

Совместим ли FortiEDR со сторонними защитными решениями?.....	2
Может ли FortiEDR защитить от вирусов-вымогателей?	2
Может ли FortiEDR автоматически реагировать на обнаруженные угрозы?	3
Может ли FortiEDR заменить решения EPP (Endpoint Protection), например, FortiClient?	3
Какие версии ОС поддерживает FortiEDR?	3
Сколько ресурсов требует агент FortiEDR? Не будет ли конечный узел перегружен?	4
Указано, что FortiEDR может быть установлен на серверные ОС. Какова вероятность, что агент своими действиями нарушит работоспособность сервера?	4
Поддерживает ли FortiEDR API?	4
Каким образом возможно передать информацию о инцидентах в сторонние системы?.....	4
Какие данные FortiEDR передает в облако? Возможно ли отключить передачу данных в облако?	5
Может ли FortiEDR восстанавливать систему в случае, например, шифрования файлов или модификации реестра?	5

Совместим ли FortiEDR со сторонними защитными решениями?

FortiEDR поддерживает гибкую настройку исключений.

The screenshot shows the 'EXCEPTION MANAGER' interface in FortiEDR. It features a search bar at the top with the text 'Search Exception' and a dropdown menu set to 'Advanced'. Below the search bar are icons for 'Edit', 'Delete', and 'Export'. A table lists various exceptions with columns for EVENT, PROCESS, PROCESS PATH, EXECUTED WITH, PATH, RULES, COLLECTOR GROUPS, DESTINATIONS, USERS, and LAST UPDATED. The table contains several entries, including 'SelfService.exe', 'updater.exe', 'NalogUL4712.exe', 'schtasks.exe', 'svchost.exe', 'Dashlane.exe', 'av_task.exe', and 'AnyDesk (7).exe'. At the bottom, there is a copyright notice 'Copyright © Fortinet Version 5.0.2.197' and a system time indicator 'System Time (UTC +02:00) 10:40:43'.

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.

The screenshot shows two interfaces in FortiEDR. The top interface is 'SECURITY POLICIES', which includes a search bar and a table with columns for POLICY NAME, RULE NAME, ACTION, and STATE. The table lists several policies, including 'Ransomware Prevention' and 'Debugged Process - Connection from a Debugged Process'. The bottom interface is 'ADVANCED POLICY & RULE DATA', which shows details for a specific rule, including its name, details, and recommendations. At the bottom, there is a copyright notice 'Copyright © Fortinet Version 5.0.2.197' and a system time indicator 'System Time (UTC +02:00) 10:44:03'.

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 – плейбуки.

NAME	MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
Default Playbook					
NOTIFICATIONS (sent in protection and simulation modes)					
Send mail notification	✓	✓	✓	✓	✓
Send syslog notification	✓	✓	✓	✓	✓
Open ticket	✓	✓	✓	✓	✓
INVESTIGATION					
Isolate device with Collector	□	□	□	□	□
Isolate device with NAC	□	□	□	□	□
Move device to the High Security Group	□	□	□	□	□
REMEDiation					
Terminate process	✓	□	□	□	□
Delete file	□	□	□	□	□
Clean persistent data	✓	□	□	□	□
Block address on Firewall	□	□	□	□	□

С помощью плейбуков 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 реагирования 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.

POLICY NAME	RULE NAME	ACTION	STATE
Device Control			
eXtended Detection			
DevC_Kirill			
ExecP_Kirill	Malicious File Detected	Block	Enabled
	Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected	Block	Enabled
	Sandbox Analysis - File was sent to the sandbox for analysis	Log	Enabled
	Stack Pivot - Stack Pointer is Out of Bounds	Block	Enabled
	Suspicious Driver Load - Attempt to load a suspicious driver	Block	Enabled
	Suspicious File Detected	Log	Enabled
	Suspicious Script Execution - A script was executed in a suspicious context	Block	Enabled
	Unconfirmed File Detected	Log	Enabled
ExecP_Renat			
Execution Prevention_OT			
ExtIP_Renat			

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 неконтролируемых устройств	+	+	+	+
Блокировка ВПО	+	+	+	+
Веб-фильтрация	+	+	+	-
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. плейбуков (playbooks) – политик автоматизированного реагирования на инциденты. Одно из действий, поддерживаемых плейбуком – восстановление модифицированных ВПО ключей реестра.

LOGS & REPORTS

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL

SECURITY SETTINGS

INVENTORY

ADMINISTRATION

Protection

AntiMalware

AUTOMATED INCIDENT RESPONSE - PLAYBOOKS

Clone Playbook | Edit Policy | Assign Collector Group | Done

NAME

Default Playbook

ARMED

ARMED

ARMED Playbook

ARMED

ARMED

isp_webinar

ARMED

ARMED

Default Playbook clone

ARMED

ARMED

MITRAC

ARMED

ARMED

NOTIFICATIONS (used in protection and simulation modes)

Send mail notification

Send syslog notification

Open ticket

INVESTIGATION

Isolate device with Collector

Isolate device with NAC

Move device to the High Security Group

REMEDATION

Terminate process

Delete file

Clean persistent data

Block address on Firewall

MITRAC

ARMED

ARMED

OT_Playbook

ARMED

ARMED

ASSIGNED COLLECTOR GROUPS

Assign Group

MITRAC (1 collector included)

ADVANCED PLAYBOOKS DATA

ACTION NAME: Clean persistent data

ACTION DETAILS

This option enables you to automatically handle any harmful persistent data (for example, registry keys), based on event-specific classification. As a specific event can generate both harmful and non-harmful persistent data, only the harmful data is identified and deleted. This feature is supported by Collectors 3.1 and up.

Copyright © Fortinet Version 5.8.2.222

System Time: UTC +02:00 10/30/18

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>