VARONIS

WHITEPAPER

Как Varonis помогает бороться с внутренними угрозами

Содержание

Обзор 3

1. Быстрое обнаружение и реагирование 10

2. Безопасное хранение данных 11

3. Полная очистка данных 12

Заключение 13

Получить персональную оценку рисков 17

Обзор

Внутренние угрозы, наряду с внешними, остаются краеугольным камнем обеспечения безопасности корпоративных данных. Varonis призывает обратить внимание на 3 ключевых момента в обеспечении безопасности данных, которые помогут вам построить работающую систему обнаружения и предотвращения внутренних угроз.

Во-первых, при обращении пользователей к данным необходимо понимать, какие виды данных они используют, сколько, когда и с каких устройств. Точно так же, как банк, выпустивший кредитную карту, создает профиль ваших привычных трат, чтобы на их фоне выявлять кражу средств, система автоматически выстраивает профиль привычных обращений с данными и использует его для обнаружения признаков злоупотребления правами доступа.

Во-вторых, для чего сотрудникам вообще нужно предоставлять такие широкие права доступа? Оценка рисков показывает, что в среднем 20 % ресурсов открыты каждому сотруднику или подрядчику по ошибке. Большая часть этих данных является конфиденциальной: почти в половине организаций не менее 1000 файлов с конфиденциальной информацией открыты для всех сотрудников. При этом один-единственный файл с уязвимыми данными, оказавшись в руках злоумышленника, может нанести ощутимый финансовый и репутационный урон организации. Задайте себе вопрос, зачем предоставлять сотрудникам больше прав доступа к данным, чем это необходимо, особенно учитывая, что существует возможность этого избежать?

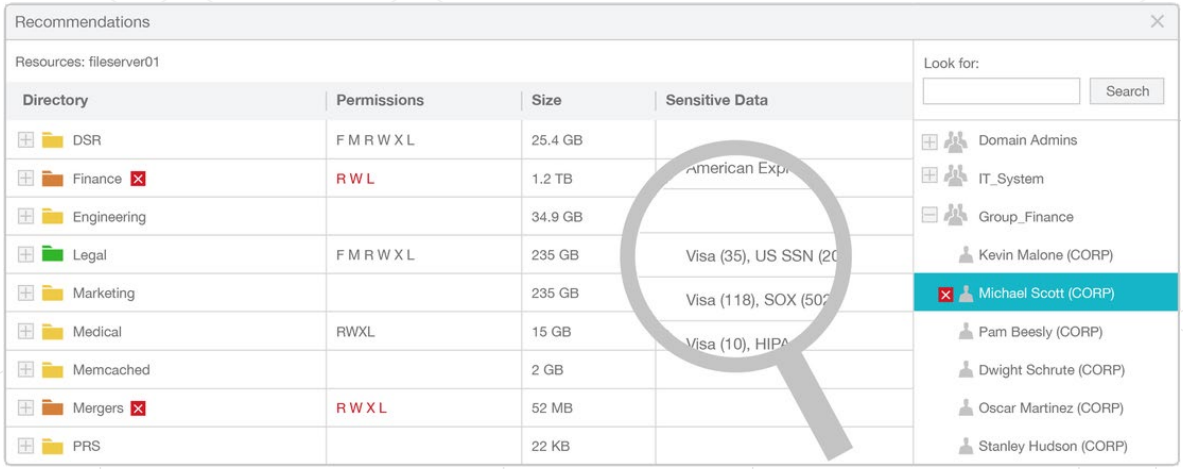
В-третьих, у данных есть свой срок хранения, но зачастую они хранятся намного дольше, чем нужно. В среднем 71 % данных не используется несколько месяцев или даже лет. Устаревшие данные не приносят особой пользы, но повышают риск утечки и занимают дисковое пространство, использование которого также необходимо оплачивать. Для решения этой проблемы достаточно своевременно выявлять устаревшие данные в уязвимых местоположениях и перемещать их в архив.

Вот как Varonis помогает решить каждую из этих трех задач. ▶

1 Быстрое обнаружение и реагирование

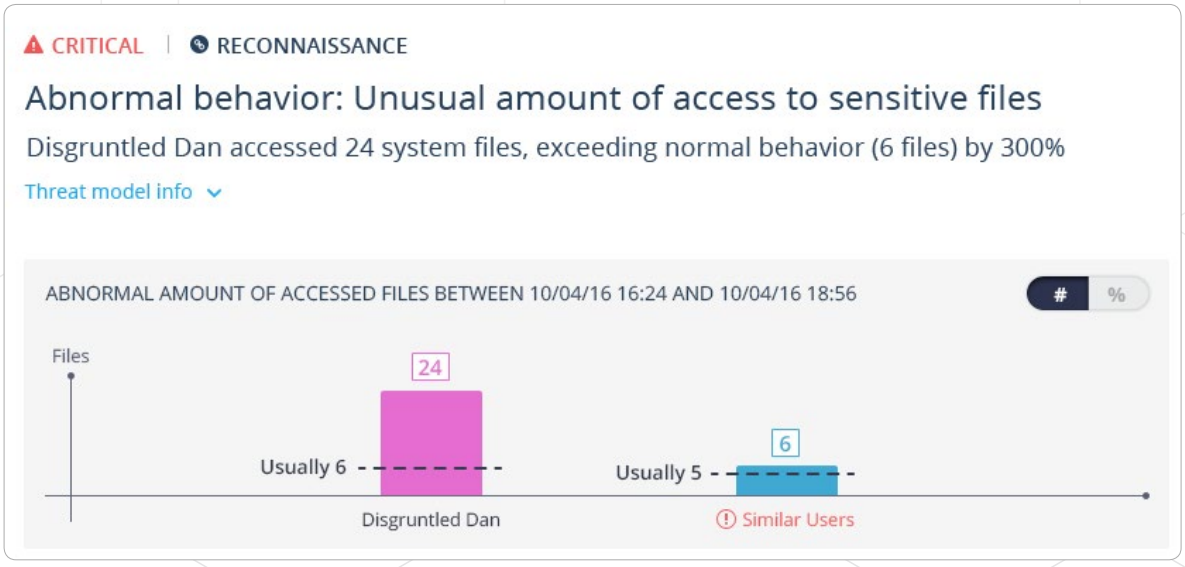
Решение Varonis DatAdvantage собирает больше информации о том, как пользователи взаимодействуют с данными, чем любая другая технология. Оно анализирует активность файловой системы на платформах, проводящих аудит на основе API, например Netapp, EMC, Office365, и с помощью фильтров файловой системы собирает метаданные для платформ без собственной системы аудита, таких как Windows, Unix, Exchange и SharePoint.

Varonis DatAdvantage также собирает информацию о критических событиях Active Directory, таких как вход в систему и внесение изменений в группы, а Varonis Edge получает телеметрию с DNS-серверов, веб-прокси и VPN-концентраторов. DatAdvantage также собирает информацию из списков разрешений и контроля доступа и с помощью механизма классификации данных сканирует файлы на предмет содержания конфиденциальной информации, такой как персональные данные, медицинские записи и финансовая информация.



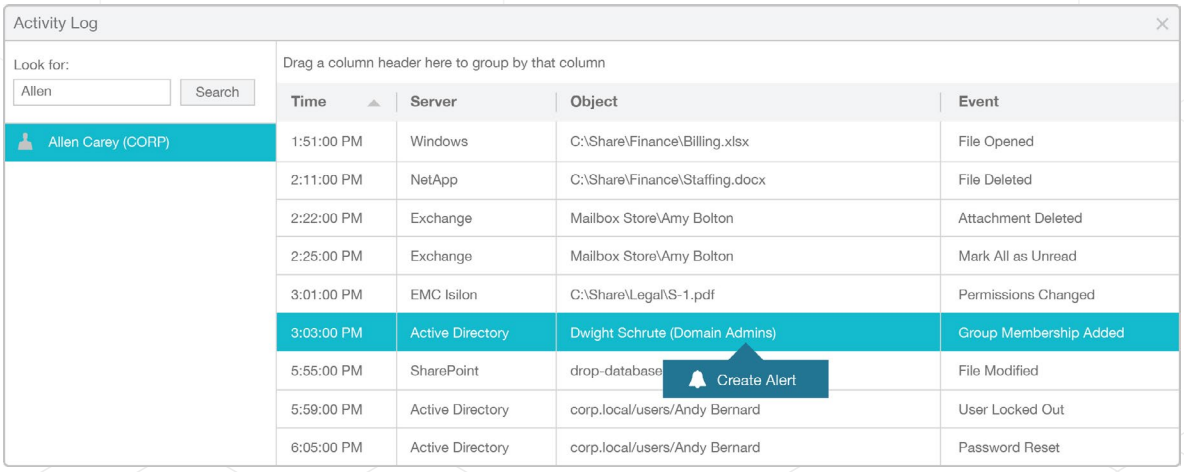
Varonis DatAlert анализирует всю описанную активность, права доступа и контент конфиденциальных файлов, выявляет учетные записи руководителей, администраторов, служебные учетные записи, а также поведенческие профили сотрудников. Когда решение DatAlert обнаруживает значимое отклонение от привычного поведения, оно сигнализирует о возможной атаке и даже может автоматически принимать меры противодействия.

Например, если пользователь ежедневно обращался к небольшой группе уязвимых файлов, а однажды внезапно использовал их сразу в большом количестве, система отправит об этом оповещение. Если пользователь, как правило, использует небольшое количество устаревших данных, а потом вдруг на протяжении недели обращается к соизмеримо большему набору данных, также будет отправлено оповещение. Если сетевой администратор обычно не читает электронную почту руководителя, а затем начинает ее читать и помечает сообщения как непрочитанные, DatAlert отследит это. DatAlert содержит более 150 встроенных моделей угроз и выявляет непривычные модели доступа, анализируя поведение пользователей.



В некоторых моделях угроз, например, по выявлению программ-вымогателей, которые внедряются в систему через конечную точку и начинают шифровать файлы в доступных файловых системах, наши клиенты используют DatAlert для оповещения ИБ-специалистов, автоматически закрывая скомпрометированные учетные записи еще до того, как они нанесут серьезный ущерб.

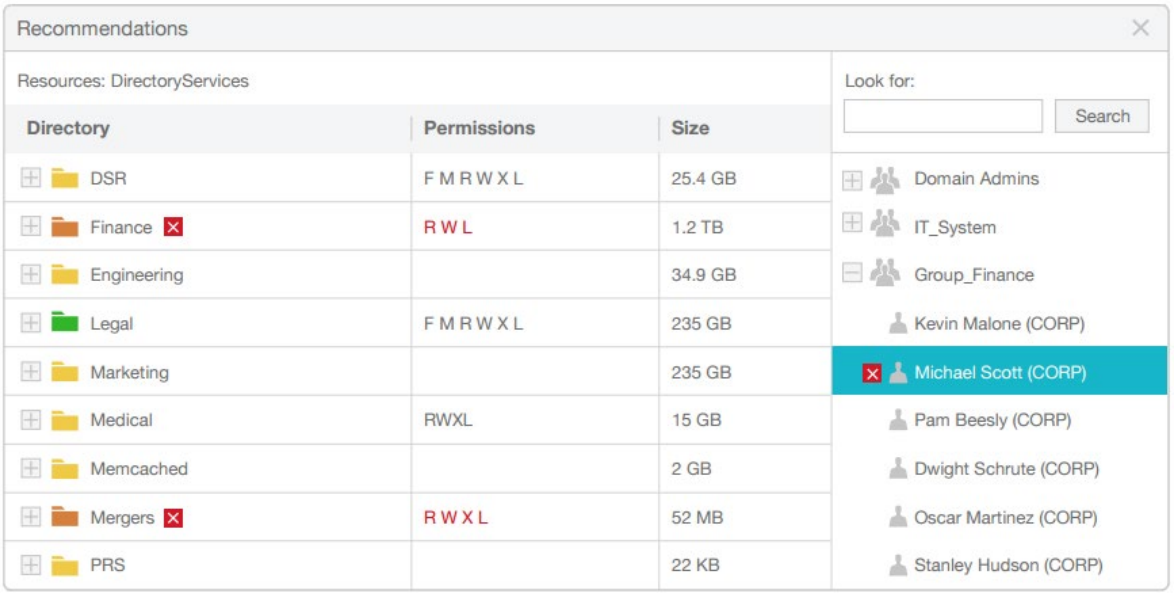
Используя подробный журнал аудита DatAdvantage, можно быстро оценить ущерб. Вместо поиска по журналам или рабочим станциям можно по запросу получить данные о всех действиях доступа любого пользователя за любой период времени и посмотреть все файлы или электронные письма, к которым он обращался, внесенные им изменения и обращения к уязвимым файлам.



2 Безопасное хранение данных

Одно из самых уязвимых мест — общие папки, в которых зачастую хранится в 10–1000 раз больше данных, чем на ноутбуке или рабочей станции. Результаты пилотных проектов Varonis подтверждают, что 20 % всех папок в общем доступе открыты вообще для всех сотрудников. Так один злонамеренный пользователь может украсть 20% конфиденциальных данных компании, просто скопировав их на диск.

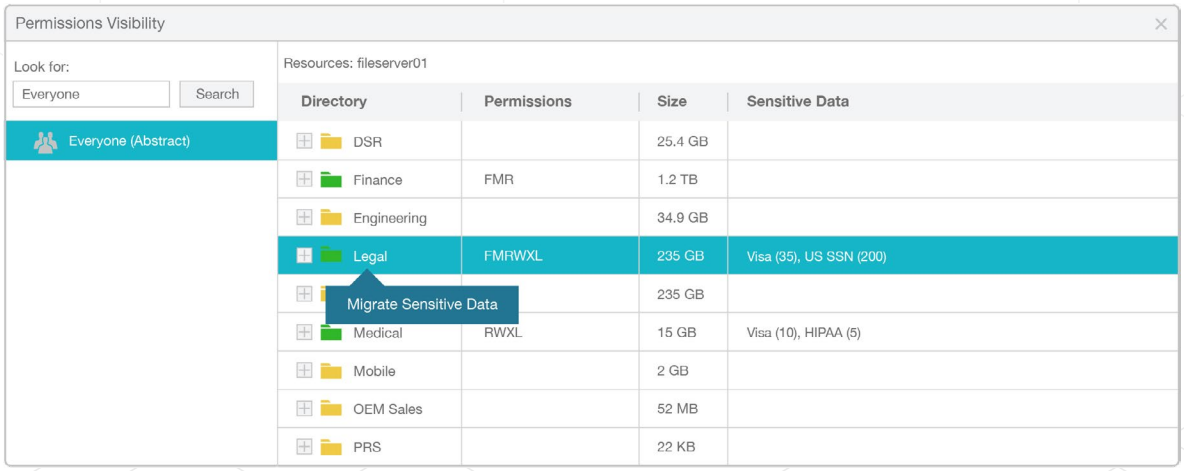
Varonis DatAdvantage анализирует разрешения файловой системы, взаимодействия пользователей и групп и их активность, выявляя места хранения конфиденциальных файлов, доступ к которым открыт всем сотрудникам. (например, доступ может быть открыт всем аутентифицированным пользователям и пользователям домена), сбои конфигурации разрешений и пользователей, состоящих в слишком большом количестве групп. DatAdvantage также предоставляет возможность моделировать и проверять в тестовой среде ограничения доступа, а затем безопасно применять их в рабочей среде. Механизм классификации данных Varonis помогает расставлять приоритеты при восстановлении данных, выявляя конфиденциальную информацию, а механизм автоматизации Varonis позволяет безопасно отключать глобальные группы доступа сразу от целого ресурса или сервера — всё это в автоматическом режиме. Не имея доступа к данным, злоумышленник не сможет нанести большого ущерба.



3 Полная очистка данных

Varonis автоматизирует архивирование и очистку данных. Конфиденциальные данные, открытые для всех сотрудников, можно заблокировать или поместить в карантин. Некоммерческие данные можно полностью удалить. Данные, которые долгое время не использовались, можно переместить в менее дорогостоящее хранилище и ограничить к ним доступ. Подсистема транспортировки данных Varonis Data Transport Engine позволяет вам определять правила идентификации данных в соответствии с критериям их уязвимости и релевантности, перемещать и удалять данные, а также изменять разрешения на доступ сразу к целым хранилищам данных и доменам.

Сокращая количество устаревших и конфиденциальных данных в открытом доступе, вы уменьшаете объем ущерба, который может нанести злоумышленник.



Заключение

Сочетая сложную аналитику с анализом контента и управлением правами доступа, Varonis обеспечивает защиту от внутренних угроз и предлагает их быстрое обнаружение, оптимизированный контроль доступа и применение политик на основе широкого контекста данных. Помимо внутренних угроз, Varonis также защищает организации от вредоносных программ, хакерских атак и кражи учетных записей, используя поведенческий анализ, мониторинг прав доступа, классификацию данных, хранящихся на файловых и почтовых серверах — локально и в облаке.

> Varonis — просто фантастическое решение

Gartner peerinsights™

DatAlert — самое популярное решение для анализа поведения пользователей и сущностей (UEBA)

Данные платформы Gartner Peer Insights.

Читайте о результатах клиентов →

О КОМПАНИИ VARONIS

Varonis — пионер в области защиты данных и аналитики. Компания специализируется на разработке ПО для защиты и контроля данных, обеспечения соответствия, классификации и аналитики. Varonis обнаруживает внутренние угрозы и кибератаки, анализируя файловую активность и поведение пользователей, предотвращает ущерб, блокируя попытки кражи конфиденциальных данных, эффективно поддерживает безопасную работу с помощью средств автоматизации.

Мы помогаем тысячам клиентов предотвращать утечки данных.

NASA ING Nasdaq CHAMPAGNE BOLLINGER MAISON FONDÉE EN 1829 DELL EMC

TOYOTA LUXEMBOURG INSTITUTE OF HEALTH RESEARCH DEDICATED TO LIFE L'ORÉAL

Получите персональную оценку рисков

Оценка рисков кибербезопасности

Закажите аудит рисков, определите существующие уязвимости и устраните проблемы безопасности, представляющие реальную угрозу.

Заказать бесплатную оценку

https://info.varonis.com/risk-assessment/ru

Онлайн-демонстрация

Узнайте, как защитить данные и выявлять кибератаки на любом этапе killchain.

Заказать персональную демонстрацию

https://info.varonis.com/demo/ru

VARONIS