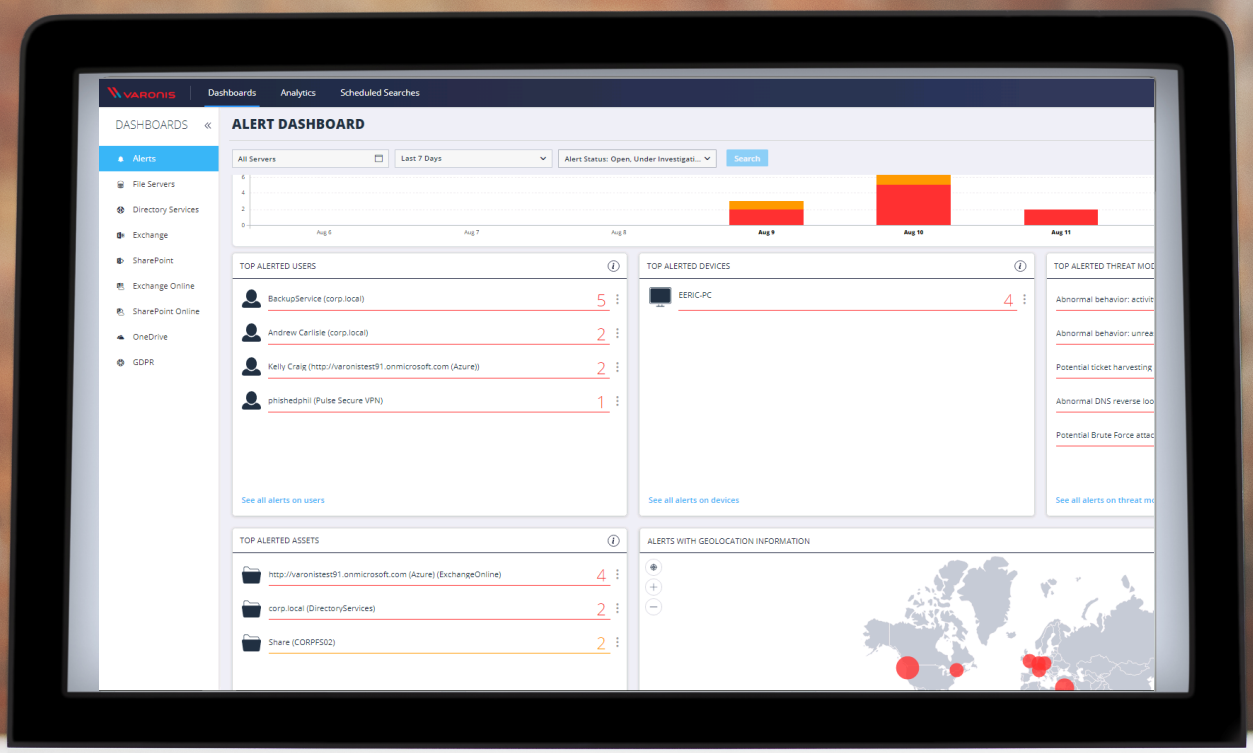


РЕШЕНИЯ VARONIS ДЛЯ ЗАЩИТЫ ОТ ВИРУСОВ-ВЫМОГАТЕЛЕЙ

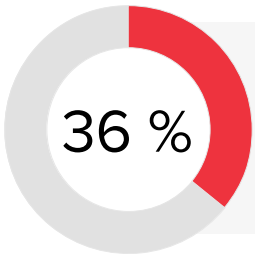
Мощные инструменты для предотвращения продвинутых кибератак и борьбы с внутренними угрозами

Varonis полностью защищает нашу организацию: контролирует состояние инфраструктуры, Active Directory, а также всего оборудования и программного обеспечения. С помощью Varonis мы отслеживаем текущие процессы и производим мониторинг внешних угроз. Благодаря Varonis нам удалось выявить и обезвредить вирус-вымогатель в течение 10 минут.

Уэйд Сендал (Wade Sendall) | Вице-президент по ИТ, Boston Globe

The Boston Globe

РЕШЕНИЯ ДЛЯ ЗАЩИТЫ ОТ ВИРУСОВ-ВЫМОГАТЕЛЕЙ



36% заказчиков Varonis обнаружили вирусы-вымогатели с помощью решения DatAlert

Принцип работы

Varonis выявляет вирусы-вымогатели в основных ИТ-системах, где хранятся терабайты важнейших данных: на файловых серверах, устройствах NAS, облачных хранилищах, — и обезвреживает их прежде, чем они смогут навредить вашей организации.

Решения Varonis обеспечивают безопасность корпоративных данных в случае атак нулевого дня: они способны остановить программы, которые легко минуют традиционные средства защиты периметра сети.

Обнаружение вирусов-вымогателей

Выявление вредоносных программ, внутренних угроз и кибератак системными средствами.

Отслеживание подозрительных действий пользователей, напоминающих поведение программ-вымогателей, с помощью моделей прогнозирования угроз.

Оповещения и инструменты автоматического реагирования позволяют остановить развитие атаки в режиме реального времени.

Минимизация ущерба

Использование модели доступа с минимальным уровнем привилегий позволяет избежать масштабных последствий для системы при заражении одного пользователя.

Сокращение площади атаки путем определения и блокировки недостаточно защищенных и неправильно настроенных параметров управления доступом, которые могут быть использованы программами-вымогателями и злоумышленниками.

Быстрое восстановление

Беспроблемное восстановление благодаря использованию записей всех зашифрованных объектов.

Расследование подозрительных действий и инцидентов безопасности на базе собираемых данных: файлах, пользователях и устройствах, затронутых атакой.

Преимущества Varonis

- Анализ поведения пользователей на различных платформах, обнаружение подозрительных действий и возможных утечек данных на основе комплексной методологии защиты данных
- Обнаружение недостаточно защищенных конфиденциальных данных и глобальных групп, которые увеличивают число уязвимостей и создают дополнительные точки входа для вирусов-вымогателей
- Определение приоритетов в ходе восстановления: ограничение доступа к конфиденциальным и регулируемым данным, автоматизация процессов на основе модели доступа с минимальным уровнем привилегий и поддержание работоспособности этой модели
- Использование моделей угроз, разработанных специально для противодействия вредоносным программам: обнаружение групп зашифрованных файлов, шаблоны поведения известных вирусов-вымогателей и действия, которые характерны для вредоносных программ, а не реальных пользователей.

Поддерживаемые платформы

Обеспечьте безопасность наиболее ценных данных, где бы они ни находились

РЕШЕНИЯ ДЛЯ ЗАЩИТЫ ОТ ВИРУСОВ-ВЫМОГАТЕЛЕЙ

Тест-драйв

Установите Varonis и оцените его возможности по блокировке вирусов-вымогателей и защите данных.

Заказать тест-драйв

Оценка рисков кибербезопасности

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

Заказать аудит рисков

Нам требовалось надежное средство мониторинга и защиты от программ-вымогателей и атак злоумышленников. Решение DatAlert сочетает в себе все эти возможности. Оно быстро показало себя в деле с наилучшей стороны. Решение Varonis соответствует всем заявленным характеристикам.

Рон Марк (Ron Mark) | Менеджер по инновациям и ИТ-технологиям, Gas Strategies

Мы помогаем тысячам организаций бороться с кибератаками и внутренними угрозами