Varonis защищает строительную компанию от трудно обнаруживаемых киберугроз

ИСТОРИЯ УСПЕХА

> Varonis Edge было **единственным решением,** способным обнаруживать угрозы, использующие DNS-туннелирование. **Ни один другой продукт не смог это обнаружить**.
>
> **СПЕЦИАЛИСТ ПО БЕЗОПАСНОСТИ**

В ЭТОЙ ИСТОРИИ

Наш клиент — строительная компания. По его просьбе мы сохраним всю конфиденциальную информацию анонимной, включая название компании и другие подробности.

КЛЮЧЕВЫЕ СВЕДЕНИЯ

ЗАДАЧИ

- Мониторинг целостности файлов во время перехода на новую облачную платформу для обмена файлами
- Защита конфиденциальной информации локально и в облаке
- Обнаружение потенциально разрушительных кибератак и утечек данных, использующих DNS-туннелирование и другие методы

РЕШЕНИЕ

Платформа кибербезопасности Varonis в составе следующих модулей:

- **DatAdvantage** для Windows и Exchange Online
- **Data Classification Engine** для Windows и SharePoint
- **DataPrivilege** для управления доступом к данным
- **DatAlert** для обнаружения потенциальных вредоносных программ или внутренних утечек данных
- **Edge** для обнаружения малозаметных признаков атаки на периметр сети

ПОЛУЧЕННЫЕ РЕЗУЛЬТАТЫ

- Защита от атак через DNS-туннелирование
- Простой и понятный пользовательский интерфейс, упрощающий обнаружение и предотвращение угроз
- Первоклассная поддержка клиентов
- Постоянные обновления и дополнительные модули для защиты данных заказчика

Почему выбирают Varonis

ЗАЩИТА ЛОКАЛЬНЫХ И ОБЛАЧНЫХ ФАЙЛОВ

В задачи департамента по информационной безопасности нашего заказчика, одной из крупнейших строительных компаний, входит защита компании от хакеров, постоянное улучшение системы обнаружения и отражения угроз и управление защитными приложениями, такими как Varonis.

Первое внедрение Varonis было реализовано в 2015 году. До этого заказчик внедрил программу Box для облачного обмена файлами, поэтому ему была нужна возможность блокировать разрешения и контролировать локальное и облачное хранение данных.

> “Изначально мы приобрели Varonis, потому что DatAdvantage помог нам составить картину доступа к данным, Data Classification Engine показал нам зоны риска для конфиденциальных данных, а модуль DataPrivilege помог нам назначить владельцев данных для крупных файловых ресурсов.
>
> Когда дело дошло до мониторинга целостности файлов, нам пришлось обратиться к Varonis. Остальные решения либо устарели, либо не выполняли свою работу, либо сильно ухудшали производительность.”

После того как компания начала сталкиваться с киберугрозами, было решено внедрить еще один продукт Varonis — DatAlert, чтобы справляться с ними и укреплять киберзащиту.

> DatAlert уведомляет, когда что-то требует пристального внимания. Оповещения могут сообщать о присутствии хакерских инструментов для подготовки вторжений, о файлах, зашифрованных вирусом CryptoLocker, или даже о том, что кто-то загружает необычный объем данных.

> Когда дело дошло до мониторинга целостности файлов, нам пришлось обратиться к Varonis. Остальные решения либо устарели, либо не выполняли свою работу, либо сильно ухудшали производительность.

Задача

ЗАЩИТА ОТ КИБЕРУГРОЗ, ОБХОДЯЩИХ ТРАДИЦИОННЫЕ СРЕДСТВА ЗАЩИТЫ

Как насчет угроз, которые особенно трудно обнаружить? DNS-туннелирование — это метод, который хакеры используют, чтобы не привлекать внимания, маскируя кражу данных под обычный веб-трафик.

Поскольку эту угрозу сложно обнаружить, ее часто не замечают. Но ее игнорирование уже стоило компаниям по всему миру миллионы долларов.

Например, DNS-атака в 2016 году скомпрометировала всю DNS-инфраструктуру крупного бразильского банка, включая корпоративную электронную почту и все 36 его доменов. Хакерам удалось перехватить все данные, от интернет-банкинга до мобильных операций, торговых точек, банкоматов и инвестиционных транзакций. От атаки пострадали тысячи, если не миллионы клиентов банка.

И банк был лишь одним из десяти компаний, пострадавших от этой DNS-атаки.

> “Каждая компания, у которой есть домен, использует DNS-серверы, и эти серверы имеют DNS-систему, открытую для всего мира. Обычно вы не можете использовать порт 53 из вашей сети вовне, но, если вы туннелируете его через DNS-серверы, это будет выглядеть вполне легитимно.”

Решение

ЗАЩИТА ДАННЫХ ОТ ПРАКТИЧЕСКИ НЕВИДИМЫХ УГРОЗ

Edge — один из новейших продуктов Varonis. Анализируя метаданные с периметра сети (DNS, VPN и веб-прокси), а также действия при доступе к данным, он помогает обнаруживать и блокировать даже самые незаметные вредоносные программы, таргетированные атаки и попытки кражи данных.

Сотрудники департамента информационной безопасности использовали эксфильтрацию DNS, смоделировав атаку через DNS-туннелирование, а затем «прогнали» через эту мясорубку все тестируемые решения.

> Я использовал инструмент под названием DNScat2 для имитации DNS-туннелирования через наши общедоступные и внутренние DNS-серверы, чтобы посмотреть, насколько это может быть опасно.
>
> **Varonis Edge был единственным продуктом, способным обнаруживать угрозы, использующие DNS-туннелирование. Ни один другой продукт не смог это обнаружить.** Некоторые из них могли собирать события DNS, но они не оповестили о потенциальной угрозе, как это сделал продукт Varonis.
>
> (Специалист по информационной безопасности)

Несмотря на то что компания инвестировала миллионы в кибербезопасность, Varonis Edge был единственным продуктом, который обнаружил DNS-туннелирование. Реальное тестирование позволило легко убедить руководство в необходимости использовать Varonis.

> Когда я хочу решить проблему или протестировать новый продукт, служба поддержки Varonis всегда на высоте, — говорит представитель заказчика. —
>
> Три года назад мы столкнулись с проблемой, и Varonis сразу пришел на помощь. Сотрудник компании работал над проблемой по 10 часов в день, пока она не была решена. Я не знаю другую компанию, которая предлагает такой же уровень обслуживания.

Хотя Varonis не единственная компания, предлагающая классификацию данных или мониторинг целостности файлов, заказчик отмечает, что только Varonis предлагает такой уровень детальной отчетности и комплексную защиту конфиденциальных данных.

> Varonis выходит за рамки контроля целостности файлов. Большинство платформ могут сказать вам, где произошло событие. Но только Varonis предоставит полную информацию о корреляции данных и единый журнал аудита событий, который точно показывает, что происходит, в том числе и в облаке.

> Varonis Edge был единственным продуктом, способным обнаруживать угрозы, использующие DNS-туннелирование. Ни один другой продукт не смог это обнаружить.

Полученные результаты

ЭКОНОМИЯ ВРЕМЕНИ И НАДЕЖНАЯ ЗАЩИТА ДАННЫХ

Заказчик много лет сотрудничает с Varonis и видит, какой путь прошла компания.

> В 2015 году мы получили решение Varonis, но потратили много времени, чтобы его освоить. Сейчас все иначе. Решение легко использовать, и оно предоставляет данные в реальном времени.

> В течение одной минуты я могу, кликнув на оповещение от Varonis, просмотреть всю аналитику по событию. Я вижу каждый файл, к которому пользователь получил доступ, как на уровне сервера, так и в облаке. Я могу увидеть, произошло ли это в нерабочее время, должен ли этот пользователь иметь доступ к этому файлу, загрузил ли он что-нибудь подозрительное или были ли какие-то другие аномалии.
>
> Если бы я пытался сделать все это с помощью нескольких инструментов, мне потребовалось бы гораздо больше времени, чтобы найти все журналы, собрать их вместе, сопоставить всё и убедиться, что все данные корректны. Varonis позволяет мне делать все это быстро и в одном месте. Это сэкономило нам кучу времени.

Технические усовершенствования и дополнительные функции, которые компания Varonis внедряла на протяжении многих лет, сделали использование их решений проще, а защиту конфиденциальных данных надежнее. Varonis Edge не пропустит даже самые трудно обнаруживаемые угрозы, такие как атаки через DNS.

> Когда дело доходит до классификации данных, мониторинга файлов и прав доступа, объединения всех этих данных воедино, вкупе с удобством использования, никакое другое решение не сравнится с Varonis.
>
> Я знаю всех основных игроков рынка, и никто другой не даст вам такого же уровня детализации, производительности и широты дополнительной информации.

“

Когда дело доходит до классификации данных, мониторинга файлов и прав доступа, объединения всех этих данных воедино, вкупе с удобством использования, никакое другое решение не сравнится с Varonis.

Не оставляйте ни одну угрозу безопасности незамеченной

Varonis обнаружит потенциальные угрозы до того, как они перерастут в серьезные проблемы.

ЗАПРОСИТЬ ДЕМОВЕРСИЮ