



Cómo protege AppsFlyer las identidades en un entorno 100 % en la nube

ESTUDIO DE CASO



“Polyrize (ahora DatAdvantage Cloud) proporciona el panel único que me faltaba para las diferentes aplicaciones en la nube”.

Guy Flechter, CISO y DPO

Este estudio de caso fue publicado originalmente por Polyrize, que Varonis adquirió en 2020.

[MÁS INFORMACIÓN >](#)

DESTACADOS



AppsFlyer, con sede en San Francisco, 18 oficinas globales y más de 1000 empleados, es la empresa líder en atribución a nivel mundial. La misión de la empresa es permitir que sus clientes (expertos en marketing de aplicaciones y desarrolladores) midan sus campañas de marketing.

DESAFÍOS

- Protección de identidades y permisos para miles de identidades y múltiples ubicaciones
- Visibilidad y control en un entorno de nube complejo
- Aplicación de un modelo de privilegios mínimos de acceso

SOLUCIÓN

- **DatAdvantage Cloud** (anteriormente Polyrize) mapea y analiza las relaciones entre los usuarios y los datos a través de aplicaciones y servicios en la nube aislados

RESULTADOS

- Posición de seguridad en la nube mejorada al tiempo que se reducen los costos
- Capacidad de identificar a los usuarios en el centro de eventos de alto riesgo
- Detectar y responder a eventos de alto riesgo

Desafíos

AppsFlyer está comprometida con su visión como empresa nativa de la nube que le da prioridad a la nube, y ha desarrollado una red corporativa que nació en la nube. Su infraestructura de productos se basa en AWS, y todas las aplicaciones comerciales que utilizan los empleados y contratistas se basan en un entorno de SaaS.

Entonces, el principal desafío de seguridad para la organización era proteger la enorme cantidad de identidades y permisos en su complejo entorno en la nube y para miles de identidades y múltiples ubicaciones, sobre las cuales el equipo de seguridad no tenía el nivel de visibilidad y control que tendría con una red local.

Guy Flechter, CISO y DPO de AppsFlyer, advirtió: “El mayor riesgo de seguridad para nuestro entorno en la nube fue la proliferación de identidades humanas y no humanas y sus complejos permisos en numerosos servicios en la nube diferentes, lo que aumentó de forma significativa nuestra superficie de ataque. Por lo tanto, aplicar un modelo de privilegios mínimos de acceso, reducir los permisos no utilizados y mal configurados, y eliminar las identidades no utilizadas en tiempo real era un objetivo clave para nosotros”.



“El mayor riesgo de seguridad para nuestro entorno en la nube fue la proliferación de identidades humanas y no humanas y sus complejos permisos en numerosos servicios en la nube diferentes, lo que aumentó de forma significativa nuestra superficie de ataque”.

Solución

AppsFlyer ya tenía experiencia con una serie de soluciones de seguridad en la nube, como una tecnología de perímetro definido por software, para brindar acceso Zero Trust a los servicios dentro de la producción y una solución de agente de seguridad de acceso a la nube (CASB). Esta última había sido desechada antes de ponerla en práctica porque, aunque su CASB era capaz de detectar filtraciones de datos y otros incidentes, tenía un valor de seguridad limitado debido a la falta de información estratégica sobre las identidades y los privilegios.

“Aunque nuestro CASB nos permitió ver algunas actividades riesgosas de los usuarios, no brindó visibilidad con respecto a los recursos a los que tenían acceso los usuarios”, dijo Flechter. “Faltaba mucho contexto y era muy complicado identificar identidades y privilegios inseguros. Tomemos como ejemplo a Salesforce o AWS. Ni siquiera se acercó a resolver el problema de la visibilidad. Al correlacionar identidades, permisos y actividades, Polyrize (ahora DatAdvantage Cloud) nos permitió comprender qué empleados y contratistas tendrían el mayor impacto en nuestra organización en caso de que se produjera una filtración de datos o una vulneración de la cuenta debido a, por ejemplo, permisos demasiado amplios o acceso a grandes cantidades de datos críticos para la empresa”.

AppsFlyer se asoció con Polyrize (adquirida por Varonis en 2020), cuya misión es proporcionar visibilidad y control sobre las identidades y el acceso. Inicialmente plantearon un desafío difícil para el equipo de Polyrize (automatizar el proceso de rastreo y monitoreo de todas sus identidades y privilegios en tiempo real, en definitiva, en múltiples servicios SaaS e IaaS), un proceso que, hasta el momento, habían intentado gestionar a través de complicadas hojas de cálculo estáticas.



“Le pedí al equipo de Polyrize que, en primer lugar, se conectara a Okta y me dijera de manera proactiva qué grupos tienen acceso a qué aplicaciones para que yo pudiera determinar si es apropiado”, dijo Flechter. “En segundo lugar, quería poder encontrar asignaciones excesivas o mal configuradas, para que mi equipo pudiera aislar rápidamente los problemas y revocar el acceso en caso de que fuera necesario”.

Detectar y responder a eventos de seguridad

Además de abordar el caso de uso original de AppsFlyer, Polyrize (ahora DatAdvantage Cloud) agregó una capa crítica de seguridad reactiva, que le permite a AppsFlyer detectar y responder a los eventos de seguridad a medida que se producen. “Polyrize proporciona el panel único que me faltaba para las diferentes aplicaciones en la nube”, dijo Flechter. “Ser capaz de descubrir identidades inseguras, ajustar el acceso y detectar su uso indebido en la misma plataforma no solo hace que el proceso de seguridad sea fácil de administrar, sino que también brinda protección adicional cuando se producen incidentes”.

Los equipos de asistencia técnica y de éxito de los clientes de Polyrize trabajaron codo a codo con el equipo de seguridad de AppsFlyer para implementar la plataforma Polyrize e integrarla en su infraestructura y sus procesos generales de seguridad en la nube.



“El equipo de Polyrize trabajó codo a codo con nosotros durante la implementación inicial y continúa sincronizándose con regularidad con nosotros para abordar cualquier problema que surja durante las verificaciones de estado periódicas, proporcionando controles de seguridad y visibilidad con respecto al cumplimiento”, dijo Flechter. “Ahora lo consideramos un socio confiable y una parte integral de nuestra estrategia de seguridad en la nube”.



“Ser capaz de descubrir identidades inseguras, ajustar el acceso y detectar su uso indebido en la misma plataforma no solo hace que el proceso de seguridad sea fácil de administrar, sino que también brinda protección adicional cuando se producen incidentes”.

Resultados

“Los resultados han sido espectaculares”, destacó Flechter. “Actualmente, Polyrize (ahora DatAdvantage Cloud) me ayuda a minimizar nuestro radio de ataque potencial al descubrir identidades no utilizadas y permisos mal configurados, identificar a los usuarios que se encuentran en el centro de eventos de alto riesgo y detectar, responder e investigar eventos de alto riesgo después de que ocurren. Además, Polyrize (ahora Varonis) ha mejorado mi posición de seguridad en la nube y, al mismo tiempo, ha reducido los costos de mi equipo de seguridad y los gastos generales de gestión de la seguridad”.



“Polyrize (ahora DatAdvantage Cloud) ha mejorado mi posición de seguridad en la nube y, al mismo tiempo, ha reducido los costos de mi equipo de seguridad y los gastos generales de gestión de la seguridad”.



**Monitoree y detecte
amenazas en sus tiendas
y aplicaciones en la nube
más importantes.**

[SOLICITAR UNA DEMOSTRACIÓN](#)