Como a AppsFlyer protege identidades em um ambiente 100% na nuvem

Estudo de caso

“Polyrize (agora DatAdvantage Cloud) oferece o painel único que eu precisava para os diferentes aplicativos de nuvem.”

Guy Flechter, CISO e DPO

Este estudo de caso foi originalmente publicado pela Polyrize, que a Varonis adquiriu em 2020.

SAIBA MAIS ›

DESTAQUES

A AppsFlyer, com sede em São Francisco, 18 escritórios no mundo e mais de 1.000 funcionários, é líder global em atribuição. A missão da empresa é permitir que seus clientes (profissionais de marketing e desenvolvedores de aplicativos) meçam suas campanhas de marketing.

CONTESTAÇÕES

- Proteger identidades e permissões entre milhares de identidades e vários locais
- Visibilidade e controle em um ambiente de nuvem complexo
- Impor o acesso com privilégios mínimos

SOLUÇÕES

- **DatAdvantage Cloud** (anteriormente Polyrize) mapeia e analisa os relacionamentos entre usuários e dados em aplicativos e serviços em nuvem isolados

RESULTADOS

- Melhor postura de segurança na nuvem e menores custos
- Capacidade de identificar usuários que protagonizam eventos de alto risco
- Detectar e responder a eventos de alto risco

Contestações

A AppsFlyer dedica-se à sua própria visão como empresa nativa da nuvem, tendo a nuvem como prioridade, e construiu uma rede corporativa na nuvem. Sua infraestrutura de produtos é baseada na AWS, e todos os aplicativos empresariais usados por funcionários e contratados são baseados em SaaS.

O principal desafio de segurança para a organização era então proteger a profusão de identidades e permissões em seu ambiente de nuvem complexo e entre milhares de identidades e vários locais, sobre os quais a equipe de segurança não tinha o nível de visibilidade e controle que teria com uma rede on-premises.

Guy Flechter, CISO e DPO da AppsFlyer comentou: “O maior risco de segurança para o nosso ambiente de nuvem foi a proliferação de identidades humanas e não humanas e suas permissões complexas em muitos serviços de nuvem distintos, o que aumentou muito a nossa superfície de ataque. Portanto, impor o acesso com privilégios mínimos, cortar as permissões não utilizadas e configuradas incorretamente e eliminar identidades não utilizadas em tempo real eram metas vitais para nós.”

> “O maior risco de segurança para o nosso ambiente de nuvem foi a proliferação de identidades humanas e não humanas e suas permissões complexas em muitos serviços de nuvem distintos, o que aumentou muito a nossa superfície de ataque."

Soluções

A AppsFlyer já tinha experiência com uma série de soluções de segurança na nuvem, como a tecnologia de perímetro definido por software, para dar acesso de confiança zero a serviços dentro da produção, e uma solução de Cloud Access Security Broker (CASB). Este último tinha sido descartado antes do trabalho porque, embora o CASB conseguisse detectar vazamentos de dados e outros incidentes, trazia um valor limitado para a segurança devido à falta de informações sobre identidades e privilégios.

“Embora nosso CASB permitisse que víssemos algumas atividades arriscadas dos usuários, ele não nos dava visibilidade sobre os ativos a que os usuários tinham acesso”, explicou Flechter. “Faltava muito contexto e identificar identidades e privilégios arriscados era muito complicado. Veja o exemplo do Salesforce ou da AWS, ele não chegava nem perto de resolver o problema da visibilidade. Ao correlacionar identidades, permissões e atividades, a Polyrize (agora DatAdvantage Cloud) nos permitiu entender quais funcionários e contratados teriam maior impacto em nossa organização, em caso de vazamento de dados ou comprometimento da conta devido a, digamos, permissões excessivamente amplas ou acesso a grandes quantidades de dados vitais da empresa.”

A AppsFlyer trabalhou com a Polyrize (adquirida pela Varonis em 2020), cuja missão é proporcionar visibilidade e controle sobre identidades e acessos. No início, foi um desafio difícil para a equipe da Polyrize automatizar o processo de rastreamento e monitoramento de todas as suas identidades e privilégios em tempo real, em última análise, entre vários serviços SaaS e IaaS. Um processo que eles tinham tentado gerenciar até aquele momento por meio de planilhas estáticas e complicadas.

> “Pedi à equipe da Polyrize que, primeiro e acima de tudo, conectassem ao Okta e me dissessem, de maneira proativa, quais grupos tinham acesso a quais aplicativos para que eu pudesse determinar se aquele acesso era apropriado”, comentou Flechter. “Em segundo lugar, eu queria encontrar tarefas excessivas ou mal configuradas, para que minha equipe pudesse isolar os problemas rapidamente e revogar o acesso, se necessário.”

Detecção e resposta a eventos de segurança

Além de tratar do caso de uso original da AppsFlyer, o Polyrize (agora DatAdvantage Cloud) adicionou uma camada vital de segurança reativa, permitindo que a AppsFlyer detectasse e respondesse aos eventos de segurança durante a ocorrência. “A Polyrize disponibiliza o painel único para os diversos aplicativos de nuvem que eu precisava”, explicou Flechter. “Poder descobrir identidades arriscadas, dimensionar corretamente o acesso e detectar seu uso indevido na mesma plataforma, além de facilitar o gerenciamento do processo de segurança, traz mais proteção quando há algum incidente.”

As equipes de suporte e sucesso do cliente da Polyrize trabalharam em estreita colaboração com a equipe de segurança da AppsFlyer para implementar a plataforma da Polyrize e integrá-la à infraestrutura e aos processos gerais de segurança na nuvem da empresa.

> “A equipe da Polyrize trabalhou em estreita colaboração conosco durante a implementação inicial e mantém o acompanhamento conosco para resolver quaisquer problemas durante as verificações de integridade periódicas, disponibilizando controles de segurança e visibilidade sobre a conformidade”, comentou Flechter, “Agora consideramos a Polaryze uma parceira de confiança e parte da nossa estratégia de segurança na nuvem.”

“Poder descobrir identidades arriscadas, dimensionar corretamente o acesso e detectar seu uso indevido na mesma plataforma, além de facilitar o gerenciamento do processo de segurança, traz mais proteção quando há algum incidente.”

Resultados

“Os resultados foram radicais”, destacou Flechter, “Hoje, a Polyrize (agora DatAdvantage Cloud) me ajuda a minimizar a possibilidade do nosso raio de alcance descobrindo identidades não utilizadas e permissões mal configuradas, identificando os usuários protagonistas dos eventos de alto risco e detectando, respondendo e investigando eventos de alto risco depois que ocorrem. Além disso, a Polyrize (agora Varonis) melhorou a postura da minha segurança na nuvem, reduzindo os custos da minha equipe de segurança e o número de pessoas que atuam no gerenciamento da segurança.”

“A Polyrize (agora DatAdvantage Cloud) melhorou a postura da minha segurança na nuvem, reduzindo os custos da minha equipe de segurança e o número de pessoas que atuam no gerenciamento da segurança.”

Monitore e detecte ameaças em seus principais aplicativos e repositórios na nuvem.

SOLICITAR UMA DEMONSTRAÇÃO