Case Study

Industry: Non-Profit

Region: North America

Solution

Grip SSCP enabled the security team to get line-of-sight to their identity attack surface, enabling centralized discovery and management for identities.

Challenge

- Identity sprawl became a major concern for the security team, and most of these identity-SaaS relationships were unreachable for IAM, CASB, and Network based controls.
- Control gaps for identities needed to be strengthened while maintaining choice and flexibility for their users to continue their mission of education and conservation.
- Although several controls were in place, such as IAM and CASB, it was impossible to manage user identities and access privileges without direct knowledge of identity exposures before they became exploits.

Results

- Eliminated identity exposures from dangling access and inactive accounts.
- Automated access revocation for risky SaaS and more complete SaaS offboarding for former employees
- Prioritized apps for SSO

Grip Helps a Leading Conservation Organization Transform Their Identity Attack Surface

> Grip was the only solution with the capabilities needed to safeguard our identity sprawl. Grip helped us discover unfederated SaaS we previously did not know were being used. We gained tremendous visibility and started removing accumulated identity risk within hours of Grip's initial deployment, including offboarding targeted users and apps using automated workflows.
>
> ***-Head of Information Security***

Centralize identity discovery and offboarding

The research and conservation organization underwent a rapid transformation, which posed significant security challenges in terms of accessing SaaS apps and services outside the direct control and management of the IT or security team. The organization faced the issue of users frequently changing roles, responsibilities, or leaving the organization, while new employees and teams pushed the organization's identity attack surface to encompass the globe.

To add to this challenge, the organization also had to manage an enormous number of SaaS applications, with an average of 74 new apps added every year. The organization's expansion increased the diversity of SaaS services, leading to an exponential rise in the need for specialized SaaS, where identity was the only constant factor.

They chose Grip SSCP because of its innovative identity-based discovery, uncovering user-SaaS relationships and automate actions such as offboarding, to eliminate risky relationships.

Grip's SaaS security innovation allowed the organization's security team to pinpoint identities whenever and wherever SaaS was used, enabling them to remove redundant SaaS and centralize control with decentralized enforcement to give identities protection they need and instantly eliminate unwarranted or unjustified identity use with targeted SaaS services.

grip

> It's a difficult balance to enable a highly distributed workforce with such diversity of tools and SaaS apps in use. Grip gives us the right balance and helps our researchers and animal specialists to stay on mission and focus on care and conservation. Users get the choice and options they want, and my team doesn't have to sacrifice security to give it to them
>
> ***-Head of Information Security***

Enhance identity risk protection

For this customer, visibility (for SaaS and identities) is crucial. Grip provided the security team with on-demand insights into SaaS use, misuse, and abuse, and continuously discovers identity-SaaS relationships, regardless of network status, device, or location, without proxies or agents.

Recent reports have shown that cyber-attacks 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 organization. In such cases, the organization can now quickly identify and locate identities that were exposed to a compromised SaaS service, without waiting for identities to be exploited.

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.

As identities are the primary target for cybercriminals and attackers, with more than 25 million brute force attacks every day worldwide, the organization was able to contain identity and SaaS sprawl by utilizing Grip's panoramic view of user-SaaS relationships, without proxies, agents, or user disruptions.

Conclusion

Identities are the top target for cybercriminals and attackers, including more than 80 million monthly identity attacks targeting corporate credentials.

By adopting Grip, the security team could now manage an enormous number of SaaS applications, their continuous identity expansion, and the emergent identity attack surface entangled in SaaS relationships. At the same time, the organization's security team got on-demand insights and automated workflows, making it easy to classify and assess SaaS services for justification, audit, and access review.

As cyber-attacks and SaaS breaches continue to rise, Grip is a key partner to control the identity attack surface anytime and anywhere SaaS is used – retaining choice while keeping identity protection airtight.

Grip empowers customers to secure modern work and business-led IT with visibility and control for the global SaaS estate—anywhere, everywhere, and on-demand. Learn more at grip.security

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

AICPA SOC