Come AppsFlyer protegge le identità in ambiente 100% cloud

CASO DI STUDIO

"Polyrize (ora DatAdvantage Cloud) fornisce un unico pannello di controllo per tutte le app cloud. Proprio quello che mi serviva."

Guy Flechter, CISO e DPO

Questo caso di studio è stato originariamente pubblicato da Polyrize, acquisita da Varonis nel 2020.

SCOPRI DI PIÙ ›

HIGHLIGHT

AppsFlyer, sede a San Francisco, 18 uffici in tutto il mondo e oltre 1.000 dipendenti, è il leader mondiale dell'attribuzione. La mission dell'azienda è quella di consentire ai propri clienti (app marketer e sviluppatori) di misurare le proprie campagne di marketing.

SFIDE

- Proteggere le identità e i permessi per migliaia di identità in diverse sedi
- Visibilità e controllo in un complesso ambiente cloud
- Applicazione degli accessi con privilegio minimo

LA SOLUZIONE

- **DatAdvantage Cloud** (ex Polyrize) mappa ed analizza le relazioni tra utenti e dati attraverso applicazioni e servizi cloud in silos

RISULTATI

- Miglioramento dell'approccio alla sicurezza sul cloud e riduzione dei costi
- Capacità di identificare utenti al centro di eventi ad alto rischio
- Individuare e rispondere agli eventi ad alto rischio

Sfide

AppsFlyer è impegnata nella sua visione di azienda cloud-first, cloud-native e ha costruito una rete aziendale nata nel cloud. L'infrastruttura si basa su AWS, e tutte le app aziendali utilizzate da dipendenti e collaboratori esterni sono basate su SaaS.

La principale sfida di sicurezza per l'organizzazione, quindi, era la sicurezza della profusione di identità e permessi nel loro complesso ambiente cloud e attraverso migliaia di identità e sedi multiple, di cui il team di sicurezza non aveva il livello di visibilità e controllo che avrebbe avuto con una rete on-prem.

Guy Flechter, CISO e DPO di AppsFlyer racconta: "Il più grande rischio di sicurezza per il nostro ambiente cloud era la proliferazione delle identità umane e non e delle loro complesse autorizzazioni tra i molti e diversi servizi cloud, che hanno aumentato significativamente la nostra superficie di attacco. Perciò far rispettare l'accesso con il minimo privilegio, rimuovere i permessi inutilizzati e mal configurati, ed eliminare le identità inutilizzate in tempo reale, era per noi un obiettivo chiave."

> "Il più grande rischio di sicurezza per il nostro ambiente cloud era la proliferazione di identità umane e non e le loro complesse autorizzazioni tra i molti servizi dissimili del cloud, che hanno aumentato significativamente la nostra superficie di attacco."

La soluzione

AppsFlyer aveva già sperimentato diverse soluzioni di sicurezza cloud, come una tecnologia software-defined perimeter per fornire Zero Trust Access ai servizi all'interno della produzione ed una soluzione Cloud Access Security Broker (CASB). Quest'ultima era stata abbandonata prima dell'uso perché, anche se in grado di rilevare perdite di dati e altri incidenti, aveva un valore di sicurezza limitato a causa di una mancanza di informazioni approfondite relative alle identità ed ai privilegi.

"Sebbene il nostro CASB ci permettesse di individuare alcune attività rischiose degli utenti, non forniva alcuna visibilità sulle risorse a cui gli utenti avevano accesso", ha detto Flechter. "Mancava parecchio contesto e identificare le identità e i privilegi rischiosi era veramente difficile. Prendete per esempio Salesforce o AWS, non si sono avvicinati a risolvere il problema della visibilità. Mettendo in correlazione identità, permessi e attività, Polyrize (ora DatAdvantage Cloud) ci ha permesso di capire quali dipendenti e collaboratori avrebbero avuto il maggior impatto sulla nostra azienda in caso di perdita di dati o compromissione degli account dovuta, per esempio, ad autorizzazioni o accessi eccessivamente ampi a grandi quantità di dati fondamentali e critici".

AppsFlyer ha poi incontrato Polyrize (acquisita da Varonis nel 2020), la cui missione è fornire visibilità e controllo sulle identità e gli accessi. Inizialmente hanno posto una sfida non da poco al team di Polyrize - automatizzare il processo di tracciamento e monitoraggio di tutte le identità e privilegi in tempo reale su più servizi SaaS e IaaS - un processo che fino a quel momento avevano cercato di gestire tramite fogli di calcolo statici e scomodi.

> "Ho chiesto al team di Polyrize di connettersi prima di tutto ad Okta e di comunicarmi in modo proattivo a quali app avessero accesso i vari gruppi, in modo da aiutarmi a capire se il loro accesso fosse appropriato", spiega Flechter. "In seconda battuta, volevo poter identificare le assegnazioni eccessive o errate, di modo che il mio team potesse isolare velocemente i problemi e, se necessario, revocare gli accessi".

Individuare e rispondere agli eventi di sicurezza

Oltre che a rispondere al caso d'uso primario di AppsFlyer, Polyrize (ora DatAdvantage Cloud) ha aggiunto un livello critico di sicurezza reattiva, consentendo a AppsFlyer di individuare e rispondere agli eventi di sicurezza man mano che si verificano. "Polyrize mi ha dato un unico pannello di controllo per tutte le app cloud. Proprio quello che mi serviva", spiega Flechter. "Essere in grado di scoprire le identità rischiose, riuscire ad assegnare gli accessi giusti e identificarne il loro uso improprio sulla stessa piattaforma non solo rende più semplice gestire il processo di sicurezza, ma garantisce anche una protezione aggiuntiva in caso di incidente".

I team di supporto e customer success di Polyrize hanno lavorato fianco a fianco con il team di sicurezza di AppsFlyer per implementare la piattaforma di Polyrize e integrarla nell'infrastruttura e nei processi di sicurezza del loro cloud.

> "Il team di Polyrize è rimasto al nostro fianco durante l'implementazione iniziale e continua a sincronizzarsi con noi per risolvere eventuali problemi durante i controlli periodici, fornendo controlli di sicurezza e visibilità sulla conformità. Ora lo consideriamo un partner di fiducia e parte integrante della nostra strategia di sicurezza cloud."

"Essere in grado di scoprire le identità rischiose, riuscire ad assegnare i corretti accessi e identificarne il loro uso improprio sulla stessa piattaforma non solo semplifica la gestione del processo di sicurezza, ma garantisce anche una protezione aggiuntiva in caso di incidente."

Risultati

"I risultati sono stati sconvolgenti", racconta Flechter. "Attualmente Polyrize (ora DatAdvantage Cloud) ci aiuta a minimizzare la nostra area di rischio scoprendo le identità non utilizzate e le autorizzazioni mal configurate, identifica gli utenti al centro di eventi ad alto rischio e individua, risponde e analizza gli eventi ad alto rischio dopo che si sono verificati. Inoltre, Polyrize (ora Varonis) ha migliorato l'approccio alla sicurezza del nostro cloud, diminuendo i costi del team di sicurezza e il carico della gestione."

"Polyrize (ora DatAdvantage Cloud) ha migliorato l'approccio alla sicurezza del nostro cloud, diminuendo i costi del team di sicurezza e il carico della gestione."

Monitora e identifica le minacce su tutti i cloud store e le app cruciali

RICHIEDI UNA DEMO