CASE STUDY

How NFP's security team leveraged Grip to keep pace with enterprise growth

INDUSTRY
Financial Services

REGION
North America

CASE + IAM
Microsoft

NFP spends 80% less time mitigating SaaS identity risk and **reduced IAM costs by $800K**

> "We improved security efficiency and protection well beyond the reach of IAM and CASB tools. Grip was built for the way SaaS is consumed at NFP, focusing on visibility and identity risks, even for SaaS services used outside IT control or oversight. Now, discovering and mitigating SaaS exposures, along with credential and identity risks gets done in minutes, not months."
>
> **- Scott Crim, Director of Cybersecurity**

Challenge

- As the company grew with 30+ mergers and acquisitions each year, the number of identities, credentials, and SaaS apps also increased. NFP needed on-demand and continuous discovery for SaaS services — most of which were outside direct IT ownership.
- NFP had to bridge the gap between business teams who just want to move fast while still providing the visibility and control that the security team needs to protect identities entangled with hundreds of SaaS apps and services.
- Though heavily invested in Microsoft CASB and IAM solutions, these tools did not properly fit to NFP's business-led SaaS reality, when identities and SaaS operate outside IT and security control.

Solution

- Efficient security operations with continuous visibility to NFP's SaaS estate and automated offboarding to reduce the risk of unauthorized access for SaaS services and apps

Outcomes

- Fast integration for acquisitions and instant security for identities
- Remove the risk of dangling access with automated offboarding
- Cut cost and exposure by consolidating SaaS apps and tenants
- Extend and enrich IAM and CASB to SaaS previously unreachable

Universal secure access and offboarding

NFP's rapid growth created additional security challenges for safe access to SaaS applications outside the direct control and management of the IT or security team. Each year, NFP had routinely acquired between 30 and 50 companies ranging from small LLCs to organizations with hundreds of users. At the same time, NFP was expanding its service lines and portfolio of wealth management products, leading to an exponential diversity of SaaS services within each business. The only constant factor was **identity.** NFP chose Grip for its identity-based SaaS discovery to uncover user-SaaS relationships and automate offboarding for risky SaaS services, dangling access, zombie accounts, and tenant redundancy.

> "Grip was the only solution that could mitigate our identity sprawl. In the first week of deployment, we eliminated years of identity risk, including offboarding targeted users and apps in just a few clicks. Our business-led IT strategy has enabled rapid growth while expanding our SaaS footprint — Grip secures our distributed identity perimeter whenever and wherever SaaS is used and gives my team the visibility and control needed to secure NFP's modern work strategy."
>
> **- James Fritz, CISO**

Grip's automated offboarding enabled NFP to remove the risk of unauthorized access to SaaS and helped the security team get more done and effectively integrate new acquisitions.

SaaS breach response and mitigation

Cyber-attacks and SaaS breaches have been well-documented in recent reports from the 0ktapus threat campaign of 2022 to the phishing, smishing, and vishing schemes that impacted Twilio, Plex, Dropbox, Signal, Uber, and Digital Ocean, among others.

When SaaS providers experience a breach, NFP can instantly see if and where they are affected, and secure identities exposed to a compromised SaaS service.

For NFP, visibility and awareness are critical. Grip gives the security team on-demand insights into SaaS use, misuse, and abuse by continuously discovering SaaS as it is consumed by NFP users, regardless of network status, device, or location — all without proxies or agents.

Grip gave NFP relevant, actionable insights to pinpoint risks that mattered based on accessibility and impact of each SaaS app's inherent risk and validates access and secure authentication for each user of the impacted SaaS service.

Automation and workflows

NFP has invested heavily in security: people and technology. It was imperative for SaaS security initiatives to integrate with NFP's overall cloud security program, enriching their current stack without adding another silo.

That's why NFP chose Grip with its seamless integration with existing IAM and email systems, allowing for a 10-minute deployment with zero infrastructure change. Additionally, Grip's automated workflows improved user access reviews, forensics, and SaaS use justification for NFP to be always audit-ready.

Conclusion

Identities are the primary focus for cyber-attacks, including more than 83 million credential attacks per month, worldwide. NFP mitigates the expansion of identity risk in their enterprise SaaS layer by harnessing Grip's panoramic view of user-SaaS relationships — no proxies, no agents.

NFP removed risk from identity sprawl and access debt as a regular challenge with rapid acquisitions, many of which had years of accumulated risk from unguarded SaaS apps and services.

NFP's security team can now scale protection and tune controls for their business-led IT reality, all while maintaining high security standards for SaaS and identities — past, present, and future.