Wie AppsFlyer Identitäten in einer 100-prozentigen Cloud-Umgebung schützt

FALLSTUDIE

„Polyrize (jetzt DatAdvantage Cloud) bietet eine einheitliche Ansicht für alle verschiedenen Cloud-Apps – genau das, was mir gefehlt hat.“

Guy Flechter, CISO & DPO

Diese Fallstudie wurde ursprünglich von Polyrize veröffentlicht, das im Jahr 2020 von Varonis übernommen wurde.

MEHR ERFAHREN >

HIGHLIGHTS

AppsFlyer, mit Hauptsitz in San Francisco, 18 weltweiten Niederlassungen und über 1.000 Mitarbeitern, ist der weltweite Marktführer im Bereich Attribution. Das Unternehmen ermöglicht es seinen Kunden – App-Vermarktern und Entwicklern –, ihre Marketingkampagnen effektiv zu messen.

HERAUSFORDERUNGEN

- Sicherung von Identitäten und Berechtigungen über tausende Identitäten und mehrere Standorte hinweg
- Transparenz und Kontrolle in einer komplexen Cloud-Umgebung
- Durchsetzung des Least Privilege-Ansatzes

DIE LÖSUNG

- **DatAdvantage Cloud** (ehemals Polyrize) erfasst und analysiert Beziehungen zwischen Benutzern und Daten über isolierte Cloud-Anwendungen und -Dienste hinweg.

ERGEBNISSE

- Verbesserte Cloud-Sicherheitslage bei geringeren Kosten
- Möglichkeit, Benutzer zu identifizieren, die im Mittelpunkt von risikoreichen Ereignissen stehen
- Erkennung von und Reaktion auf risikoreiche Ereignisse

Herausforderungen

AppsFlyer hat sich seiner Vision als Cloud-first und Cloud-natives Unternehmen verschrieben und ein Unternehmensnetzwerk aufgebaut, das von Anfang an in der Cloud entstand – die Produktinfrastruktur baut auf AWS auf, und alle von den Mitarbeitern und Auftragnehmern genutzten Unternehmensanwendungen sind SaaS-basiert.

Die größte Sicherheitsherausforderung für das Unternehmen bestand also darin, die zahlreichen Identitäten und Berechtigungen in seiner komplexen Cloud-Umgebung und über Tausende Identitäten und mehrere Standorte hinweg zu sichern. Hierbei verfügte das Sicherheitsteam nicht über den Grad an Transparenz und Kontrolle, der bei einem lokalen Netzwerk vorhanden wäre.

Guy Flechter, CISO und DPO bei AppsFlyer, bemerkt: „Das größte Sicherheitsrisiko für unsere Cloud-Umgebung war eine übermäßige Anzahl an menschlichen und nicht-menschlichen Identitäten sowie deren komplexe Berechtigungen über viele unterschiedliche Cloud-Dienste hinweg. Das vergrößerte unsere Angriffsfläche enorm. Die Umsetzung eines Least Privilege-Ansatzes, das Entfernen ungenutzter und falsch konfigurierter Berechtigungen sowie das Beseitigen ungenutzter Identitäten in Echtzeit waren für uns wichtige Ziele.“

> „Das größte Sicherheitsrisiko für unsere Cloud-Umgebung war eine übermäßige Anzahl an menschlichen und nicht-menschlichen Identitäten sowie deren komplexe Berechtigungen über viele unterschiedliche Cloud-Dienste hinweg. Das vergrößerte unsere Angriffsfläche enorm.“

Die Lösung

AppsFlyer hatte bereits Erfahrung mit einer Reihe von Cloud-Sicherheitslösungen, etwa mit einer Software-definierten Perimeter-Technologie, um Zero-Trust-Zugriff auf Dienste innerhalb der Produktionsumgebung zu ermöglichen, sowie mit einer CASB-Lösung (Cloud Access Security Broker). Letztere wurde vor der Beauftragung über Bord geworfen, da sie zwar Datenlecks und andere Vorfälle erkennen konnte, aber aufgrund fehlender Transparenz in Identitäten und Berechtigungen nur einen begrenzten Sicherheitswert hatte.

„Obwohl unser CASB uns erlaubte, bestimmte riskante Benutzeraktivitäten zu sehen, bot es keinen Einblick in die Assets, auf die die Benutzer Zugriff hatten“, so Flechter. „Viele Kontextinformationen fehlten und die Identifizierung riskanter Identitäten und Privilegien war ein Chaos. Auch in Salesforce oder AWS bleibt das Transparenzproblem ungelöst. Durch Korrelierung von Identitäten, Berechtigungen und Aktivitäten konnten wir mit Polyrize (jetzt DatAdvantage Cloud) nachvollziehen, bei welchen Mitarbeitern und Auftragnehmern im Falle eines Datenlecks oder einer Kompromittierung der größte Schaden für unser Unternehmen entstehen würde – beispielsweise durch übermäßige Berechtigungen oder durch Zugriff auf große Mengen geschäftskritischer Daten.“

AppsFlyer entschied sich für die Zusammenarbeit mit Polyrize (2020 von Varonis übernommen), um eine umfassende Transparenz und Kontrolle über Identitäten und Zugriffe zu erhalten. Für das Polyrize-Team war es zunächst eine große Herausforderung – den Verfolgungs- und Überwachungsprozess aller Identitäten und Berechtigungen über mehrere SaaS- und IaaS-Dienste hinweg in Echtzeit zu automatisieren. Zuvor hatte AppsFlyer mühsam versucht, diese Prozesse über statische Spreadsheets zu verwalten.

> „Ich habe das Polyrize-Team gebeten, sich in erster Linie mit Okta zu verbinden und mir proaktiv zu sagen, welche Gruppen Zugriff auf welche Anwendungen haben. Dadurch kann ich feststellen, ob ihr Zugriff angemessen ist“, erklärt Flechter. „Außerdem wollte ich in der Lage sein, übermäßige oder falsch konfigurierte Zuweisungen zu finden, damit mein Team Probleme schnell eingrenzen und den Zugriff bei Bedarf entfernen kann.“

Erkennen von und Reagieren auf Sicherheitsereignisse

Zusätzlich zum ursprünglichen Anwendungsfall von AppsFlyer fügte Polyrize (jetzt DatAdvantage Cloud) eine kritische reaktive Sicherheitsschicht hinzu, die es AppsFlyer ermöglicht, Sicherheitsereignisse zu erkennen und darauf zu reagieren, sobald sie eintreten. „Polyrize bietet eine einheitliche Ansicht für alle verschiedenen Cloud-Apps – genau das, was mir gefehlt hat“, so Fletcher. „Die Möglichkeit, riskante Identitäten zu entdecken, deren Zugriff auf das nötige Maß zu reduzieren und ihren Missbrauch zu erkennen – alles auf einer Plattform – vereinfacht nicht nur den Sicherheitsprozess, sondern bietet auch zusätzlichen Schutz, wenn es zu Vorfällen kommt.“

Die Support- und Kundenerfolgs-Teams von Polyrize arbeiteten eng mit dem Sicherheitsteam von AppsFlyer zusammen, um die Polyrize-Plattform zu implementieren und sie in die gesamte Infrastruktur und alle Prozesse für die Cloud-Sicherheit zu integrieren.

> „Das Polyrize-Team arbeitete während der ersten Bereitstellung eng mit uns zusammen und spricht sich weiterhin regelmäßig mit uns ab, um Probleme bei regelmäßigen Statusprüfungen zu beheben sowie Sicherheitskontrollen und Compliance-Transparenz zu gewährleisten“, sagt Flechter. „Wir betrachten es jetzt als zuverlässigen Partner und als integralen Bestandteil unserer Cloud-Sicherheitsstrategie.“

„Die Möglichkeit, riskante Identitäten zu entdecken, deren Zugriff auf das nötige Maß zu reduzieren und ihren Missbrauch zu erkennen – alles auf einer Plattform – vereinfacht nicht nur den Sicherheitsprozess, sondern bietet auch zusätzlichen Schutz, wenn es zu Vorfällen kommt.“

Ergebnisse

„Die Ergebnisse waren hervorragend“, merkt Flechter an. „Heute hilft mir Polyrize (jetzt DatAdvantage Cloud), unseren potenziellen Explosionsradius zu minimieren, indem ungenutzte Identitäten und falsch konfigurierte Berechtigungen aufgedeckt und die Benutzer im Mittelpunkt von risikoreichen Ereignissen identifiziert werden. Darüber hinaus werden Hochrisiko-Ereignisse erkannt, es wird darauf reagiert und sie werden untersucht, nachdem sie aufgetreten sind. Außerdem hat Polyrize (jetzt Varonis) meine Cloud-Sicherheitslage verbessert und gleichzeitig die Kosten für mein Sicherheitsteam und den Aufwand für das Sicherheitsmanagement gesenkt.“

„Polyrize (jetzt DatAdvantage Cloud) hat meine Cloud-Sicherheitslage verbessert und gleichzeitig die Kosten für mein Sicherheitsteam und den Aufwand für das Sicherheitsmanagement gesenkt.“

Überwachen und erkennen Sie Bedrohungen in Ihren geschäftskritischen Cloud-Speichern und -Anwendungen.

FORDERN SIE EINE DEMO AN