Fortune 300 Interpublic Group's Journey to SaaS Security and Empowerment

Industry:
Advertising Services

Size:
Fortune 300; 90,000 employees

Headquarters:
New York, NY

Primary Challenges

- Shadow IT
- SaaS Sprawl
- SaaS Cost Reduction

Grip Impact

- Uncovered 10x the number of account IDs in existence.
- Reduced software costs by millions of dollars.
- Identified and prioritized which apps should be considered for SSO and MFA.

> "Grip solves real risk problems that no one else is solving."
>
> Troy Wilkinson
> Global CISO

Every company has a SaaS problem, regardless of industry. The Interpublic Group (IPG), a publicly traded Fortune 300 advertising company, was no exception. Containing SaaS sprawl and reducing SaaS risks were significant challenges for the premier global advertising conglomerate—problems they could not solve with other tools.

IPG's operating environment is expansive and complex, comprised of 400 subsidiaries rolling up into ten global groups, each with its own CISO and all reporting to the parent enterprise. Even with centralized IT and security, IPG knew they had a shadow IT problem. The dynamic and high-stakes nature of the advertising business often required staff to acquire SaaS tools quickly, bypassing standard procurement procedures. Thus, IPG began their quest to find an appropriate solution to fix a massive problem, although, at the time, they had no idea just how big their problem was.

The Challenges

IPG needed a comprehensive SaaS risk management solution based on the staff behaviors they observed, including:

Unmonitored SaaS Adoption:

Employees were independently registering for SaaS and AI services, such as ChatGPT, without proper company oversight or usage tracking, potentially compromising data privacy compliance.

Complex Offboarding Processes:

The organization's vast size made employee offboarding cumbersome, highlighting the need for an automated solution to reset passwords and revoke access to SaaS tools promptly and securely.

Insufficient Visibility into SaaS Apps and Cloud Services:

A lack of comprehensive insight into their extensive SaaS and cloud infrastructure, including AWS, GCP, and Azure, made it challenging to administer and enforce security controls.

License Utilization and Reclamation:

With operations on a global scale, IPG needed to ensure that software licenses were optimally allocated and actively used, aiming to recover and reallocate resources from inactive accounts.

Unauthorized Data Handling:

IPG discovered a recurring problem of employees uploading sensitive information to non-approved platforms, bypassing established data governance protocols.

Each of these pain points contributed to an environment ripe for malicious actors. IPG was intent on finding a solution that could provide clear visibility into its SaaS and cloud usage, facilitate the enforcement of policies, and reduce vulnerabilities within its digital ecosystem.

Demonstrating Impact

IPG experienced immediate value after implementing Grip, including:

Discovery of Rogue Cloud Accounts:

IPG estimated they had 35 AWS account IDs, but the actual number was far greater. Grip SSCP discovered ten times that amount, uncovering 350. The improved visibility into their cloud environment has allowed IPG to gather more information on the newly discovered IDs, implement stricter security controls, and move them under their corporate account, saving them millions of dollars.

Software License Cost Reduction & Optimization:

Using Grip's ability to audit SaaS usage by user, allowed IPG to reclaim unused SaaS licenses and renegotiate software contracts, saving them more than the cost to purchase the Grip solution.

Consolidation of SaaS Applications:

By identifying overlapping apps, IPG merged duplicate SaaS tools, phased out redundancies, and further decreased software expenditures.

Policy Enforcement:

IPG strengthened the enforcement of company policies on handling sensitive data and client documents. Access to unauthorized data repositories was terminated, and the use of approved applications was reinforced.

Prioritized Security Measures:

Grip provided recommendations of which apps needed Single Sign-On (SSO) and Multi-Factor Authentication (MFA) based on app risk rankings and the number of users. IPG achieved its risk reduction objectives and more. They have successfully identified Shadow IT accounts, enforced security protocols, and reduced IT costs by eliminating unused software licenses.

Developing an automated offboarding process, including using Grip for automated password resets, is currently in the queue.

> "Grip is a one-to-many solution—it's effortless to activate and delivers immediate benefits."

Troy Wilkinson
Global CISO

Looking Ahead

Reflecting on their Grip experience thus far, Troy Wilkinson, IPG's Global CISO, has nothing but positive words: "Grip solves real risk problems that no one else is solving. Our application of Grip has surpassed our initial objectives, and we have several other projects in process to reduce our SaaS risks and costs further. Grip is a one-to-many solution—it's effortless to activate and delivers immediate benefits. Our entire team is a proponent of its capabilities. In fact, the value of Grip is so pronounced that even board members routinely inquire about the insights revealed, a testament to the depth and utility of the platform's findings."

The story of IPG and Grip is not just a success story of overcoming SaaS risk challenges; it illustrates how the right SIRM technology can transform an organization.

- IPG went from a lack of visibility and control of SaaS and cloud account usage to identifying rogue account IDs and taking action to prevent misuse.
- IPG shifted from a position of vulnerability due to shadow IT and employee-driven SaaS acquisition to a business-led IT strategy, implementing the necessary SaaS security measures to safeguard the organization.
- IPG also moved from unmanaged software licenses and excessive costs to aligning software expenditures according to actual usage and need.

IPG came to Grip with specific SaaS concerns. Grip delivered more than insights into their shadow IT and cloud risks. Grip reshaped IPG's strategy towards SaaS security, demonstrating the comprehensive impact and the enabling power SIRM can have throughout an organization.

The story of IPG and Grip is not just a success story of overcoming SaaS risk challenges; it illustrates how the right SIRM technology can transform an organization.