Software Company Improves SaaS Governance and CASB Performance

Industry:
Software

Size:
200 FTE's plus 200-300 seasonal employees

Headquarters:
Southeastern US

Primary Challenges

- Uncontrolled employee-led IT and shadow SaaS
- Gaps in SaaS security, particularly for Mac users
- Inefficient SaaS account offboarding

Grip Impact

- 91-95% of SaaS runs through SSO.
- 300 apps and 1,110 identities now centrally managed.
- 100% automated offboarding workflows.

> "We finally have a system in place to see who's using what, track authentication methods, and enforce security policies."

> "We assumed there was some shadow IT happening, but we didn't expect to find entire teams using paid applications with annual contracts—without any business justification or proper security reviews."

For years, a software company's security team had a handle on their IT ecosystem—or so they thought. Like many companies, they relied on a mix of security tools, including Microsoft Defender, to manage risks and monitor endpoints. But as their workforce grew, evolved, and more teams independently embraced SaaS, an unsettling realization emerged: entire departments were using SaaS applications that IT had no visibility into.

Finance, marketing, developers, and other teams across their organization all had adopted their own preferred tools, often purchased with company funds but never documented, never vetted, and never aligned with security policies. Employees using Mac computers presented another challenge—Microsoft's security stack lacked adequate coverage for them, creating more blind spots for the security team.

The Lead Security Engineer described the scope of the problem: "We assumed there was some shadow IT happening, but we didn't expect to find entire teams using paid applications with annual contracts—without any business justification or proper security reviews."

Despite their best efforts, the security team knew they had gaps in securing the SaaS used across the organization. The company had 300 SaaS applications and over 1,100 identities in use, and seasonal hiring spikes only added to the SaaS account and identity complexity. They needed a way to gain control over SaaS usage without disrupting business operations—and without adding an unmanageable burden to their small security team.

Searching for a Better SaaS Security Solution

As the gaps became more apparent, the security team explored their options. They had considered expanding their use of Microsoft's tools, but the limitations—particularly around Mac coverage—still left gaps. They also explored third-party security vendors, including CrowdStrike, to complement their stack. But none of these solutions gave them what they truly needed: real-time visibility into SaaS adoption, automatic enforcement of security policies, and a way to proactively manage the unwieldy nature of employee-led IT.

They needed a tool that wasn't just about blocking or monitoring SaaS applications—it had to help them understand their SaaS ecosystem and take meaningful action. That's when they found Grip.

Gaining Control Over SaaS Sprawl

With Grip, this software company finally gained the oversight they had been missing. Almost immediately, the platform uncovered a staggering amount of shadow IT—entire departments using applications that no one in IT had approved. Grip's automated business justification process helped them assess whether these apps were truly necessary, and in some cases, identify overlapping tools that could be consolidated.

"In one instance, we found five different tools that all did the same thing," one analyst noted. "A lot of it came down to employee preference, but Grip helped us rationalize our SaaS portfolio and enforce better policies."

Beyond just discovery, Grip's integration with Zscaler allowed them to enforce policies in near real-time. If an employee attempted to access a risky application or use a business email for a personal application, Grip automatically flagged it, prompting IT to intervene or block access as needed. And when it came to offboarding employees—a previously cumbersome and inconsistent process—Grip provided clear insights into which SaaS accounts needed to be revoked, preventing lingering access risks.

Grip wasn't just another security tool—it was a fundamental shift in how they managed SaaS risk.
"We finally have a system in place to see who's using what, track authentication methods, and enforce security policies. Before Grip, that level of insight just didn't exist," their lead security engineer commented.

A More Secure, Efficient Future

Since implementing Grip, this software company has transformed its approach to SaaS security. Their identity management process is tighter, with 91-95% of SaaS applications now running through SSO. They've gone from zero archived applications to 300 actively monitored, giving them full transparency into what's in use and what needs to be eliminated.

Perhaps most importantly, their small security team is no longer overwhelmed by manual reviews and reactive firefighting. Automation now ensures accounts are properly offboarded when employees leave or change roles, allowing the team to focus on strategic improvements—monitoring account influx, tracking unmanaged app volume, and mitigating SaaS risks.

And the experience of working with Grip's customer success team? They report it's been one of the best vendor relationships they've had. "We've worked with 50+ vendors, and Grip's team stands out. The support, the reporting process, the onboarding—it's top-notch. They truly feel like an extension of our team."

> "We've worked with 50+ vendors, and Grip's team stands out. The support, the reporting process, the onboarding—it's top-notch. They truly feel like an extension of our team."

Grip has delivered more than just visibility—it's given them confidence. Confidence that their SaaS landscape is under control, their security policies are being enforced, and their IT team is able to support employee-led IT while simultaneously safeguarding their organization.

And for any company struggling with the challenges of employee-led IT? The security team has a simple message: "Grip makes it easy. Grip provides the oversight needed before SaaS sprawl becomes an unmanageable problem."