grip

CASE STUDY

TEXAS BAPTISTS®

INDUSTRY
Non-Profit

REGION
North America

Texas Baptists spend 80% less time
mitigating SaaS identity risk

How Texas Baptists Leverage Grip to Secure SaaS and Stay on Mission

"We improved security efficiency and protection well beyond the reach of other tools. Grip was built for the way SaaS is consumed across our users, focusing on visibility and identity risks for all SaaS classes and types, especially those self-provisioned by users. Now, discovering and mitigating SaaS exposures, along with removing the cost of redundant apps has made us more secure and better stewards of our IT resources."

- Dave Lyons, Director of IT and Security

Challenge

- As modern work and work-from-anywhere transformed the environment for Texas Baptists, the number of identities, credentials, and SaaS apps also increased. The security team needed on-demand and continuous discovery for SaaS services — most of which were out of sight.
- Texas Baptists needed to bridge the gap between ministers and ministry teams who just want to forge ahead while still providing the visibility and control that the security team needed to protect identities entangled with hundreds of SaaS apps and services.
- Although several controls were in place, such as Google Workspace for OIDC, the security team at Texas Baptists still needed to maintain line-of-sight to all user and SaaS connections, especially those outside sanctioned access controls.

Solution

- Efficient security operations with continuous visibility to each identity-SaaS relationship and automated offboarding to reduce the risk of unauthorized access to the SaaS estate

Outcomes

- Remove the risk of dangling access with automated offboarding
- Cut cost and exposure by consolidating SaaS apps and tenants
- Extend and enrich IAM and OIDC to SaaS previously unknown

Universal secure access and offboarding

Texas Baptists' rapid transformation created additional security challenges for safe access to SaaS applications outside the direct control and management of the IT or security team. Each year, Texas Baptists have cohorts of users changing roles, responsibilities, and even leaving the organization just in time for another round of ministers and ministry teams to join. The continuous fluctuation of users was matched only by the sheer number of SaaS applications, tallying up to an average of 62 new apps per year.

> "I thought Grip was going to be a one-trick pony. What surprised us was just how much our SaaS and identity landscape changed day-to-day, week-to-week. In the first week of deployment, we eliminated years of identity risk, including offboarding targeted users and apps in just a few clicks. Then, we just kept piling up victories for safer SaaS by leveraging Grip regularly. Grip sees it all as it happens, so we're never in the dark about which SaaS are being used, who's using it and what protections are in place for secure access. Then, Grip secures those identities whenever SaaS is used."
>
> **- Dave Lyons, Director of IT and Security**

At the same time, Texas Baptists were expanding the reach of its ministries and ministers to nearly encompass the globe, leading to an exponential diversity of SaaS services within each individualized ministry need. The only constant factor was **identity**.

Texas Baptists chose Grip for its identity-based SaaS discovery to reveal user-SaaS relationships and automate actions, such as offboarding, to sever risk relationships. Additionally, Grip's SaaS security innovation enabled the security team to pinpoint identities whenever and wherever SaaS was used — identifying key areas of opportunity to remove redundancy, reclaim licenses, and consolidate redundancies as they emerged.

Finally, Texas Baptists leveraged Grip's automated offboarding enabled to remove the risk of unauthorized access to SaaS (such as dangling access for former users) and helped the security team get more done and effectively integrate new identities and initiatives.

SaaS visibility and risk response

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

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 are compromised or abandoned SaaS contains zombie accounts, Texas Baptists can instantly see if and where identities are exposed to a compromised SaaS service, without sitting back to wait for "an event".

Grip gave the security team relevant, actionable insights for risks that mattered and prioritizing mitigations for each SaaS app's inherent risk and access controls for each user of the SaaS service.

Conclusion

Identities are the top target for cybercriminals and attackers, including more than 25 million brute force attacks every day, worldwide.

Texas Baptists identity and SaaS sprawl by utilizing Grip's panoramic view of user-SaaS relationships — without proxies, agents, or user disruptions.

Texas Baptists removed risk (and cost) from hidden and redundant SaaS services, easily classified and assessed with automated workflows for justification, audit, and access review.

The security team can now scale safeguards to all SaaS whenever and wherever it is used — along with shaving license cost from better awareness of SaaS and the identities consuming it — anywhere, everywhere, and on-demand.