Case Study

Global Streaming Service Chose Grip for SaaS Identity Risk Management

Global Streaming and Entertainment

One of the largest music and video streaming service with more than 150 million subscribers worldwide.

Industry: Entertainment mass media, content and streaming service

Region: North America

Solution

Grip SaaS Security Control Plane

Challenge

- Manual, incomplete process to discover all SaaS users and accounts
- Thousands of business-led SaaS apps across teams and projects, not governed by IT
- High volume of transient users, dynamic account provisioning, and sporadic access
- Distributed access authorization without centralized control or monitoring

Results

- Continuous discovery and visibility of new SaaS services and cloud accounts
- Automated offboarding and access governance for unfederated SaaS
- Reduce the workload for security and identity teams by 80%
- Decrease the time to authorize new SaaS usage from days to minutes

> Grip gives my team centralized visibility into all the SaaS that is being used by and reduced our workload by more than 80% by automating unfederated SaaS offboarding and mitigating SaaS identity risks.
>
> *Head of Information Security*

Like many modern enterprises, the employees of this company use SaaS heavily. But entertainment studios face a unique challenge because teams scale up and down based on production schedules, and access needs are sporadic. Though everyone is working off the same script, the work is very decentralized with teams using the tools of their choice to get the job done. The industry also tends to use a high number of contractors, and their access needs also vary depending on the team and work they are doing.

The sprawling production supply chain creates identity risk because each person uses dozens of different SaaS apps, and they may also be members of multiple production teams. The SaaS-Identity risk landscape is continuously in flux, with people joining, leaving, or changing teams constantly. The company supports the use of SaaS for its productivity and cost benefits, however, monitoring all the SaaS being used and controlling the access was extremely difficult.

The team was manually searching multiple systems and tracking the SaaS usage manually. Multiple teams were involved, and the workload had unpredictable spikes because it was driven by production schedules. Every time there was a production project starting, people were dedicated to do the initial discovery and track the SaaS usage throughout the project. The data was collected in spreadsheets, and the team struggled to keep it up to date and accurate.

Every time there was a production project starting, people were dedicated to do the initial discovery and track the SaaS usage throughout the project. The data was collected in spreadsheets, and the team struggled to keep it up to date and accurate.

grip

These were the natural outcomes of providing agility and user choice when it comes to SaaS tools and cloud apps for the company. However, the growing complexity inherent in their business-led IT strategy demonstrated how the company needed a solution to effectively monitor, secure, and manage their SaaS-Identity risk landscape.

Simplify SaaS Identity Risk Management

The team had a very manual process, and it was a challenge to keep up with the constantly changing SaaS identity risk landscape. The Grip SSSCP provided out of the box automation that included workflows such as SaaS use justification, risk analysis, and user offboarding for the unfederated apps that production employees and contractors were using.

By leveraging the automation of the Grip SSCP, the workload was reduced by over 80%. After a project is over, the security team was able to clean up SaaS access by easily identifying every SaaS account the production team was using leverage an automated workflow to secure each one of the accounts, which could run into the hundreds.

Centralized SaaS Visibility with Decentralized SaaS Usage

The Grip SSCP provided visibility to all the SaaS being used regardless of who sourced it. Every time a production employee initiates a SaaS account, the Grip SSCP discovers it and provides a risk assessment of the app. If needed, the system can also initiate a user survey to gather additional risk-related information. If an app is too risky or an alternative app is already available, the user is prompted to stop using it or move to an alternative app.

By centrally monitoring the apps being used and gathering the usage justification, the security teams can keep track of all the users and apps and only get involved when there is a security risk that needs to be addressed. The production teams can move quickly and get the job done without having to think about what apps they use or waiting for approvals.

Conclusion

With Grip SSCP, the security team can help the production teams leverage SaaS and realize benefits such as reducing costs, greater collaboration, and utilizing the newest technologies. Rather than dictating the apps and technologies centrally, the teams are given the flexibility to make those decisions on their own.

With Grip the team is enabling nearly infinite user choice without compromising security, access control, or compliance. Partnering with Grip helped the company protect their SaaS identity risk landscape and embrace SaaS usage to help production teams work more effectively and deliver the award winning content for their streaming platform.