Как AppsFlyer защищает учетные записи в своей облачной среде

ИСТОРИЯ УСПЕХА

«Polyrize (теперь — DatAdvantage Cloud) является единой платформой для различных облачных приложений — именно такой, какая была мне необходима».

Гай Флехтер, директор по информационной безопасности и по защите данных

Данную информацию первоначально опубликовала компания Polyrize, приобретенная Varonis в 2020 году.

УЗНАТЬ БОЛЬШЕ >

КЛЮЧЕВАЯ ИНФОРМАЦИЯ

Компания AppsFlyer, головной офис которой расположен в Сан-Франциско, имеет 18 представительств по всему миру, более 1 000 сотрудников и является мировым лидером в области аналитики и атрибуции. Миссия компании — дать возможность своим клиентам, маркетологам и разработчикам приложений оценивать эффективность своих маркетинговых программ.

ЗАДАЧИ И ОСОБЕННОСТИ ПРОЕКТА

- Защита тысяч учетных записей и прав доступа в разных местоположениях
- Прозрачность и контроль в комплексной облачной среде
- Обеспечение доступа с минимальными привилегиями

РЕШЕНИЕ

- **DatAdvantage Cloud** (ранее — Polyrize) отображает и анализирует связи между пользователями и данными в разрозненных облачных приложениях и сервисах

РЕЗУЛЬТАТЫ

- Безопасность данных в облаке с минимальными затратами
- Способность выявлять пользователей с подозрительной активностью
- Обнаружение событий с высоким риском и реагирование на них

Задачи и особенности проекта

AppsFlyer остается верной своему имиджу компании, ориентированной на облачные технологии, построив корпоративную облачную сеть: ее инфраструктура основана на AWS, а все бизнес-приложения, используемые сотрудниками и подрядчиками, — на SaaS.

Основная задача заключалась в обеспечении безопасности множества цифровых личностей и прав доступа в сложной облачной среде. Из-за тысяч учетных записей в нескольких местоположениях уровень прозрачности и контроля над ними были на порядок ниже по сравнению с локальной сетью.

По словам директора по информационной безопасности и защите данных AppsFlyer Гая Флехтера, «самая большая угроза безопасности для нашей облачной среды заключалась в распространении пользовательских и машинных учетных записей и их сложных прав доступа в различных облачных сервисах, что значительно увеличивало поверхность кибератак. Поэтому ключевой целью для нас было обеспечение доступа на основе модели наименьших привилегий, удаление неиспользуемых и неправильно настроенных прав доступа и удаление неиспользуемых учетных записей в режиме реального времени».

> «Самая большая проблема безопасности для нашей облачной среды заключалась в наличии большого количества пользовательских и машинных учетных записей и их сложных прав доступа в разрозненных облачных сервисах, что значительно увеличивало поверхность для кибератак».

Решение

Компания AppsFlyer уже использовала ряд решений для облачной безопасности, включая технологию программно определяемого периметра для обеспечения доступа к производственным сервисам, использующих принцип «нулевого доверия» и решение Cloud Access Security Broker (CASB). От использования CASB отказались еще до его внедрения, поскольку, несмотря на способность обнаруживать утечку данных и другие инциденты, система была не способна определять учетные записи и сопоставлять их с правами доступа к критичным данным.

«Несмотря на то, что решение CASB позволяло отслеживать некоторые подозрительные действия пользователей, оно не предоставляло сведения о том, к каким объектам пользователи имели доступ», — говорит Флехтер. «Из-за недостаточного контекста отсутствовал порядок в идентификации учетных записей, привилегий и связанных с ними рисков. К примеру, Salesforce или AWS не могли обеспечить прозрачность. Коррелируя учетные записи, права доступа и активность, DatAdvantage Cloud обеспечило понимание того, из-за каких сотрудников и подрядчиков наша организация может больше всего пострадать в случае утечки данных или взлома учетных записей, потому что были предоставлены чрезмерные права доступа к большим объемам критически важных для бизнеса данных».

AppsFlyer использует решение Polyrize (компания была приобретена Varonis в 2020 году) для обеспечения прозрачности и контроля над учетными записями и правами доступа. Изначально перед командой Polyrize стояла сложная задача — автоматизировать процесс отслеживания и контроля всех учетных записей и привилегий в режиме реального времени в нескольких сервисах SaaS и IaaS. До этого компания AppsFlyer управляла данным процессом с помощью громоздких, статических таблиц.

> «Я попросил команду Polyrize в первую очередь подключиться к Okta и оперативно информировать меня о доступе различных групп пользователей к приложениям, чтобы я мог определить, имеют ли они право на такой доступ», — говорит Флехтер. «Во-вторых, я хотел иметь возможность находить излишние или неправильно настроенные права, чтобы моя команда могла быстро изолировать проблемы и при необходимости отозвать доступ».

Обнаружение событий безопасности и реагирование на них

Помимо решения этой задачи, технология Polyrize (теперь — DatAdvantage Cloud) позволила AppsFlyer обнаруживать события безопасности и реагировать на них по мере их возникновения. «Polyrize является единой платформой для различных облачных приложений — именно такой, какая была мне необходима». «Возможность обнаруживать высокорисковые учетные записи, определять правильные объемы доступа и выявлять неправомерное их использование в рамках единой платформы не только упрощает управление процессом безопасности, но и обеспечивает дополнительную уверенность при возникновении инцидентов».

Службы поддержки и клиентского сервиса компании Polyrize тесно сотрудничали со службой безопасности AppsFlyer для внедрения платформы Polyrize и ее интеграции в общую инфраструктуру и процессы облачной безопасности.

> «Команда Polyrize тесно сотрудничала с нами на протяжении всего первоначального внедрения и продолжает регулярно содействовать нам в решении любых проблем во время периодических проверок работоспособности, обеспечивая контроль безопасности и прозрачность», — утверждает Флехтер. «Сегодня мы считаем Polyrize нашим надежным партнером и неотъемлемой частью стратегии облачной безопасности».

«Возможность обнаруживать высокорисковые учетные записи, определять правильные объемы доступа и выявлять неправомерное их использование в рамках единой платформы не только упрощает управление процессом безопасности, но и обеспечивает дополнительную уверенность при возникновении инцидентов».

Результаты

«Результаты были впечатляющими», — отмечает Флехтер. — «Сегодня Polyrize (теперь — DatAdvantage Cloud) помогает минимизировать наш потенциальный радиус поражения за счет обнаружения неиспользуемых учетных записей и неправильно настроенных прав доступа, идентификации пользователей с высоким риском, а также обнаруживать, реагировать и расследовать такие события сразу после их возникновения. В целом, платформа Polyrize (теперь — Varonis) повысила уровень нашей облачной безопасности, снизив затраты на управление безопасностью».

«В целом, платформа Polyrize (теперь — Varonis) повысила уровень нашей облачной безопасности, снизив затраты на управление безопасностью».

Мониторинг и обнаружение угроз в критически важных облачных хранилищах и приложениях.

ЗАПРОС ДЕМОНСТРАЦИИ