ОБЗОР РЕШЕНИЯ

Повышение безопасности конечных точек: автоматическая реакция в режиме реального времени

Краткий обзор

С 1 января 2016 года в среднем ежедневно происходит более 4,000 атак с целью вымогательства.

Для поражения конечных точек сложным атакам хватает нескольких минут или даже секунд. Инструменты обнаружения угроз и реакции на конечных точках (EDR) первого поколения уже не отвечают вызовам времени. Они требуют расстановки приоритетов вручную, реагируют слишком медленно и генерируют чересчур много предупреждений. Подобные решения увеличивают стоимость операций по обеспечению безопасности и замедляют реагирование на инциденты, приводят к остановке производства и нарушают работу пользователей системы. FortiEDR устраняет эти недостатки благодаря усовершенствованной защите конечных точек от угроз в режиме реального времени как до, так и после заражения. FortiEDR превентивно уменьшает поверхность атак, предотвращает заражение вредоносными программами, а также обнаруживает и устраняет потенциальные угрозы в режиме реального времени. FortiEDR эффективно борется со взломами и вредоносными программами в автоматическом режиме, оптимизирует операции по обеспечению безопасности, поддерживает пользователей и производственное оборудование в рабочем состоянии

Как работает защита FortiEDR после заражения

Агент FortiEDR на конечной точке борется с заражением, блокируя большинство вредоносных программ.

В случае заражения FortiEDR находит и обезвреживает угрозу в режиме реального времени, чтобы минимизировать ущерб.

Остановив угрозу, FortiEDR запускает реакцию на нее на основании набора сценариев и облачной аналитики.

FortiEDR сохраняет отчёт и снимки памяти для последующего анализа атаки.

Как FortiEDR повышает безопасность конечных точек

FortiEDR — современное высокопроизводительное решение для защиты конечных точек; оно включает широкий набор средств по предотвращению, обнаружению и реагированию и легко развёртывается даже на устройствах с ограниченными системными ресурсами. Среди ключевых возможностей FortiEDR — поиск и минимизирование рисков, антивирус нового поколения (NGAV), выявление на основе поведения, блокирование в режиме реального времени, автоматическое реагирование на инциденты, аналитика, поиск угроз и виртуальная вставка «заплат» (Рисунок 1). FortiEDR использует архитектуру Fortinet Security Fabric и интегрируется с такими компонентами Security Fabric, как FortiGate, FortiNAC, FortiSandbox и FortiSIEM.

Упреждающее снижение рисков

FortiEDR непрерывно ищет неуправляемые устройства и приложения с помощью сборщиков данных, установленных на существующих конечных точках, и обеспечивает командам по обеспечению безопасности полную видимость. Аналитики могут настраивать политики управления коммуникациями на основе рейтинга приложений, уязвимостей и данных об угрозах в реальном времени. Упреждающее снижение рисков сводит к минимуму количество незащищённых конечных точек и уменьшает поверхность атаки.

Защита в режиме реального времени

FortiEDR включает антивирусный модуль на базе технологии машинного обучения для защиты от файловых вредоносных программ. FortiEDR защищает конечные точки, даже если они не подключены к интернету. Благодаря компактности и широкой поддержке операционных систем, FortiEDR можно развернуть на устройствах с ограниченными ресурсами, например, на POS-терминалах, работающих в режиме реального времени, и контроллерах производственных процессов.

Автоматическое обнаружение и блокировка

Для автоматического определения и обезвреживания потенциальных угроз FortiEDR использует систему обнаружения, основанную на анализе поведения. Этот подход особенно эффективен против бесфайловых вредоносных программ, которые легко обходят традиционные антивирусы, прячась в памяти, а не атакуя диск. Бесфайловые угрозы используют реальные системные ресурсы (иначе говоря, "пользуются местными ресурсами") и либо выполняют свои действия исключительно в памяти, либо задают вектор другим атакам, например, программам-вымогателям.

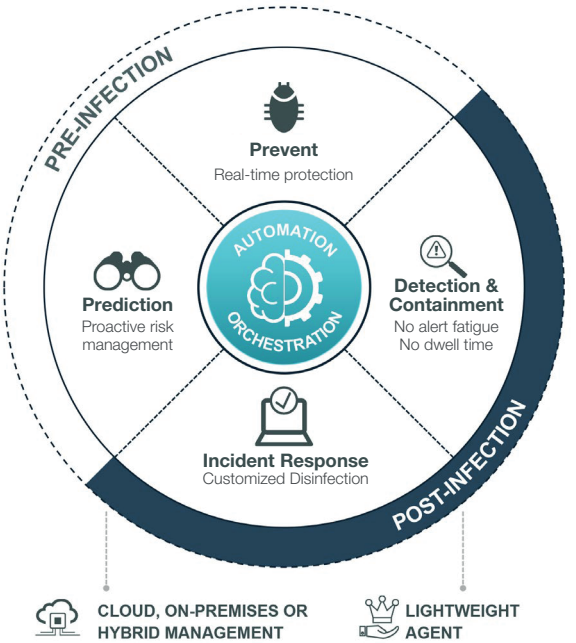

Рисунок 1: FortiEDR — улучшенное средство реагирования и защиты конечных точек как до, так и после заражения.

При выявлении подозрительного поведения FortiEDR немедленно предотвращает атаки, блокируя все запрашиваемые исходящие соединения и доступ к файловой системе. Параллельно с этим серверная часть FortiEDR непрерывно классифицирует угрозы, чтобы предпринять адекватные ответные действия, и устраняет помехи, чтобы оптимизировать анализ безопасности и операции.

Скоординированная реакция на инциденты

FortiEDR включает в себя настраиваемый набор сценариев, которые позволяют координировать автоматическое реагирование и устранение угроз. Типичные автоматизированные стратегии включают в себя прерывание вредоносных процессов, удаление файлов, очистку постоянных данных, откат вредоносных изменений, уведомление пользователей, изоляцию приложений и устройств, создание запросов.

Не все конечные точки одинаково устойчивы к рискам. Например, система контроллеров на производственном участке требует высокой доступности и поэтому обладает более низкой устойчивостью к риску, чем ноутбук сотрудника. Но сценарии защиты позволяют разработать контекстно-ориентированное реагирование на инциденты, которое запускает соответствующие действия на основе классификации угроз и группы конечных точек. Такой подход обеспечивает последовательное реагирование на инциденты, сокращает специалистам по безопасности время на выполнение рутинных задач и помогает организациям привести политики безопасности конечных точек в соответствие с допустимым уровнем риска.

Сбор данных

FortiEDR обладает уникальным управляемым интерфейсом — он отображает критерии, по которым событие признаётся подозрительным и предлагает логичные аналитические меры. Опираясь на доверенные источники — например, на базу данных ATT&CK — FortiEDR автоматически вносит в свою базу подробную информацию о методах атак. Запатентованная технология отслеживания кода позволяет специалистам по безопасности полностью отследить всю цепочку кибератак. Кроме того, для облегчения анализа FortiEDR сохраняет снимки памяти.

Преимущества для бизнеса

FortiEDR представляет значительную ценность для бизнеса в таких областях, как защита конечных точек, реагирование на инциденты, безопасность операций и непрерывность бизнес-процессов.

Защита в режиме реального времени: повышение безопасности

Работая на базе технологии машинного обучения, FortiEDR устраняет нарушения, предотвращает хищения данных, блокирует программы-вымогатели в режиме реального времени, устраняет временной зазор между обнаружением угрозы и реакцией. FortiEDR не только улучшает защиту конечных точек организации, но и минимизирует воздействие угроз, которым удается обойти защитную систему.

Оптимизация защитных процессов

FortiEDR оптимизирует рабочие процессы с помощью настраиваемых стандартизированных процедур реагирования на инциденты. FortiEDR разгружает сотрудников и снижает количество оповещений за счет автоматизации повторяющихся задач и минимизации ложных срабатываний. Автоматическое объединение оповещений, выстраивание взаимосвязи между событиями и понятный график атак позволяют упростить реагирование на инциденты и аналитику.

Непрерывность бизнес-процессов

FortiEDR реагирует и устраняет неполадки в работающих системах — это предотвращает сбои в производстве и сохраняет производительность пользователей. FortiEDR можно развернуть на устаревшем оборудовании с ограниченными системными ресурсами, продлив тем самым срок его службы. С помощью FortiEDR специалисты по безопасности могут откатить вредоносные изменения и избежать дорогостоящего переформатирования системы.

FortiEDR: Обзор функций

Pre-infection		Post-infection			
Выявление и прогнозирование	**Предотвращение**	**Обнаружение**	**Обезвреживание**	**Реагирование и анализ**	**Очистка и откат**
Упреждающее снижение рисков	**Предварительная защита**	**Обнаружение угроз в режиме реального времени**	**Устранение нарушений и потери данных**	**Полная видимость атаки**	**Устранение последствий**
•Выявление подозрительных устройств и устройств IoT •Приложение и репутация •Уязвимости •Политики на основе рисков снижают поверхность атак •Виртуальные заплатки	•На уровне ядра •Машинное обучение, без подписи •Приложение	•Снижение количества оповещений •Классификация вредоносных программ •Отображение контроллера ввода-вывода •Отображение полной цепочки атаки	•Первая и единственная система блокировки после заражения в режиме реального времени •Блокировка исходящих запросов •Предотвращение утечки данных •Предотвращение изменения данных программами-вымогателями	•Настраиваемые сценарии реагирования на инциденты •Устранение временного зазора •Сбор данных для анализа •Снимки памяти в случае безфайловых атак •Удобно настраиваемый поиск угроз	•Откат вредоносных изменений •Удаление плохих файлов •Очистка данных на сервере •Нет необходимости в переустановке •Непрерывность бизнес-процессов •Выход REST API для внешних инструментов по восстановлению

Служба развертывания Fortinet и реагирование на угрозы

- Программа профессионального обслуживания Fortinet оказывает экспертную помощь в планировании архитектуры, конфигурации, настройке сценариев, адаптации под клиента и обучении.
- Управляемая служба выявления и реагирования на угрозы (MDR) FortiResponder обеспечивает круглосуточный мониторинг угроз, сортировку оповещений и удалённое восстановление системы, не беспокоя пользователей.
- Сертифицированные партнёры Fortinet предоставляют услуги управляемой безопасности, в том числе полностью контролируемое разделение обязанностей.

Заключение

Неуклонный рост и усложнение типов атак и программ-вымогателей вынуждает компании укреплять безопасность по всем направлениям, в том числе — защищать конечные точки. FortiEDR предлагает защиту конечных точек следующего поколения, легкую и простую в развертывании систему обнаружения и реагирования на угрозы. FortiEDR повышает защиту конечных точек, а это ускоряет реагирование на инциденты, упрощает процесс обеспечения безопасности и позволяет избежать дорогостоящих перебоев в работе производственных линий и специалистов.

Примеры использования FortiEDR

Защита эксплуатационных технологий

FortiEDR предотвращает, выявляет и обезвреживает угрозы в операционных технологиях (OT)без остановки работы компьютеров и производства. FortiEDR ищет уязвимости и контролирует их устранение (например, с помощью виртуальных заплаток), чтобы система оставалась защищённой до следующего доступного окна обслуживания. За счет своей компактности FortiEDR обеспечивает поддержку устаревших и отключённых от сети устройств, не замедляя их.

Защита систем POS

FortiEDR защищает данные кредитных карт в точках продаж (POS), останавливая атаки на источник. FortiEDR сертифицирован по стандарту безопасности данных индустрии платёжных карт (PCI DSS) и предотвращает утечку данных в случае компрометации системы. FortiEDR обеспечивает виртуальные исправления для защиты POS-систем от уязвимостей. Встроенная поддержка ОС от FortiEDR, благодаря своей компактности, подходит для устаревшего POS-оборудования.

FORTINET

https://www.fortinet.com/ru

February 15, 2020 4:48 AM

580266-0-0-EN

D:\Fortinet\Solution Briefs\purple solution briefs\FortiEDR\sb-boosting-endpoint-security-with-realtime-automated-incident-response-V1.1-2152020-445AM