AppsFlyer

CASE STUDY

> With Ermetic, we immediately saw the access-related risks to our environment and could quickly remediate them. No other solution provided this type of deep visibility into access entitlements and publicly accessible resources.
>
> Guy Flechter, CISO at Appsflyer.

AppsFlyer, the global attribution leader, empowers marketers to grow their business and innovate with a suite of comprehensive measurement and analytics solutions. Built around privacy by design, AppsFlyer takes a customer-centric approach to help 12,000+ brands and 8,000+ technology partners make better business decisions every day.

The Challenge

Since 2011, AppsFlyer has been on the cutting edge of cloud technology and security. The AppsFlyer platform leverages multiple clouds including AWS, Google Cloud, Azure and Alibaba Cloud. With more than 90,000 active mobile applications and more than 6,000 tech partner integrations, Appsflyer is also ahead of the curve when it comes to securing their cloud infrastructure environment. Appsflyer has one of the largest AWS deployments outside of the US, with tens of thousands of resources.

The security team made identity governance and access entitlement management a priority for 2020. For developers, DevOps and data scientists, the goal was to ensure that least-privilege access was enforced and that policies were “right-sized” for each user profile. While federating users from Okta provided control over users and groups, it was difficult to govern the use of access entitlements inside the cloud environment.

At the same time, AppsFlyer wanted to audit all access entitlements granted to the infrastructure to limit high-risk access to important resources, harden the environment and remove unused users, roles and permissions. They realized that using native CSP tools was complex, time-consuming and not repeatable, so they looked for a scalable solution.

The Solution

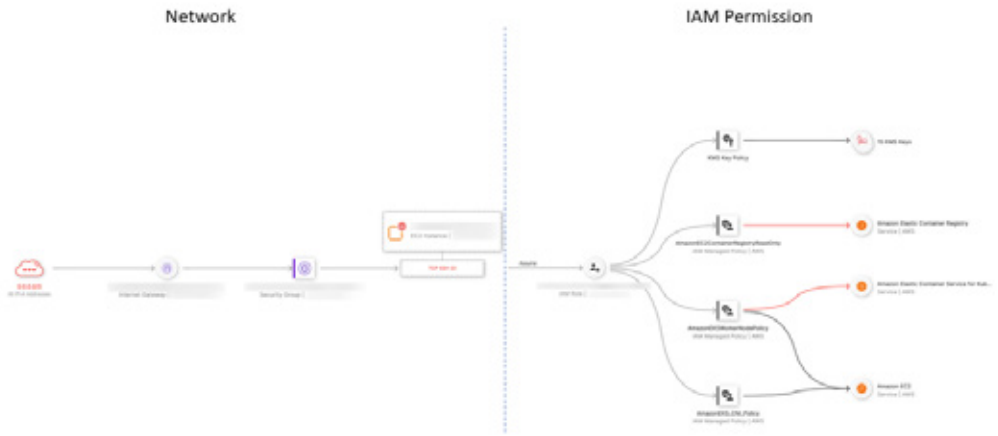
The Appsflyer security team deployed Ermetic in the staging environment. The platform immediately revealed a large number of excessive entitlements, and using the risk score provided by the platform, the team began to harden the environment by downloading improved policies and sending them to the DevOps team via the built-in integration with Jira.

For example, the team was able to visualize:

S3 buckets with sensitive information that exposed read/write permissions to the public

Public EC2 instances that are both accessible from the internet and have high IAM privileges.

Databases that are exposed to the internet



Next, the team audited all third-party access to the environment. They removed all SaaS applications (e.g. security and optimization tools) that were no longer in use. Next, they reviewed the applications that had privileged access to sensitive data, and removed unnecessary permissions. They also cleaned up IAM identities that were no longer in use. In addition, they were finally able to view the activity of the federated users from Okta, and to accurately right-size their roles.

As the team rolled out the platform into the production environment, they worked together with the development and DevOps teams to determine the process for governing identities and access entitlements on an ongoing basis from responding to new risks to integrating hardened, least privilege policies in the CI/CD pipeline.

About Ermetic

Ermetic enables enterprises to protect cloud infrastructures (IaaS/PaaS) by governing identities, access entitlements and enforcing least privilege at scale. Through the continuous analysis of entitlements and activity, Ermetic provides full-stack visibility into the effectiveness and risks of policies attached to human and machine identities for accessing compute resources, data stores and the network.The company is led by proven cyber security veterans whose previous companies were acquired by Microsoft, Palo Alto Networks and others. Ermetic is funded by Accel, Glilot Capital Partners, Norwest Venture Partners and Target Global.

For more information, visit https://ermetic.com/