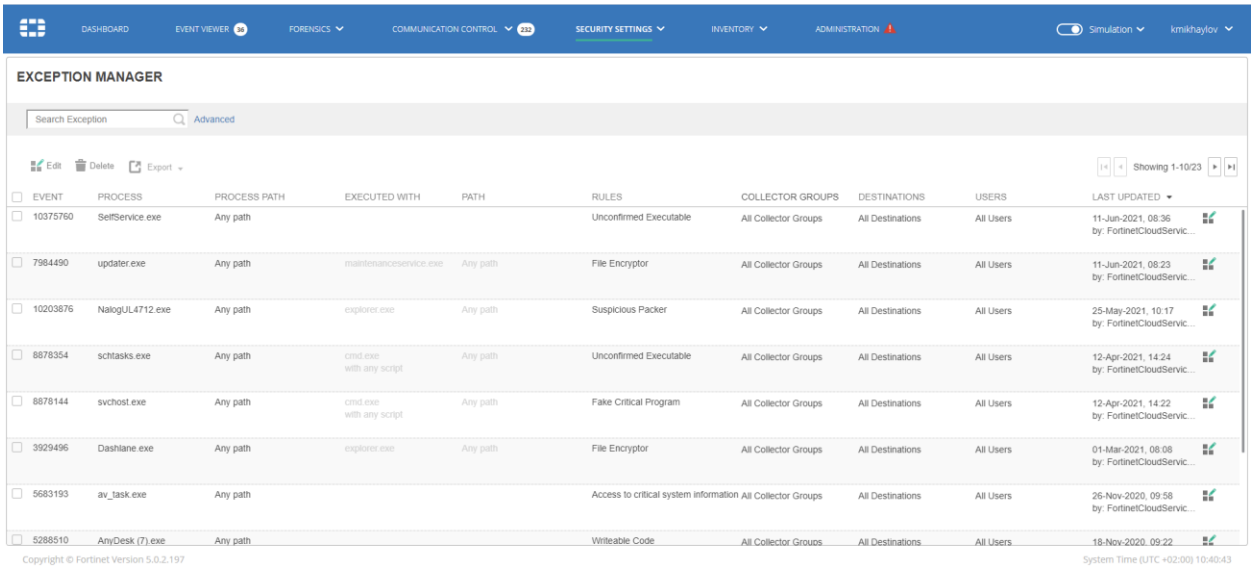
Совместим ли FortiEDR со сторонними защитными решениями?

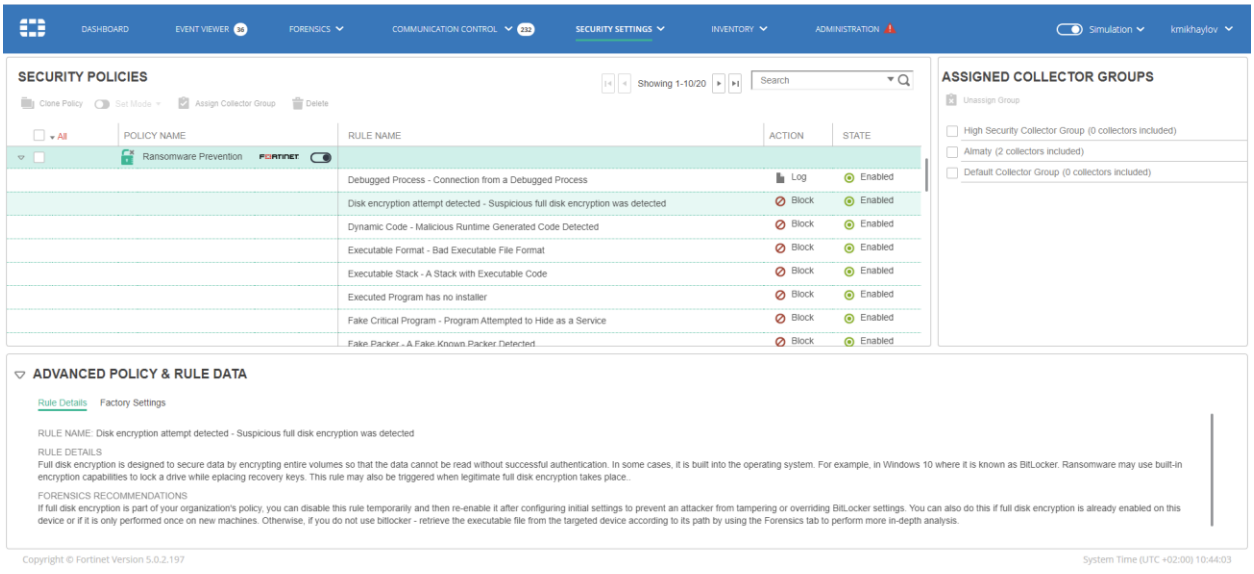
FortiEDR поддерживает гибкую настройку исключений.



В случае необходимости сторонние агенты можно легко добавить в исключения и тем самым решить проблему совместимости.

Может ли FortiEDR защитить от вирусов-вымогателей?

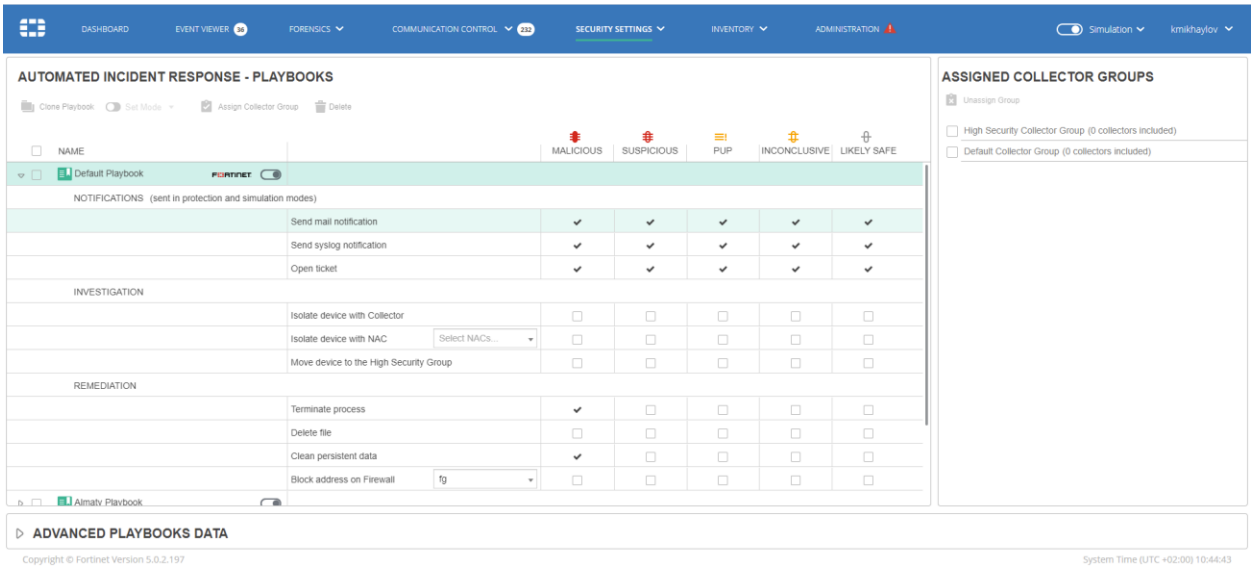
FortiEDR позволяет реализовать комплексную защиту рабочих станций и серверов, в том числе от вирусов-вымогателей. Защита от ransomware реализуется с помощью политик ransomware protection.



С помощью данных политик FortiEDR анализирует поведение процессов на конечном узле и, в случае если действия процесса схожи с действиями характерными для вирусов-вымогателей, блокирует вредоносные действия.

Может ли FortiEDR автоматически реагировать на обнаруженные угрозы?

В FortiEDR реализован функционал автоматизированных политик реагирования на обнаруженные инциденты безопасности – плэйбуки.



С помощью плэйбуков администратор системы может настроить автоматические реагирование на инциденты: остановку процесса, удаление файла, изоляция рабочей станции от сети и др.

Может ли FortiEDR заменить решения EPP (Endpoint Protection), например, FortiClient?

Функционал решений класса EPP (в том числе FortiClient) включает в себя несколько функциональных модулей: модуль антивирусной защиты (чаще всего работает на основе сигнатурных методов и позволяет защитить конечный узел от известных угроз), модуль безопасного удаленного доступа (ztna/vpn), модуль проверки конечных узлов на соответствие корпоративным политикам (compliance).

Функционал же FortiEDR включает в себя модули обнаружения и блокировки угроз (основанные как на сигнатурных методах обнаружения, так и на поведенческом анализе), модуль реагорования на обнаруженные инциденты, а также вспомогательные модули обнаружения подключаемых к сети IOT/неуправляемых устройств, виртуального патчинга.

В сухом остатке для защиты от простейших угроз (по сути фильтрации), а также для построения безопасного удаленного доступа и контроля устройств используется FortiClient, в то время как FortiEDR позволяет защититься от более сложных, комплексных угроз.

Отсюда мы можем сделать вывод, что FortiEDR и FortiClient функционально дополняют друг друга.

Какие версии ОС поддерживает FortiEDR?

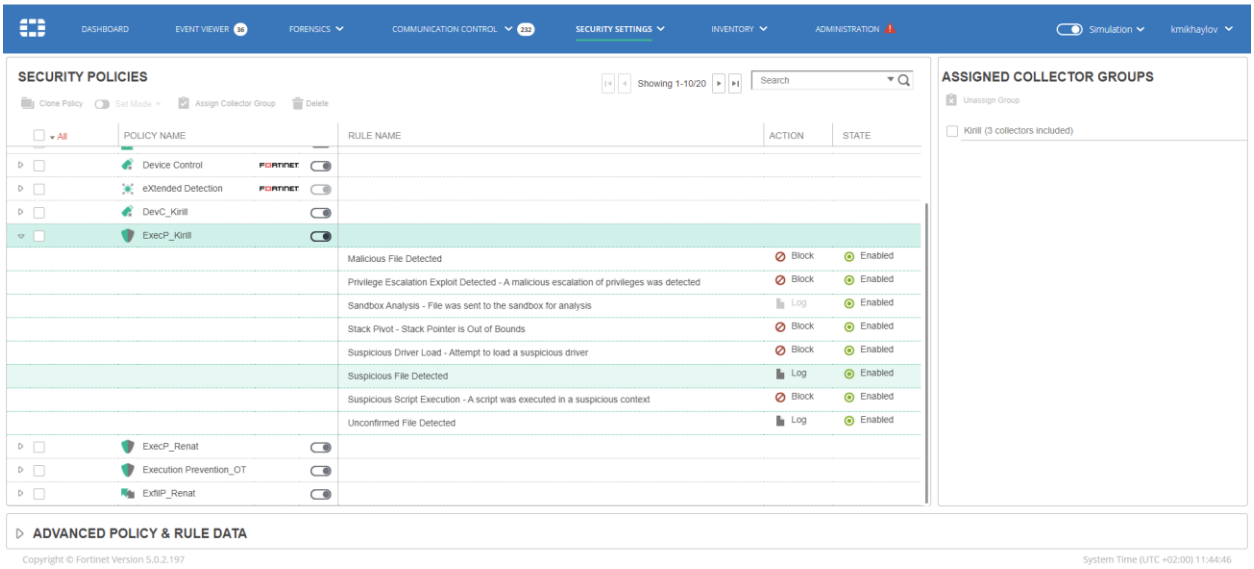
FortiEDR поддерживает три типа ОС: Windows, Linux, MacOS. Если говорить о Windows – FortiEDR поддерживает как современные версии, так и старые, начиная с Windows XP и Windows Server 2003 R2. Полный список поддерживаемых ОС доступен на портале документации: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/0b972a70-7201-11eb-9995-00505692583a/FortiEDR_Installation_and_Administration_Guide_V5.0.pdf

Сколько ресурсов требует агент FortiEDR? Не будет ли конечный узел перегружен?

Агент FortiEDR является легким агентом. Для работы ему требуется около 60 MB RAM, 200 MB на жестком диске. Системные требования для компонентов FortiEDR доступны на портале документации: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/0b972a70-7201-11eb-9995-00505692583a/FortiEDR_Installation_and_Administration_Guide_V5.0.pdf

Указано, что FortiEDR может быть установлен на серверные ОС. Какова вероятность, что агент своими действиями нарушит работоспособность сервера?

FortiEDR поддерживает два режима работы – логирование и блокировка. В режиме логирования FortiEDR создает нотификацию, но не блокирует обнаруженные действия. Также FortiEDR позволяет применять различные политики для разных групп устройств.



Таким образом FortiEDR позволяет настроить политики обнаружения в режиме логирования на критичных для бизнеса устройствах, но для пользовательских устройств назначить более строгие политики в режиме блокировки.

Поддерживает ли FortiEDR API?

Да, FortiEDR поддерживает REST API. С помощью API возможно автоматизировать действия по администрированию FortiEDR, работе с инцидентами. Описание API FortiEDR доступно по следующей ссылке:
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/df7ab511-7435-11ea-9384-00505692583a/API_Guide_V4.1.pdf

Каким образом возможно передать информацию о инцидентах в сторонние системы?

FortiEDR поддерживает нотификацию об обнаруженных инцидентах средствами e-mail, syslog, а также позволяет открыть тикет в сторонней системе. Также FortiEDR поддерживает API, с помощью которого возможно, в том числе, запрашивать данные об инцидентах.

Какие данные FortiEDR передает в облако? Возможно ли отключить передачу данных в облако?

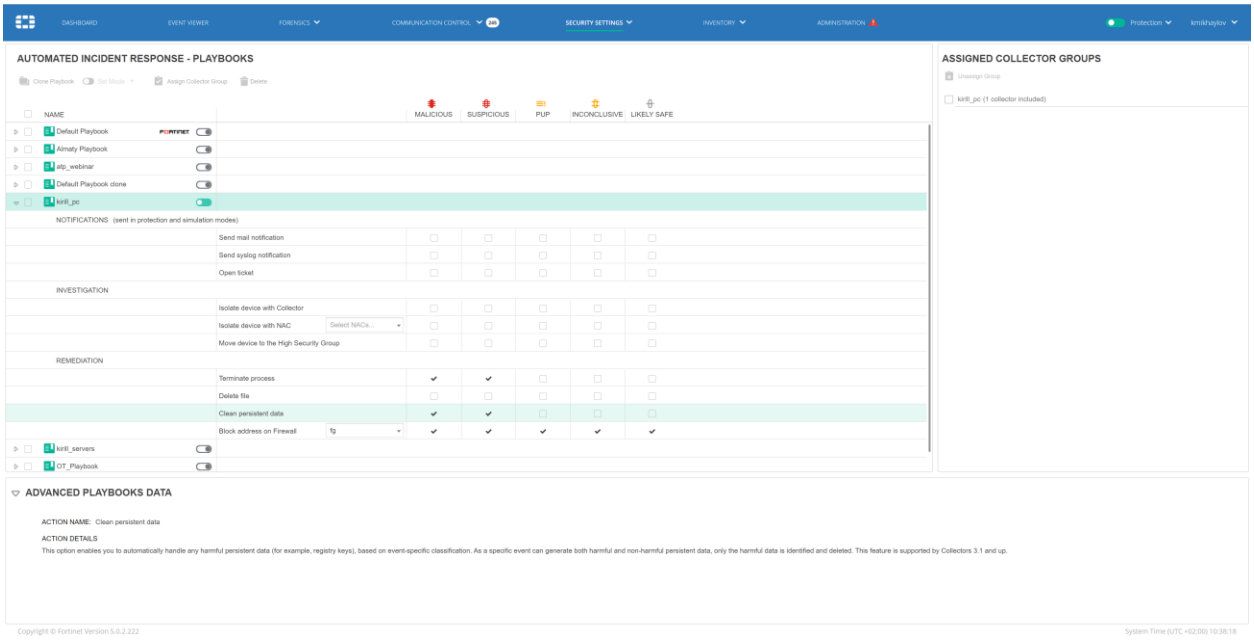
Список данных, передаваемых в облако доступен по следующей ссылке: https://fortinet.egnyte.com/fl/HMatujQpKx

FortiEDR позволяет отдельно отключить передачу файлов на анализ в облако. FortiEDR поддерживает возможность установки в изолированной среде (airgap), но в таком случае часть функционала недоступна. Сравнительная таблица для различных вариантов развертывания приведена ниже:

Функционал	Облако	Гибридный	Локальный с доступом к облаку FCS	Локальный без доступа к облаку FCS
Контроль сетевых соединений уязвимых приложений	+	+	+	-
Контроль USB	+	+	+	+
Поиск IOT устройств	+	+	+	+
Поиск неконтролируеммых устройств	+	+	+	+
Блокировка ВПО	+	+	+	+
Веб-фильтеринг	+	+	+	-
Автоматизированное реагирование	+	+	+	+
Обогащение репутационных данных	+	+	+	-
Реклассификация событий	+	+	+	-
Облачная песочница	+	+	+	-
Threat hunting	+	+	+	+
Managed detection and response (MDR)	+	+	-	-
Extended detection and response (XDR)	+	+	-	-

Может ли FortiEDR восстанавливать систему в случае, например, шифрования файлов или модификации реестра?

Для автоматизированного реагирования на инциденты в FortiEDR заложен функционал т.н. плэйбуков (playbooks) – политик автоматизированного реагирования на инциденты. Одно из действий, поддерживаемых плэйбуком – восстановление модифицированных ВПО ключей реестра.



Помимо этого, в функционал коллектора (агента) FortiEDR заложен функционал автоматического восстановления файлов, к которым происходило обращение ВПО. Данный функционал работает следующим образом: при обращении процесса к файлам коллектор FortiEDR создаёт в оперативной памяти копию файла, к которому происходит обращение, после чего, в случае обнаружения процесса как вредоносного автоматически восстанавливает модифицированный файл. Демо видео с примером работы данного функционала доступно по следующей ссылке: https://fortinet.egnyte.com/dl/20AvNA2XKz