Case Study

Insurance Company Chose Grip to Protect the SaaS-Identity Risk Landscape

Insurance

Innovative insurance company that expands affordability and accessibility for renters, combining expert knowledge in finance, technology, and real estate

Industry: Fintech, Real Estate

Region: North America

Solution

Grip SaaS Security Control Plane

Challenge

- Incomplete picture of the SaaS-Identity risk landscape, allowing user choice but expanding the identity perimeter.
- Other solutions could not balance the need for business-led IT strategy and user choice with appropriate security and control.
- Without a continuous line-of-sight to SaaS usage and identity sprawl, the persistent control and compliance gap came to a breaking point.

Results

- Automated workflows for SaaS onboarding, user justification, and user offboarding reducing 80% of the team's workload
- Continuous discovery and visibility of new SaaS services and cloud accounts
- Reduced the time to authorize new SaaS usage from days to minutes
- Automatic identification of unused SaaS accounts for reclamation or revocation

> Only Grip could enable my team to secure more than we could touch – shielding identities from threats and maintaining compliance. Now, discovering and mitigating identity-SaaS risks gets done in one place and in minutes, not months.
>
> *VP Information Security*

The company, a well-known fintech and financial services organization, underwent a rapid transformation that posed significant security challenges in terms of accessing SaaS apps and services outside the direct control or oversight of the security team.

This presented a challenge, as the company faced the issue of users frequently changing roles, responsibilities, or departing the organization, while new employees and teams pushed the organization's identity attack surface to hundreds of SaaS services, most of which were unknown, unguarded, and unmanaged.

The company also had to mitigate identity risks associated with a massive number of SaaS services, with an average of 109 new apps added every year. At the same time, The organization was expanding its service lines and its financial products for renters and operators, leading to a complex and diverse set of SaaS services within each business initiative and group.

Centralize Identity Discovery and Offboarding

The company chose Grip to give its security teams on-demand insights into identities using web apps, SaaS services, and cloud accounts. With Grip, the company's security team can uncover federated and unfederated SaaS accounts and automate offboarding for risky SaaS services, dangling access, zombie accounts, and tenant redundancy in just a few clicks.

The same workflows are now being applied to SaaS breach response. When SaaS providers or web services experience a breach, The company's security team can instantly see if and where they are affected, and secure identities and access to the compromised SaaS and web apps.

grip

Case Study

Responding to Identity Attacks

For the company, visibility to the global identity attack surface is crucial. Grip provided the security team with relevant, actionable insights into risks that matter, prioritizing mitigations for each SaaS app's inherent risk and access controls for each user of the SaaS service. This helped the company to stay ahead of cyber threats and ensure the protection of its identities and assets.

Cyber-attacks against identities and SaaS breaches are on the rise. As with the 0ktapus threat campaign targeted SaaS services, and phishing, smishing, and vishing schemes impacted popular services like Twilio, Uber, Dropbox, and CircleCI, among others, the identity attack surface has never been more exposed for the company, too.

In such cases, their security team can now quickly identify, and pinpoint identities exposed to a compromised SaaS service, without waiting for identities to be exploited by "an event".

The company's Vice President for Information Security echoed the need for SaaS security to be identity-first: "The only way to manage SaaS security at scale is to focus on identity as the only available constant in every SaaS account. At the company, we want to secure the workforce, not block them. But our SaaS-Identity risk landscape is often hidden as our typical business philosophy enables users to have choice. Grip eliminated that struggle with continuous line-of-sight to secure identities and SaaS from one place, and its ability to automate routine and response tasks."

Mitigating SaaS Sprawl Risk

The company recognized the need to contain identity and SaaS sprawl. Grip's panoramic view of all SaaS usage, without proxies, agents, or user disruptions, helped them to do just that.

With just a 10-minute deployment, Grip uncovered hundreds of previously unknown SaaS accounts, abandoned credentials, and dangling access for former employees. By finding these risks, The company's security team was able to prioritize risks for remediation and implement consistent playbooks as their SaaS-Identity risk landscape evolves.

Conclusion

For the company, SaaS and identity security are inextricably linked. And the challenge is only getting more complex with the proliferation of SaaS applications and the increasing sophistication of cyber threats – specifically targeting employee accounts to SaaS services that have become essential for running a digital enterprise.

By adopting Grip, the security team can mitigate and control the worldwide SaaS identity risk landscape, prioritize risks that matter, and curb risk or respond to cyber-attacks.

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