto projects that only they can do. The move away from centralized technology acquisition breaks how companies, up to now, managed their security risks and compliance programs related to technology acquisition. Security teams do have products that help them discover and manage SaaS apps that are being used by their employees. However, the problem is that these products still rely on the outdated assumption that the company controls the endpoint, network access, or authentication method. Single-sign-on products(SSO) are a great example where the company controls the authentication method. But for many reasons SSO is insufficient for the hundreds of apps used by employees, many of which may only have a few users. Cloud access security broker products (CASBs) are also commonly used, but CASBs have critical limitations, and they are not designed to control SaaS sprawl.

What has become apparent is that the industry's approach to SaaS security needs to be redefined. To secure SaaS properly requires an architectural change, where there is a SaaS security control plane that discovers, prioritizes, secures, and orchestrates security. Implementing a strategy with this approach can help companies address the following five risks every company needs to address.

1. Authentication Using Local App Credentials

When users create accounts for SaaS apps, they sometimes have the choice to use and identity provider (IdP), such as Google or Microsoft AzureAD, or creating their own username and password. Many users choose to do the latter, which means only the employee can access the account. SSO and IdP products are unable to mitigate this risk because they are not being used. SSO requires integration with the SaaS application, and the IdP authentication method is voluntary. Though official company policy may require it, compliance is likely very low.

2. Zero Day SaaS Usage

By some estimates there are approximately 25,000 SaaS companies, and in 2021 there were 4,459 SaaS company deals with $94 billion in capital invested. This means that that there are thousands of new SaaS companies being created every year. Many SaaS security products rely on a SaaS catalog, which will be obviously behind when hundreds of new apps are being created every month.

3. SaaS Access from Unmanaged Devices

SaaS can be accessed from anywhere from any device, and that includes unmanaged or personal devices. Employees consider this an advantage, since they do not have always have their work laptop to do work, and they can do their work from anywhere. Security teams view this as a risk because company data accessed from an unmanaged endpoint could result in a breach if the endpoint has been compromised. Using SSO or an IdP does provide some visibility into the type of device and location. However, those products do not have the coverage needed to really solve the risk problem of business-led SaaS being used on unmanaged devices.

4. Add High Risk SaaS Apps to SSO

SSO can be an effective solution for core SaaS apps where access needs to be closely monitored and controlled. An average company with 1,000 employees uses more than 150 SaaS apps. Not every app needs to be in SSO, but the highest risk apps should be added and governed by an SSO product. Factors to consider when prioritizing whether SaaS apps for SSO include:

· Total number of employees using the app
· The growth in user adoption
· Number of departments using
· Authentication using local app credentials
· Type of data being used by the app

5. EmployeeAwareness of Security Policies

Most employees go through some sort of new hire onboarding, which may or may not include security policy training. Most company policies require employees to notify IT when they sign up for a new SaaS app and record vendor information. This almost never happens, because using new SaaS is just the way people work today. Ask any employee, including security professionals, if they can do their job using only apps that are officially sanctioned by the company, and the answered would almost certainly be “No.”

Why is Business-Led IT SaaS So Risky?

SaaS unknown to IT can be a huge risk, especially if company data is used in the app. By not monitoring or mitigating this risk, the company risks falling out of compliance with its own policies. Any of the scenarios below would violate most companies' policies.

· IT does not know that company data is being used in a SaaS app, whose provider may not comply with the company's security requirements

· If an employee were to leave, and they still have access to the SaaS app and any data that is stored or used by the app

· SaaS app credentials were stolen, and all users must reset their passwords, but the security team cannot identify all users of the app

Redefining SaaS Security

SaaS security is one of the most pressing challenges CISOs are facing today. Every day, employees are signing up for more SaaS, putting the company at greater risk. Unfortunately, this risk is largely invisible and growing unmitigated. The solution is not to lock down the environment but to support businesses with governance and guardrails. To do this requires that companies modernize their security architectures with a layer that addresses the unique challenges of SaaS security.

The Grip SaaS Security Control Plane does just that. It is a purpose-built solution that leverages existing infrastructure and is designed to simplify SaaS security operations with built-in, out-of-the-box automation that focuses on identity management that works on managed or unmanaged devices and all SaaS applications. With automation at its core, the SaaS security control plane coordinates and automates security processes and allows security teams to scale, reduce workload, and enforce risk management policies across disparate systems. Grip provides an end-to-end platform that identifies incidents, provides the remediation options, and automates the implementation—from alert to security outcome.

The Grip solution does not require an endpoint client or require proxy or CASB integration. Installation is simple and only takes ten minutes to complete. Schedule a free SaaS security assessment or you can learn more by reading our datasheet.