CASE STUDY

Why a leading Fintech chose Grip to automate SaaS security

Industry
E-commerce, Fintech

Company Profile
International e-commerce and fintech developer, enabling organizations and brands to optimize online commerce, customer loyalty, and revenue growth.

Problem

- Lacked visibility of employee SaaS usage
- Manual SaaS discovery process
- Manual employee offboarding process

Solution
Grip SaaS Security Control Plane

Outcomes

- Continuous visibility of new SaaS applications used by employees
- One-click secure access and automate secure offboarding
- Relevant risks, prioritized based on real-world observations
- Avoid SSO upgrade costs for SaaS applications

> *““Grip has automated our ability to gain full visibility of SaaS applications. The platform centralizes SaaS risk management, and it is more comprehensive and automated than the other solutions we evaluated.“*

Director of Corporate Security and IT

The company is one of the fastest growing e-commerce platforms and helps entrepreneurs, agencies, and developers build amazing online shopping experiences. With more than 20,000 brands, and millions of brand customers have created more than one million pages to compete with behemoths like Amazon. As a fast-growing company in a booming segment, the company has expanded in almost every area as it strives to maintain category leadership.

Automating SaaS Security Risk

The company’s security strategy has been to partner with business owners and never get in the way of productivity. Using SaaS services helped employees use the most effective tools for their job, and it has allowed the organization to move quickly and respond to market needs faster. One downside of a decentralized SaaS model, however, was the security team did not have visibility into the cloud services and apps being used. Grip automated SaaS discovery and access control for cloud services and apps, giving the security team a unified view of SaaS risk.

Leverage Existing Infrastructure, Easy Deployment, Clear ROI

As standard practice, the organization conducted a detailed review of competing solutions on the market and selected Grip for its ability to leverage their existing infrastructure, fast deployment with zero disruptions. Grip requires no agents, proxies, or network dependencies.

Other solutions were not compatible with existing systems and infrastructure, which included an IdP, single sign-on, and a password manager. Several of the other solutions the team evaluated would have required the company to add to or change their infrastructure, adding cost and complexity to the project.

The Grip SaaS Security Control Plane was compatible with their existing environment. The deployment required only a few minutes of technical work to provide access to an internal system. Grip identified existing and former users, which allowed the security team to mitigate dangling access for 100+ former employees to over 40 SaaS applications.

Most Comprehensive SaaS Discovery

Initially, the firm's security team knew of about 150 applications that current employees were using. After the first Grip discovery, 335 different applications were identified—more than 100 percent more than expected. Grip, then attributed SaaS apps to business groups and rated each with Grip's SaaS Risk Index (SRI) — prioritizing risks based on real-world observations and SaaS functions.

In addition to the total number of applications being used, the Grip dashboard also showed the following data:

- Sanctioned or unsanctioned status
- Number of users for each application
- SSO integration (or missing SSO)
- Authentication type used by the user

Grip's analysis helped the security team understand which applications were widely used in the company, which would help them prioritize their risk assessment work. The security team uncovered overlapping applications that served the same purpose, acknowledging the benefits to the company's strategy to standardize the SaaS security lifecycle for all apps rather than operating security separately for each app or business group silos.

Automated Employee Offboarding

Grip's secure access and automated offboarding was an instant success—the ultimate quick win with high impact.

When an employee leaves the company, the security team was tasked to discover and turn off access to all the employee's SaaS apps. The challenge became more daunting when trying to deprovision and offboard user access when SaaS apps were accessed via simple username and password.

Grip's orchestration workflows enabled the security team to offboard hundreds of users and apps with just a few clicks—reducing the time to validate user-access revocation from weeks to minutes—even for users with more than 150 SaaS apps and 100+credential pairs (username/password).

Before Grip, offboarding SaaS apps and users was a manual process with the security buried in logs and stitching data from across 9 different network-based systems. Now, with Grip, an uncertain and time-consuming process became easy, fast, and complete with the click of a button.

Conclusion

The challenge for today's enterprise is to unify SaaS security—core-IT and business-led IT—to make SaaS safe for everyone, anywhere, and on-demand. Often, SaaS security consists of blending capabilities from a patchwork of technologies ill-suited to business-led IT strategies.

Early wins turned into standard practice to identify SaaS threats, mitigate business-led SaaS risks, and corral the global SaaS estate with automated detection and intelligent workflows for fast, effective SaaS security.