Как Varonis помогает трейдерам уверенно перейти на Office 365

ИСТОРИЯ УСПЕХА

«Сочетание возможностей Varonis на уровне аудита и обнаружения угроз в реальном времени открывает огромные возможности для любого директора по информационной безопасности, независимо от бизнеса, вертикали или основной деятельности».

В ЭТОЙ ИСТОРИИ:

Наш клиент — трейдер сырьевых товаров. По его просьбе мы сохраняем все имена и местоположение в тайне.

КЛЮЧЕВЫЕ СВЕДЕНИЯ

ЗАДАЧИ

- Сокращение рисков утечки данных из-за внутренних и внешних угроз
- Миграция в облако Office 365 с максимально возможным уровнем безопасности данных
- Обеспечение соответствия национальным и международным нормативным требованиям

РЕШЕНИЕ

Платформа кибербезопасности Varonis в составе следующих модулей:

- DatAdvantage проверяет, у кого есть доступ и кто имеет доступ к данным в облаке и локально
- Data Classification Engine находит и классифицирует конфиденциальные данные
- DatAlert отслеживает потенциальные внутренние и внешние угрозы и оповещает офицеров безопасности

ПОЛУЧЕННЫЕ РЕЗУЛЬТАТЫ

- Сформировано полное представление об инфраструктуре данных при переходе в облако
- Исправлены ошибки в предоставлении прав доступа к конфиденциальным данным
- Решена задача приведения в соответствие требованиям стандартов в частности, GDPR

Задачи

Проведение всестороннего анализа перед миграцией в облако

Отвечая на вопрос о наиболее распространенных угрозах, с которыми сталкивается современный бизнес, директор по информационной безопасности (CISO) сказал:

> «С облачным хранилищем мы вступили в новую эру, к которой многие еще не готовы. Переход в облако без проведения всестороннего анализа подвергает бизнес риску, и это самая распространенная проблема, которую я вижу».

Многие руководители, принимающие решения, переходят на Office 365, не понимая всех связанных с этим рисков. У них нет базовых средств контроля для ограничения доступа к конфиденциальной информации, включая персональные данные, торговые алгоритмы, стратегии развития, сведения о слияниях и поглощениях.

Если компания не может отследить, где хранятся конфиденциальные данные, кому они принадлежат и у кого есть к ним доступ, у нее нет шанса обнаружить утечки данных до того, как это нанесет серьезный ущерб. При миграции этих данных в облако уязвимость для атак увеличивается в геометрической прогрессии».

> «В обязанности поставщика облачных услуг не входит автоматическое устранение проблем с безопасностью данных. Мы видели множество примеров утечки данных, вызванной печально известными ошибками конфигурации».

В то время как внешние угрозы всегда важны для директора по информационным технологиям, все говорят, что более коварные угрозы часто исходят изнутри.

> «87% утечек данных изнутри не являются злонамеренными — их невольно вызвали пользователи со слишком большим уровнем доступа, бывшие сотрудники, чьи разрешения никогда не отменялись, а иногда причиной были давно не используемые файлы».
>
> «Вредоносные инсайдеры — их не так много. Однако угроза, которую они представляют, является самой разрушительной, особенно, когда нет развернутых средств контроля».

Утечки данных могут привести к катастрофическим последствиям для компаний.
В сегодняшнем цифровом ландшафте бизнеса устаревшие данные и слабые стандарты кибербезопасности могут разрушить бизнес целиком.

> «Штрафы за неспособность защитить конфиденциальность пользователей — совсем не малые. В ЕС штрафы достигают до 4 % от общего дохода вашей компании».

> «Переход в облако без всестороннего анализа подвергает бизнес риску, и это самая распространенная проблема, которую я вижу».

Решение

Аналитика и визуализация данных в облаке и локально

DatAdvantage для Windows и Directory Services: поддержка локальных хранилищ данных трейдеров и защита их электронной почты. В сочетании с механизмом классификации данных Data Classification Engine CISO формирует полное и всестороннее представление о доступе к данным.

Это представление данных имеет огромное значение для руководителей отделов, позволяя им узнать, кто владеет данными и работает с ними. Кроме того, можно автоматизировать изменения в списках управления и группах безопасности.

> «В 99% случаев реакция одинакова — гнев, удивление, крики: "У этого человека не должно быть доступа!" или "Этот человек ушел несколько месяцев назад!". С помощью Varonis я могу визуализировать все наши риски на одном экране».

После завершения миграции в Office 365 заказчик расширил использование облачных приложений, добавив OneDrive.

> «С расширением облачных операций становится все более важным формировать представление о том, что происходит в облаке».

Для бизнеса с филиалами по всему миру необходимость такого полного представления о своей облачной среде даже не подлежит обсуждению, особенно с учетом большого числа требований от различных регулирующих органов.

Пакет Varonis Policy Pack расширяет возможности Data Classification Engine и упрощает соблюдение нормативных требований. Сотни готовых шаблонов помогают быстро и точно обнаруживать защищаемые данные.

> «Поскольку требования регулирующих органов постоянно меняются, не всегда возможно оперативно отслеживать эти изменения. Varonis делает это за нас с помощью готовой классификации данных».

Еще одно решение, которое внедрил заказчик, — DatAlert, которое связывает все модули воедино. Непрерывный мониторинг локальных и облачных систем позволяет директорам по информационной безопасности оценивать области повышенного риска и заблаговременно устранять потенциальные угрозы до того, как они приведут к реальному ущербу.

> «Varonis позволяет настраивать оповещения на основе преднастроенных моделей угроз. DatAlert - ключевое для нас решение, которое мы используем, чтобы связать оповещения с субъектом и типом данных, к которым злоумышленники пытаются получить доступ. По сути, это дает нам детальный снимок всего, что происходит в нашей сети, и позволяет получить более подробные сведения об инциденте».

«Поскольку требования регулирующих органов постоянно меняются, не всегда возможно оперативно отслеживать эти изменения. Varonis делает это за нас с помощью готовой классификации данных».

Полученные результаты

Успешная миграция в облако и соответствие нормативным требованиям

С помощью Varonis заказчик смог определить владельцев данных, а затем обозначить степень важности конфиденциальных данных. После этого решен вопрос с избыточными правами доступа.

> «Сочетание возможностей Varonis на уровне аудита и превентивного обнаружения угроз предоставляет множество сценариев использования для службы информационной безопасности, независимо от бизнеса, вертикали или основной деятельности».

Высокоуровневое представление о состоянии хранилищ данных компании, средствах контроля доступа и областях риска, которое дает Varonis, позволяет уверенно расширять использование Office 365 в компании.

> «Без Varonis каждое решение является реактивным — инструменты Microsoft не обеспечивают такой же полноты представления данных. С помощью Varonis мы можем принимать стратегические решения и заблаговременно защищать наши данные».

С Varonis директор по информационной безопасности также может быть уверен в том, что компания не нарушает требований регулирующих органов, даже когда эти требования неожиданно меняются.

Компания использует Varonis для соблюдения различных государственных и международных нормативных актов, в том числе Общий регламент по защите данных (GDPR) и требования Агентства Европейского союза по кибербезопасности (ENISA).

И поскольку они также работают в ЕС, им нужно соблюдать международные нормативы, такие как Общий регламент по защите данных (GDPR) и требования Европейского агентства по сетевой и информационной безопасности (ENISA).

«Требования регуляторов постоянно обновляются и сложно отслеживать их актуальность. Если вы получаете запрос на доступ к субъекту данных, вы должны иметь возможность быстро получить эти данные. Вы не можете сделать это с помощью поиска в браузере — для этого вам нужно такое решение, как Varonis».

«С помощью Varonis мы можем принимать стратегические решения и заблаговременно защищать наши данные».

VARONIS

Уверенная миграция в Office 365

Varonis показывает, где хранятся конфиденциальные данные, к каким данным и где открыт слишком широкий доступ, а также указывает на риски нарушения нормативных требований.

ЗАПРОСИТЬ ДЕМОВЕРСИЮ