



Endor Labs Improved SaaS Visibility, Control, and Efficiency

Key Outcomes:

Automated offboarding workflows now in place

Improved SaaS governance and access controls

Optimized SaaS usage and costs

ENDOR LABS

Industry:

Technology / Supply Chain Security

Size:

124 Employees

Headquarters:

California, with offices globally

Primary Challenges

- SaaS visibility blind spots
- Incomplete account offboarding
- Credential hygiene & operational efficiency
- High-risk OAuth connections

Grip Impact

- Automated offboarding workflows now in place
- Improved SaaS governance and access controls
- Optimized SaaS usage and costs

“The Grip team has been phenomenal—proactive, responsive, and truly invested in our success. They understand the challenges modern security teams face and deliver solutions that actually work.”

– Varun Badhwar, Founder & CEO, Endor Labs

When you're a company that helps developers secure their software dependencies, securing your own environment isn't just important—it's imperative. As a rapidly growing innovator in software supply chain security, [Endor Labs](#) recognized the urgency of managing [SaaS security](#) at scale and set out to tackle the challenge head-on.

Like many modern organizations, Endor Labs relied on a growing ecosystem of SaaS applications to power its operations. But with no centralized oversight, the company faced significant security and operational risks. Unmanaged apps were being adopted without proper review, [high-risk OAuth connections](#) left lingering access, and inefficient offboarding meant former employees retained access to corporate tools. Without full visibility, tracking SaaS usage, role-based accounts, and redundant applications was nearly impossible.



“As a security-first organization, we knew we needed to get ahead of our SaaS sprawl before it turned into a real risk. But the lack of visibility and control made it difficult to enforce strong security practices across our environment,

– Karl Mattson, CISO of Endor Labs

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.

The Challenge: Shadow SaaS and Operational Inefficiencies

- **Visibility Blind Spots** – Without a full view of their SaaS footprint, the security team struggled to track usage, access, and integration points. Some apps were integrated with Google, but many others were completely unmanaged.
- **Offboarding Risks** – Employees who left the company sometimes retained access to SaaS tools due to inconsistent offboarding processes.
- **High-Risk OAuth Connections** – Third-party integrations created potential security risks, as some applications retained excessive permissions even after they were no longer actively used.
- **Credential Hygiene & Operational Efficiency** – Manual security hygiene efforts slowed productivity, while redundant and underutilized SaaS tools increased costs.
- **Uncontrolled SaaS Sprawl** – Without a standardized intake process, employees adopting new SaaS apps opened the company to potential compliance and security risks.

Endor Labs knew they needed a proactive SaaS security strategy—one that provided visibility, control, and automation, especially as they continued to grow. Having seen Grip's impact firsthand at a previous company, Karl knew exactly where to turn. Grip's proven ability to uncover hidden risks and streamline SaaS security made it the clear choice.

The Solution: How Grip Helped Endor Labs Take Control

Using Grip's [SaaS Security Control Plane](#) and Grip [Extend User Security](#), Endor Labs gained a centralized and automated approach to SaaS security. Almost immediately, Grip's platform uncovered unmanaged and [shadow SaaS](#) applications, strengthened access controls, and optimized security operations. With these insights, the Endor Labs security team was empowered to take proactive control over their SaaS environment, gaining:

Full Visibility into Shadow SaaS

[Grip](#) mapped out every SaaS application in use across Endor Labs, giving the security team a complete and accurate baseline of their SaaS environment. This allowed them to track unmanaged apps, role-based tools, and last-known app usage, including SaaS outside of their IdP or lacking SSO.

Secure & Efficient Offboarding Workflows

By automating the revocation of access, Grip eliminated dangling permissions left behind by former employees, ensuring that no user retained access to accounts or sensitive data after their departure.

Real-Time User Access Insights

Grip provided granular visibility into who had access to which applications and how they were authenticating into them, significantly improving access governance and reducing risks from excessive permissions.

SaaS Usage & Cost Optimization

By tracking the last-known usage of SaaS applications, Grip enabled Endor Labs to reduce unnecessary licenses and reallocate resources efficiently.

Redundant SaaS Identification

Grip's insights revealed duplicative or overlapping applications, allowing Endor Labs to consolidate software usage, improve efficiency, and further reduce costs.

Better App Adoption Controls

With Grip's structured intake processes, Endor Labs could enforce security policies and compliance controls when new SaaS tools were introduced, including the tools adopted independently by employees.

"Grip transformed the way we manage SaaS security. From visibility to offboarding and access controls, their platform gave us the automation and intelligence we needed to stay ahead of threats," remarked Karl.

Building a Stronger Security Posture with Grip SSPM

Endor Labs built a strong SaaS security foundation by actively managing identity risks. To further strengthen their defenses, they recently added [Grip's SSPM](#) to secure business-critical applications like Salesforce and Google Workspace. This ensured that hidden misconfigurations wouldn't expose the company to unnecessary risk. "Adding Grip SSPM broadened the SaaS security program we have in place," said Karl. "With our user identities secure, proactively identifying and correcting application misconfigurations provides another layer of defense, ensuring our SaaS environment is as secure as possible."



"Grip transformed the way we manage SaaS security. From visibility to offboarding and access controls, their platform gave us the automation and intelligence we needed to stay ahead of threats,"

- Karl Mattson, CISO of Endor Labs

Grip: A Trusted Security Partner

Beyond the technology, the partnership with Grip has been a key differentiator. "The Grip team has been phenomenal—proactive, responsive, and truly invested in our success," said Varun Badhwar, Endor's Founder and CEO. "They understand the challenges modern security teams face and deliver solutions that actually work." With Grip, Endor Labs has turned SaaS security from a blind spot into a strength, ensuring they remain at the forefront of both software security and operational efficiency.