FortiClient

Next Generation Endpoint Security
Интеграция с Security Fabric

russia@fortinet.com

Тема

- **Введение**
  - Что такое FortiClient и EMS FortiClient
  - Какие бывают FortiClient и EMS FortiClient
  - Функционал FortiClient и EMS FortiClient
  - Оценки независимого тестирования
- **FortiClient что появилось нового**
- **FortiClient общая информация**
- **FortiClient 6.4. Демонстрация сценариев**
  - Применение профилей FortiClient к группам пользователей
  - Изменения в интеграции с Security Fabric – EMS, FGT, FAZ
  - SSL-VPN аутентификация с использованием SAML

Что такое FortiClient.
Какие бывают FortiClient
Функционал FortiClient

FortiClient

FortiClient. Типы клиентов

- FortiClient - это программный клиент с поддержкой различных операционных систем для комплексной защиты конечных устройств от продвинутых угроз, с модульной конструкцией, интегрированный в Fortinet Security Fabric, с встроенным SSL VPN и IPSEC VPN клиентом, SSO агентом, поддержкой многофакторной аутентификации и SD-WAN, обеспечивающий инвентаризацию установленного ПО, а также поиск неустановленных обновлений угрожающих безопасности и установку обновлений для ОС и приложений, а также установку сертификатов, централизованный карантин и управление белыми списками, управляемый из единой консоли EMS
- FortiClient бывает управляемый EMS FortiClient и Standalone FortiClient
  - **Standalone FortiClient** бывает **SSO Mobility Agent** или **VPN Only** клиент. Данные клиенты бесплатны при условии что не будут использоваться одновременно SSO и VPN функции. (для FortiAuthenticator покупается лицензия SSO для возможности использовать SSO Mobility Agent).
  - **Managed (управляемый) EMS FortiClient** включает весь функционал и может быть с поддержкой облачной песочницы или без поддержки облачной песочницы.

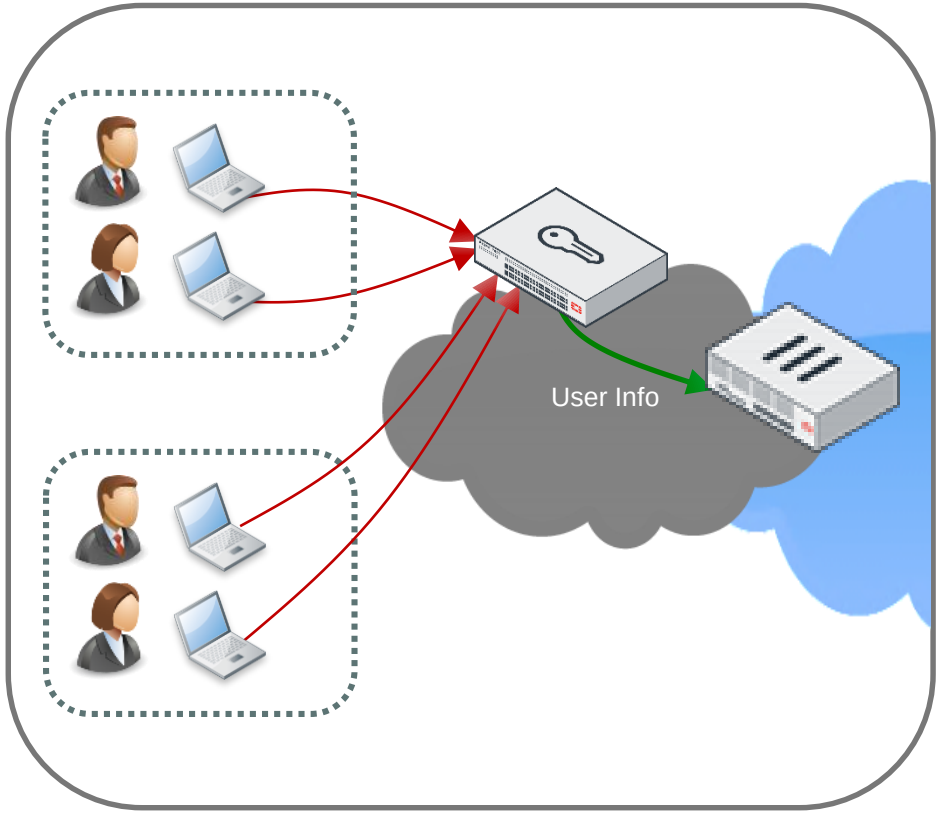
FortiClient

Standalone FortiClient

- Standalone FortiClient не лицензируется, используются без необходимости оплаты:
  - SSO Mobility Agent (на FortiAuthenticator необходима лицензия для использования данных агентов)
  - VPN Only
  - Full Standalone FortiClient v6.0 (уже почти не используется, устарел)
- SSO Mobility Agent используется в сценариях SSO для совместной работы с FortiAuthenticator. Агент автоматически передает имя пользователя и IP-адрес в модуль FortiAuthenticator для обеспечения прозрачной аутентификации. Полезен при изменениях IP-адреса, например, из-за роуминга WiFi или при переключении устройства между проводной и беспроводной сетью чтобы не спрашивать повторно аутентификацию пользователя. Когда пользователь выходит из системы или иным образом отключается от сети, устройство FortiAuthenticator знает об этом и деаутентифицирует пользователя. Поддерживает NTLM аутентификацию.
- VPN Only – это FortiClient с функцией SSL VPN и IPSEC VPN, с поддержкой 2FA аутентификации
- Full Standalone FortiClient v6.0 - бесплатный старая версия FortiClient который не рекомендуется для использования.

Standalone и Managed варианты FortiClient SSO Mobility Agent

SSO Mobility Agent работает в связке с FortiAuthenticator



Лучшая масштабируемость и эффективное обнаружение выхода пользователя из системы

SSO Mobility Agent

- Идентификация пользователя FortiClient
  - Обнаруживает login/logout/изменение IP
  - Шлет hello пакеты каждые 5 мин. чтобы обнаружить выключение, засыпание ПК и т.д.
- Автономный (возможность установки в виде фонового сервиса)
- Наиболее масштабируемый FSSO ID метод
- Поддерживает разные леса AD, домены и кросс доменные группы

Standalone и Managed варианты FortiClient VPN

Обзор вариантов VPN клиента

Группа	Функция	Безагентский SSL VPN	Нативный VPN	FortiClient VPN	FortiClient EMS
Лицензирование	Стоимость	Бесплатно веб-приложение HTML5	Бесплатно в составе ОС	Бесплатно загружаемый дистрибутив	Платно по количеству пользователей
	Техническая поддержка	Да	Нет	Нет	Да
ОС	Windows, Mac OS X, Android	SSL VPN web mode	IPsec VPN L2TP/IPsec VPN	IPsec VPN SSL VPN tunnel mode	IPsec VPN SSL VPN tunnel mode
	iOS, Linux	SSL VPN web mode	IPsec VPN	SSL VPN tunnel mode	SSL VPN tunnel mode
	Поддерживаемые приложения	Ограниченная поддержка Веб: HTTP, HTTPS Удаленный доступ: RDP, VNC Общие папки: SMB, SFTP, FTP Терминал: SSH, Telnet	Любые сетевые приложения (TCP/IP)	Любые сетевые приложения (TCP/IP)	Любые сетевые приложения (TCP/IP)
VPN	Поддержка двухфакторной аутентификации	Да	Да	Да	Да
	Поддержка Push аутентификации	Нет	Нет	Да	Да
	Split tunneling - частичное туннелирование	Не применимо	Ограниченно зависит от ОС	Да	Да
	Всегда включенный VPN	Не применимо	Ограниченно зависит от ОС	Нет	Да
	Автоматическая установка VPN за пределами доверенной сети	Не применимо	Ограниченно зависит от ОС	Нет	Да
	Автоматическая установка VPN при входе пользователя	Не применимо	Нет	Нет	Да
	Возможность преднастройки дистрибутива	Да	Нет	Нет	Да
Расширенные возможности	Защита от угроз	Нет	Нет	Нет	Да
	Проверка на соответствие политикам	Нет	Нет	Нет	Да
	Управление клиентами	Нет	Нет	Нет	Да

Managed вариант
EMS FortiClient или
FortiClient Security Fabric агент

FortiClient

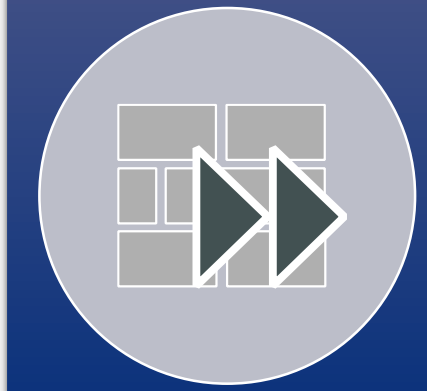
Managed или EMS FortiClient или FortiClient Security Fabric агент

- Managed или EMS FortiClient бывает:
  - С поддержкой Cloud FortiSandbox
  - Без поддержки Cloud FortiSandbox
- Оба типа EMS FortiClient идентичны, отличаются только наличием/отсутствием подписки на облачный Sandbox, оба могут использовать местную песочницу FortiSandbox.
- Распространяется как дистрибутив Windows или MacOS сформированный в консоли сервера EMS
- Дистрибутив Linux EMS FortiClient устанавливается как Standalone FortiClient, после чего подключается к EMS серверу и далее управляется из централизованной консоли EMS
- Дистрибутивы Android и iOS клиентов FortiClient устанавливаются из Google Play Market и AppStore репозиториев , после чего подключаются к консоли управления EMS.

Функционал FortiClient Security Fabric агента (EMS FortiClient)

Встроенное обнаружение любых угроз

ИНТЕЛЛЕКТУ-АЛЬНОЕ УПРАВЛЕНИЕ УГРОЗАМИ



МЕЖСЕТЕВОЙ ЭКРАН НОВОГО ПОКОЛЕНИЯ

ПЕСОЧНИЦА

КОМПЛЕКСНАЯ ЗАЩИТА КОНЕЧНЫХ УСТРОЙСТВ

Web Security

AV

Anti-Malware

Anti-Exploit

Anti-Botnet

и т.д.

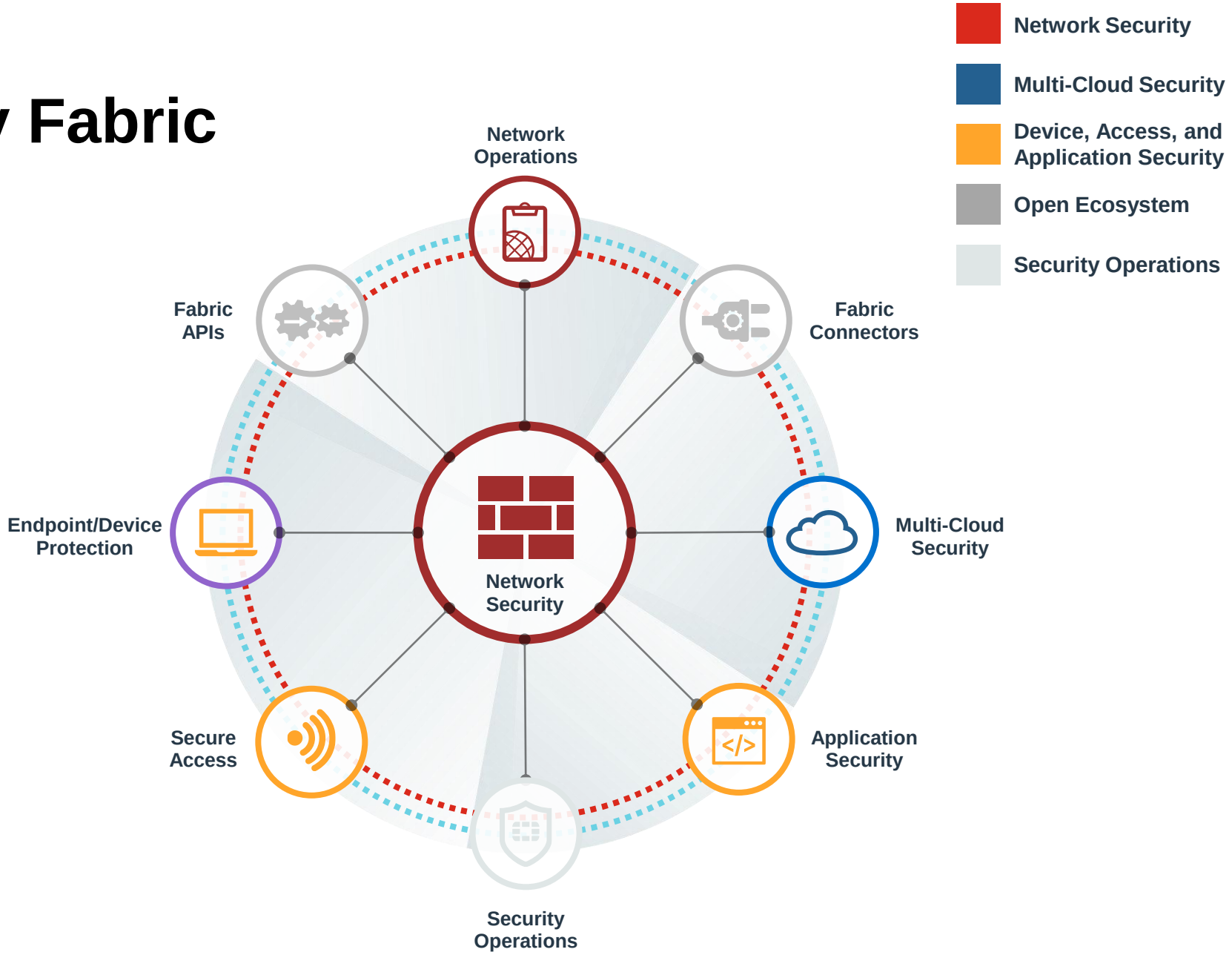
АНАЛИТИКА И АНАЛИЗ ПОВЕДЕНИЯ

Fortinet Security Fabric

ПОКРЫТИЕ
Видимость всей поверхности возможных атак

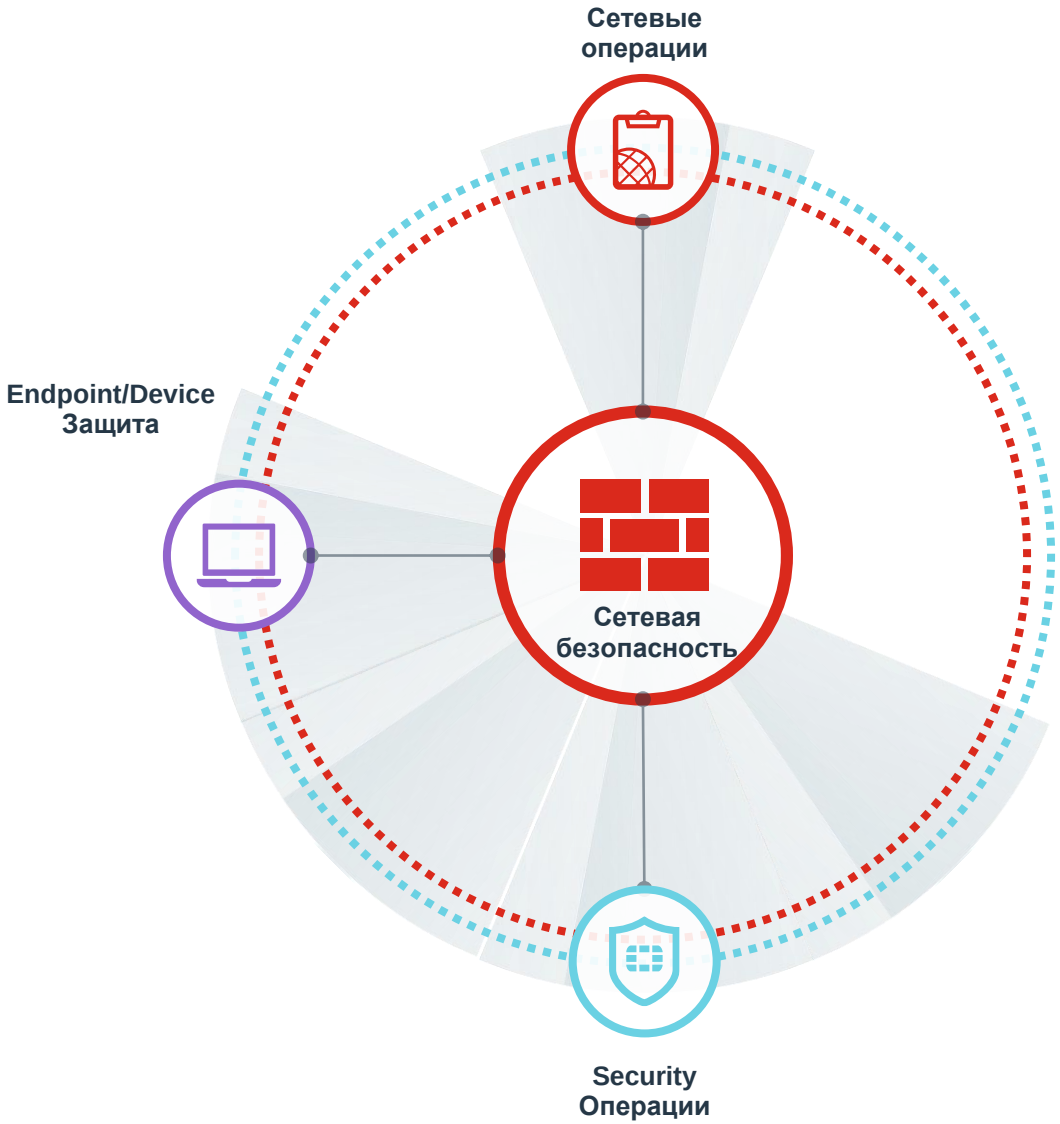
ИНТЕГРАЦИЯ
Управляемая искусственным интеллектом система предотвращения взлома через устройства, сети и приложения

АВТОМАТИЗАЦИЯ
автоматизация операций, оркестрация и обратная реакция



Комплексная защита конечной точки с интеграцией в Fortinet Security Fabric

Видимость конечных точек
Endpoint телеметрия Оценка состояния безопасности устройства Поиск уязвимостей
Динамический контроль доступа
Динамические группы Поддержка сегментации на основе намерений
Проактивная защита
AV с поддержкой ML,AI Интеграция Sandbox Anti-exploit Автоматическое ограничение, изоляция



FortiClient Security Fabric агент

Больше, чем расширенная защита конечных точек - уникальный набор функций

Комплексная защита рабочих станций (EPP)

Контроль приложений, Anti-malware, Anti-exploit, Web фильтрация

3

Защита от продвинутых угроз

Интеграция с песочницами Cloud/On-Prem Sandbox

Безопасный удаленный доступ

2

SSL & IPSec VPN, SSO, 2FA, Поддержка SAML, SD-WAN

Агент для интеграции с Security Fabric

1

Телеметрия, Централизованный Карантин, Централизованный белый список, Управление сертификатами, Динамические группы, Управление уязвимостями, Инвентаризация ПО

Интеграция с Fortinet Security Fabric

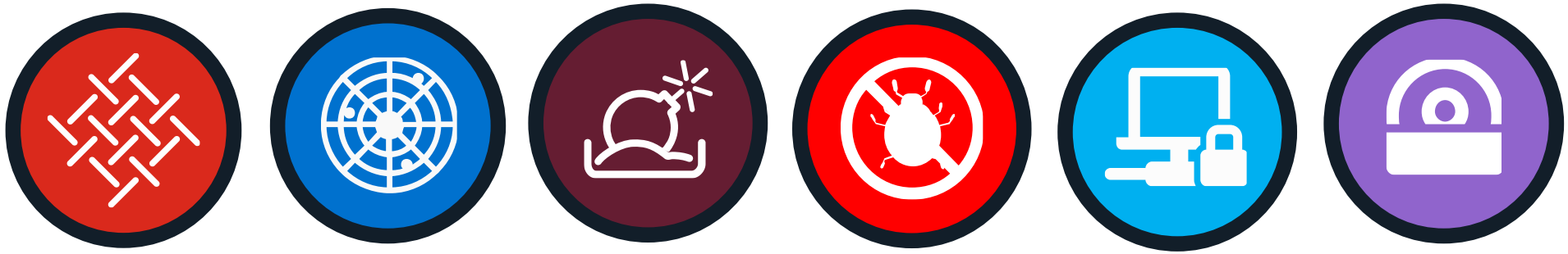
FortiGate, FortiSandbox, FortiAnalyzer, FortiAuthenticator, FortiNAC, FortiSOAR, FortiSIEM

FortiGuard Сервисы

CPRL AV, Web фильтрация, App Firewall, Управление уязвимостями (выявление, устранение)

1	2	3
Endpoint/IoT Видимость, Контроль, и Соответствие политикам	**Безопасный удаленный доступ**	**Комплексная защита рабочих станция от продвинутых угроз**
FortiClient FortiGate FortiAnalyzer Fabric Partners	**FortiClient FortiGate, FortiAuthenticator FortiNAC**	**FortiClient FortiSandbox FortiGuard**

Клиент удаленного доступа – FortiClient



Агент Security Fabric

Управление уязвимостями

Sandbox Агент

Anti-Malware Защита

Удаленный Доступ

Инвентаризация установленного ПО

Работает с другими сторонними Антивирусами в качестве дополнительного уровня защиты

Функциональные возможности FortiClient в зависимости от версии

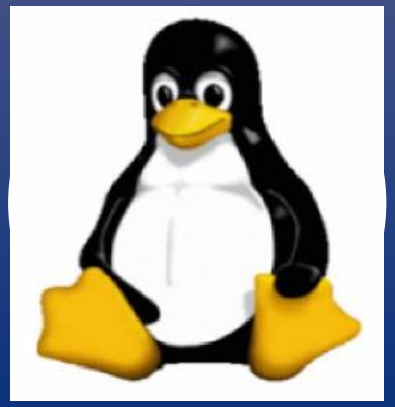
	WINDOWS	MAC OS X	ANDROID	iOS	CHROMEBOOK	LINUX
Security Fabric Components						
Endpoint Telemetry[1]	✓	✓	✓	✓	✓	✓
Compliance Enforcement using Dynamic Access Control[1]	✓	✓	✓	✓		✓
Endpoint Audit and Remediation with Vulnerability Scanning[1]	✓	✓				✓
Automated Endpoint Quarantine	✓	✓				
Host Security and VPN Components						
Antivirus	✓	✓				✓
Cloud-based Threat Detection	✓					
Anti-Exploit	✓					
Sandbox Detection (on-prem)	✓	✓				✓*
Sandbox Cloud Detection	✓	✓				
Web Filtering[2]	✓	✓	✓	✓	✓	
Application Firewall[1]	✓	✓				
IPsec VPN	✓	✓	✓			
SSL VPN[3]	✓	✓	✓	✓		✓
Others						
Remote Logging and Reporting[4]	✓	✓		✓	✓	✓
Windows AD SSO Agent	✓	✓				
USB Device Control	✓	✓				✓

FORTINET

РАБОТАЕТ НА РАЗЛИЧНЫХ ОС

WINDOWS SERVER

WINDOWS ENDPOINT



LINUX

CENTOS

UBUNTU

RED HAT

MacOS

iOS

Android,

Chrome OS

FortiClient

Больше, чем расширенная защита конечных точек

Fabric Agent

4 **Комплексная защита рабочих станций (EPP)**

Контроль приложений, Anti-malware, Anti-exploit, Web фильтрация

3 **Защита от продвинутых угроз**

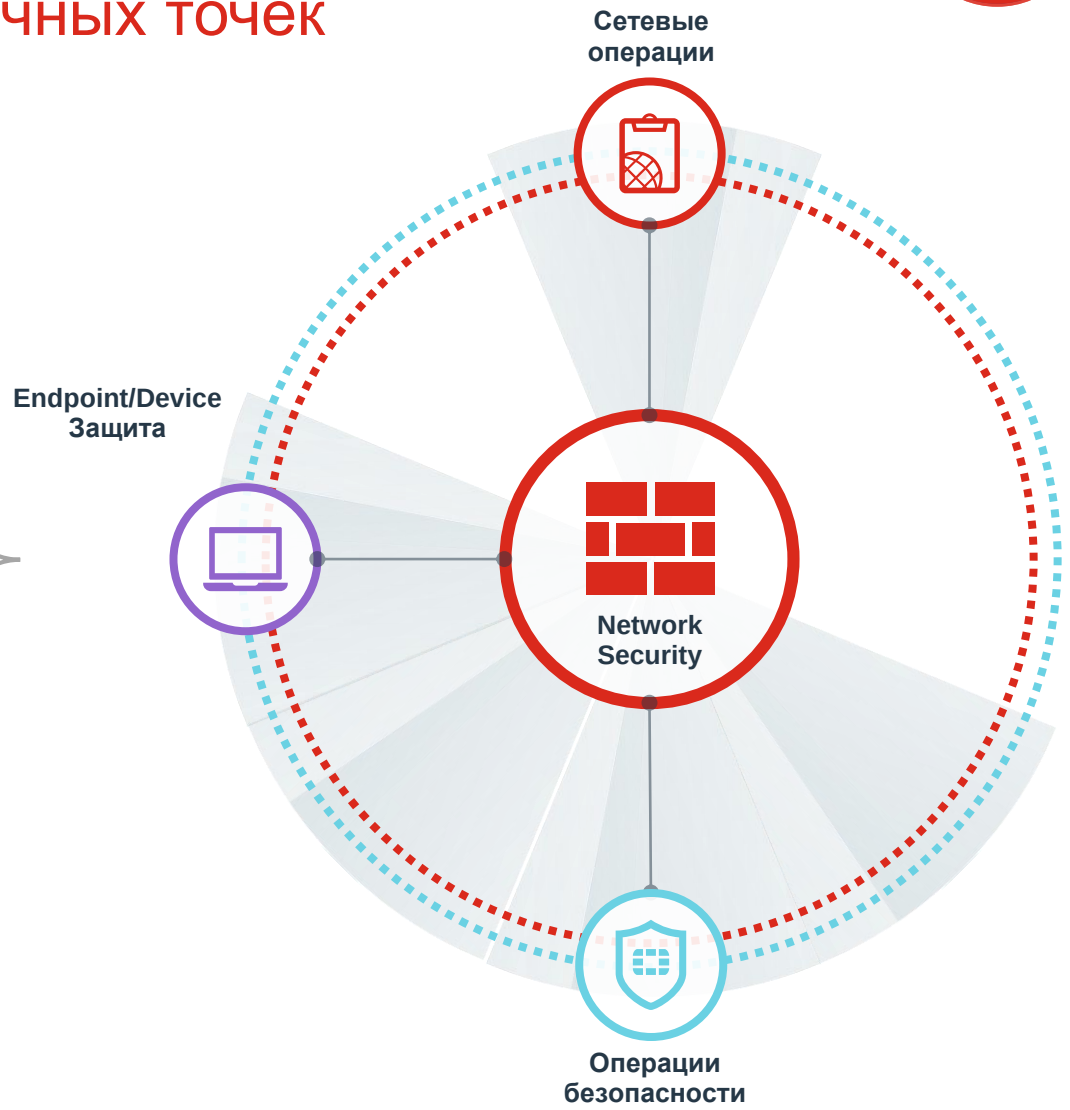
Интеграция с песочницами Cloud/On-Prem Sandbox

2 **Безопасный удаленный доступ**

SSL & IPSec VPN, SSO, 2FA, Поддержка SAML, SD-WAN

1 **Агент для интеграции с Security Fabric**

Телеметрия, Централизованный Карантин, Централизованный белый список, Управление сертификатами, Динамические группы, Управление уязвимостями, Инвентаризация ПО



Fabric Agent примеры использования

- Видимость всех событий с указанием рисков
  - Идентификация уязвимостей, указание на патч, с возможностью установки
  - Видимость всех установленных приложений, версий. Инвентаризация
  - Определение принадлежности станции, уровня риска, концентрация на важных событиях
- Динамический контроль доступа
- Интеграция и автоматизация
  - Интеграция с Security Fabric
  - Автоматическое реагирование на инциденты
- Совместимость
- Контроль соответствия

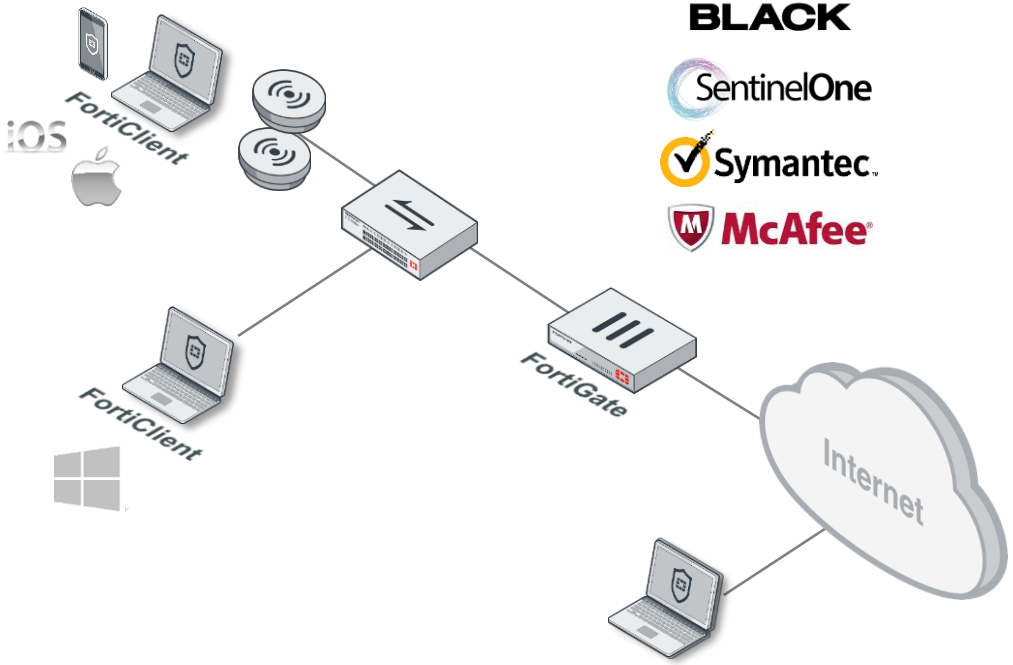
FORTINET Fabric-Ready

CARBON BLACK

SentinelOne

Symantec

McAfee



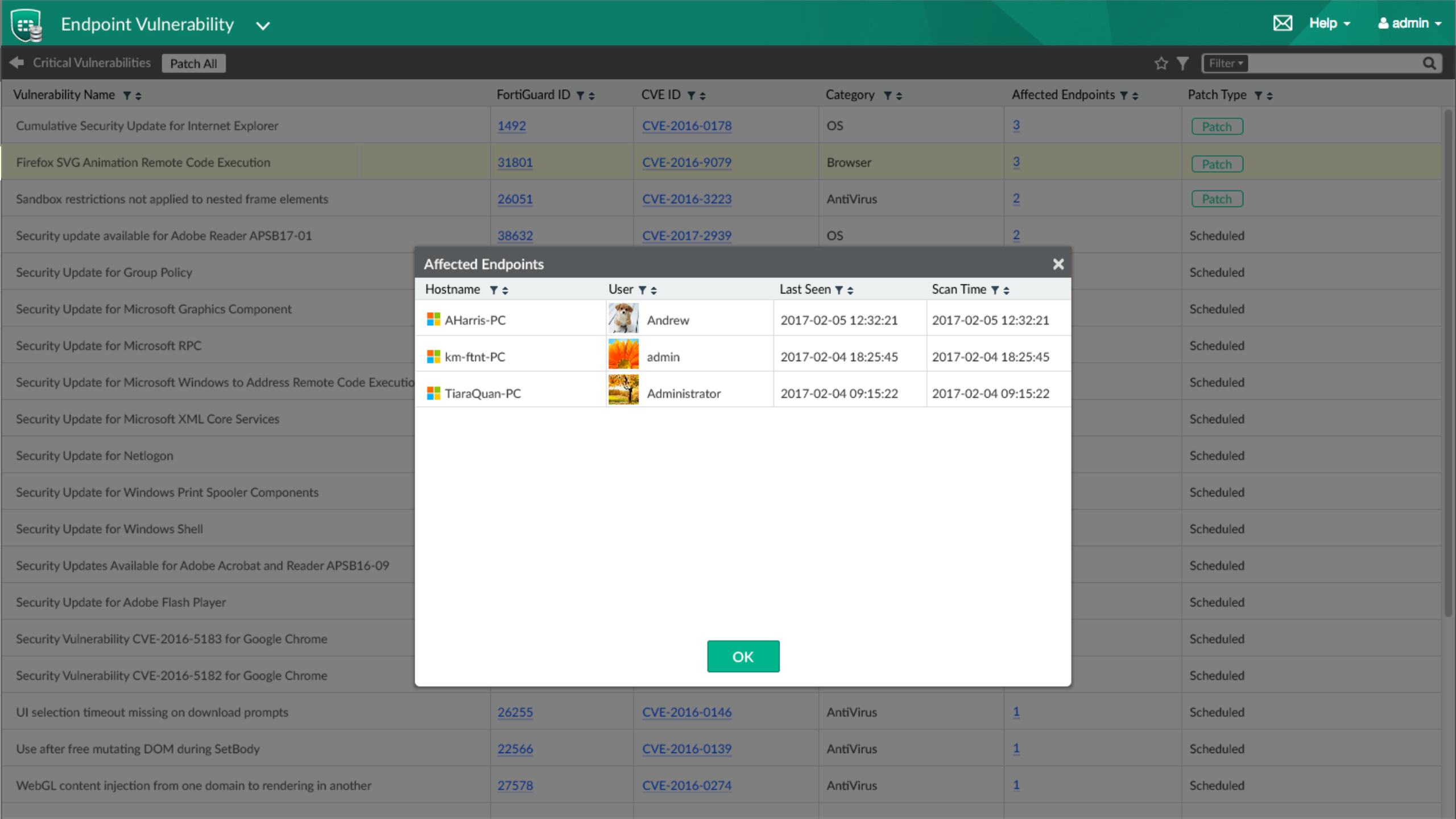
Пример использования Fabric Agent

Автосалоны

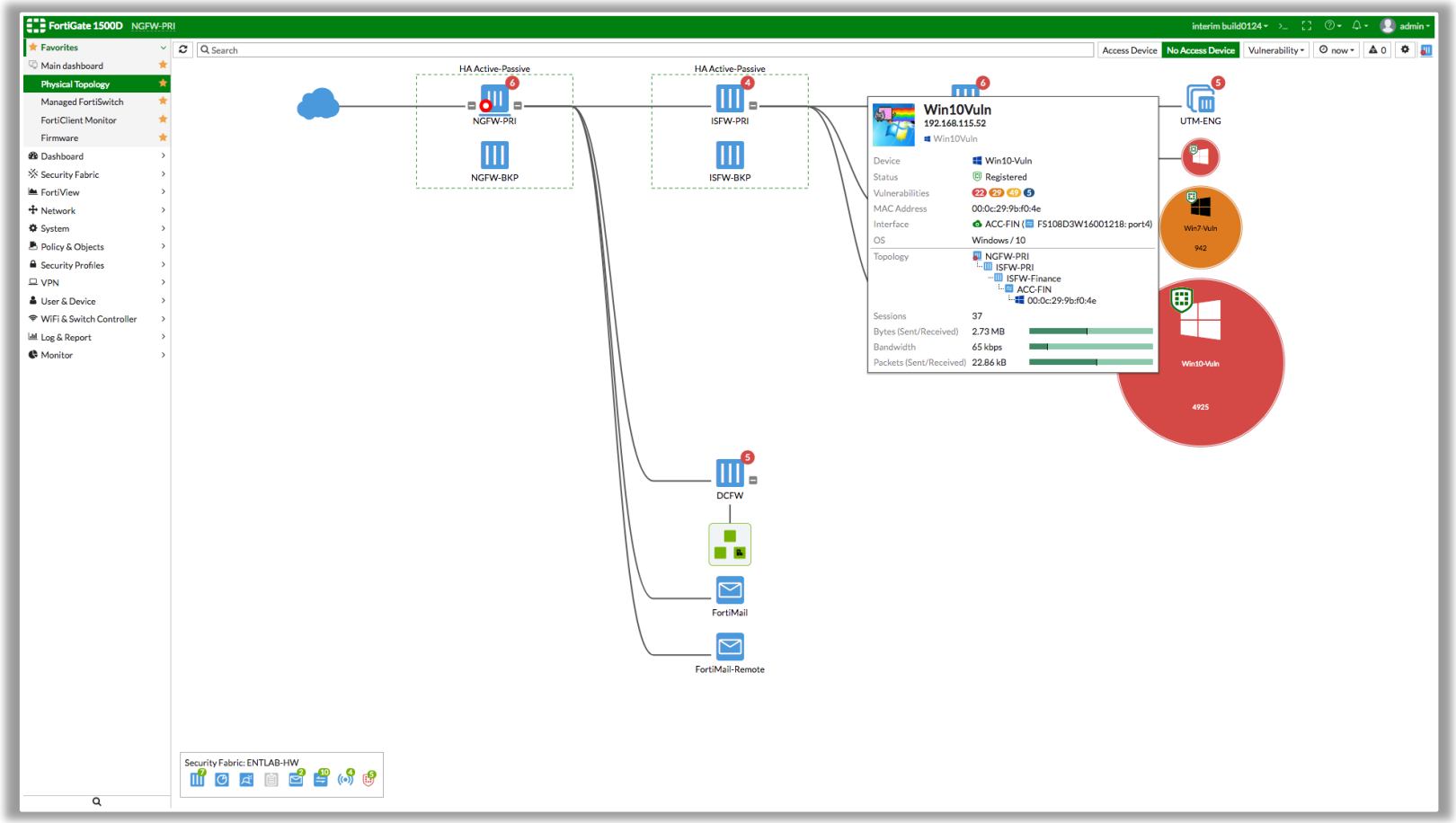
Почему интересен продукт

- ✓ Интеграция - Security Fabric архитектура
- ✓ Решения от одного вендора
- ✓ Видимость всех событий, топологии, трафика, процессов, уровня соответствия, пользователей и т.д.
- ✓ Безопасный SD-WAN с встроенным NGFW функционалом от одного из лидеров рынка NGFW и SD-WAN
- ✓ Открытая экосистема, совместимость

Пример используемых продуктов	Проекты	Ключевые требования
✓ FortiGate 601E, 101F and 40F ✓ FortiGate VM (for Azure) ✓ FortiClient w/ EMS 2300 licenses ✓ FortiManager VM ✓ FortiAnalyzer ✓ FortiSwitch/ FortiAP	✓ Проекты нацеленные на увеличение уровня безопасности для соответствия требованиям (GDPR) ✓ Безопасная организация сетевой связности – Портативные компьютеры пользователей, все офисы с центрами обработки данных и общедоступное облако ✓ Защита ЦОД ✓ Проекты SDWAN	✓ Сильная безопасность ✓ Комплексное решение - один поставщик для защиты центра обработки данных, филиала, конечных точек.. ✓ Соответствие GDPR для обеспечения безопасности данных ✓ Endpoint видимость/соответствие, управление

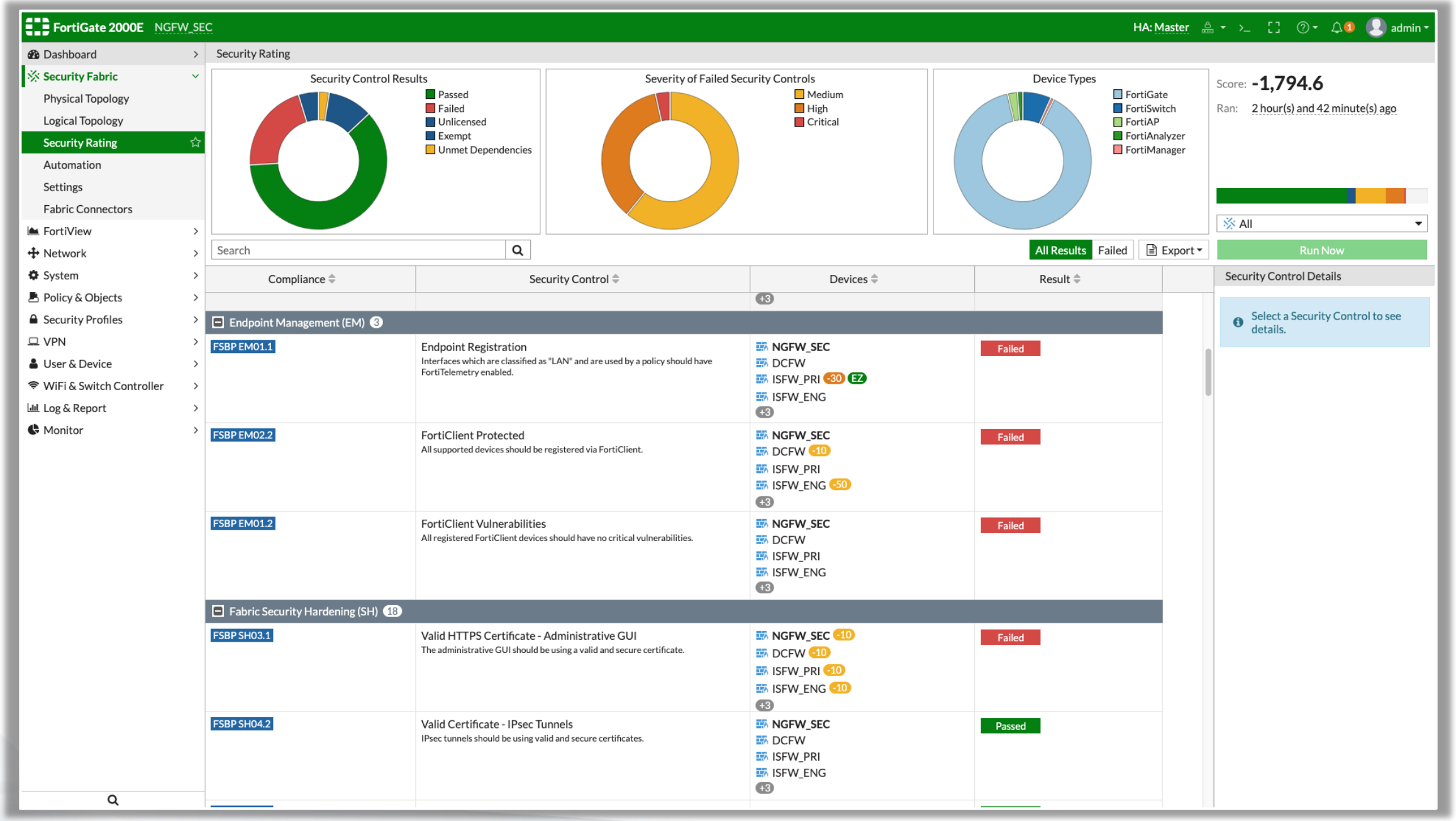

Endpoint Vulnerability
Help
admin
Critical Vulnerabilities
Patch All
Filter
Vulnerability Name
FortiGuard ID
CVE ID
Category
Affected Endpoints
Patch Type
Cumulative Security Update for Internet Explorer 1492 CVE-2016-0178 OS 3 Patch
Firefox SVG Animation Remote Code Execution 31801 CVE-2016-9079 Browser 3 Patch
Sandbox restrictions not applied to nested frame elements 26051 CVE-2016-3223 AntiVirus 2 Patch
Security update available for Adobe Reader APSB17-01 38632 CVE-2017-2939 OS 2 Scheduled
Security Update for Group Policy Scheduled
Security Update for Microsoft Graphics Component Scheduled
Security Update for Microsoft RPC Scheduled
Security Update for Microsoft Windows to Address Remote Code Executio Scheduled
Security Update for Microsoft XML Core Services Scheduled
Security Update for Netlogon Scheduled
Security Update for Windows Print Spooler Components Scheduled
Security Update for Windows Shell Scheduled
Security Updates Available for Adobe Acrobat and Reader APSB16-09 Scheduled
Security Update for Adobe Flash Player Scheduled
Security Vulnerability CVE-2016-5183 for Google Chrome Scheduled
Security Vulnerability CVE-2016-5182 for Google Chrome Scheduled
UI selection timeout missing on download prompts 26255 CVE-2016-0146 AntiVirus 1 Scheduled
Use after free mutating DOM during SetBody 22566 CVE-2016-0139 AntiVirus 1 Scheduled
WebGL content injection from one domain to rendering in another 27578 CVE-2016-0274 AntiVirus 1 Scheduled
Affected Endpoints
Hostname
User
Last Seen
Scan Time
AHarris-PC Andrew 2017-02-05 12:32:21 2017-02-05 12:32:21
km-ftnt-PC admin 2017-02-04 18:25:45 2017-02-04 18:25:45
TiaraQuan-PC Administrator 2017-02-04 09:15:22 2017-02-04 09:15:22
OK

Видимость риска в контексте сети за счет сбора данных с каждой конечной точки

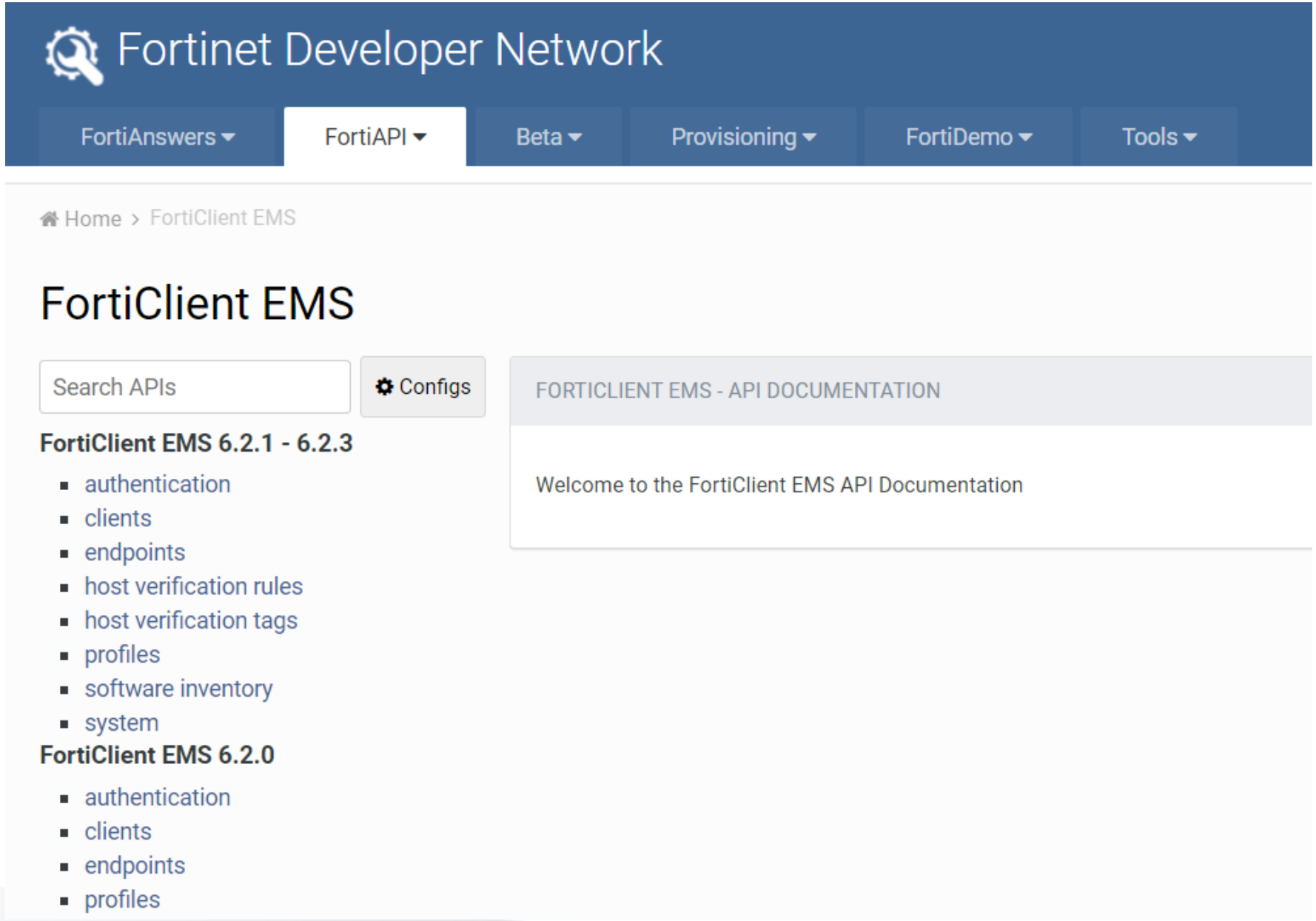


- Информация об устройстве
  - OS
  - Все MAC адреса, IP адреса, порт и т.д.
- Статус FortiClient
- Уязвимости существующие
- Текущий пользователь
- Фото
- Social ID идентификатор
- Online/Off-line статус
- События и логи связанные с устройством

Рейтинг безопасности

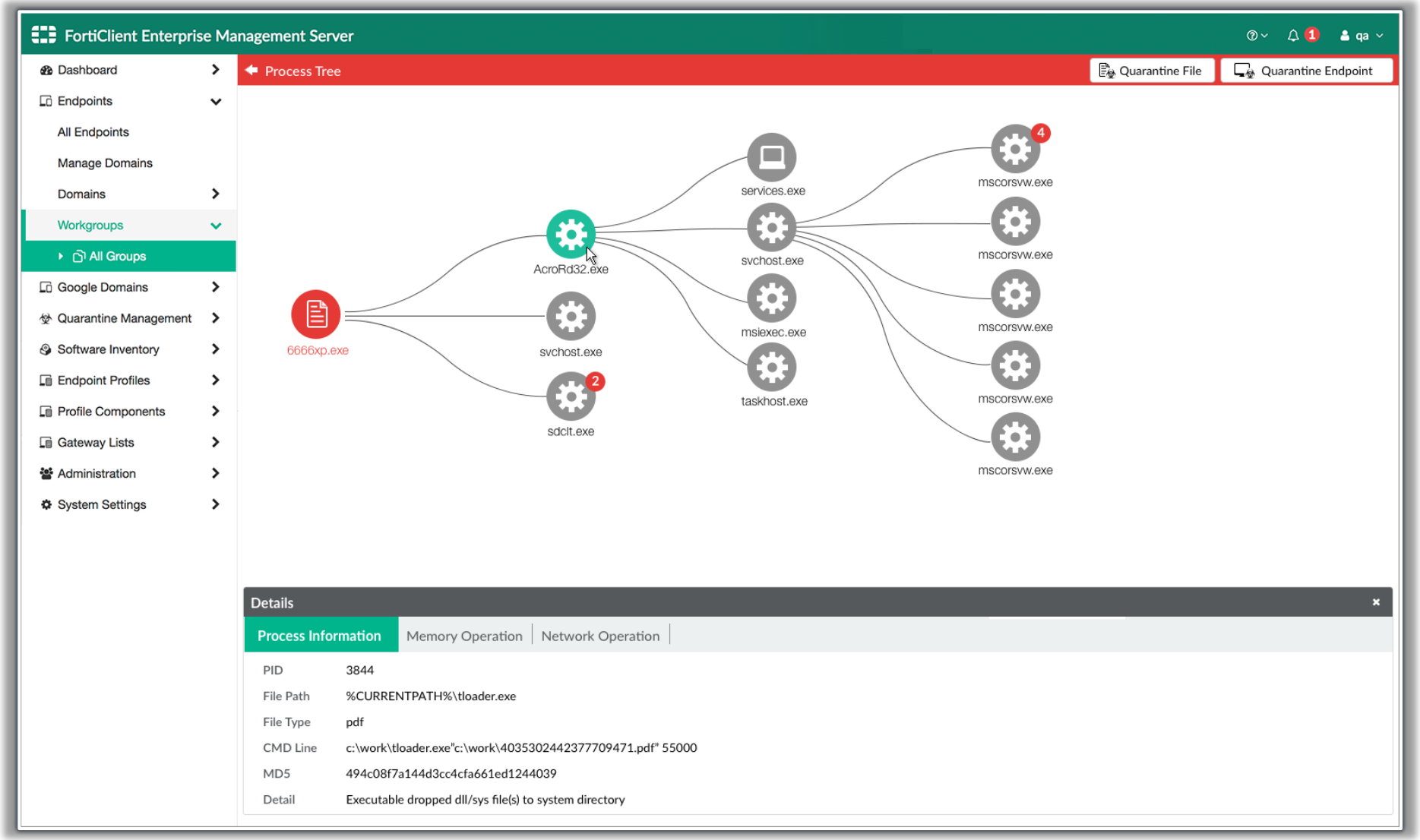


FortiClient EMS API



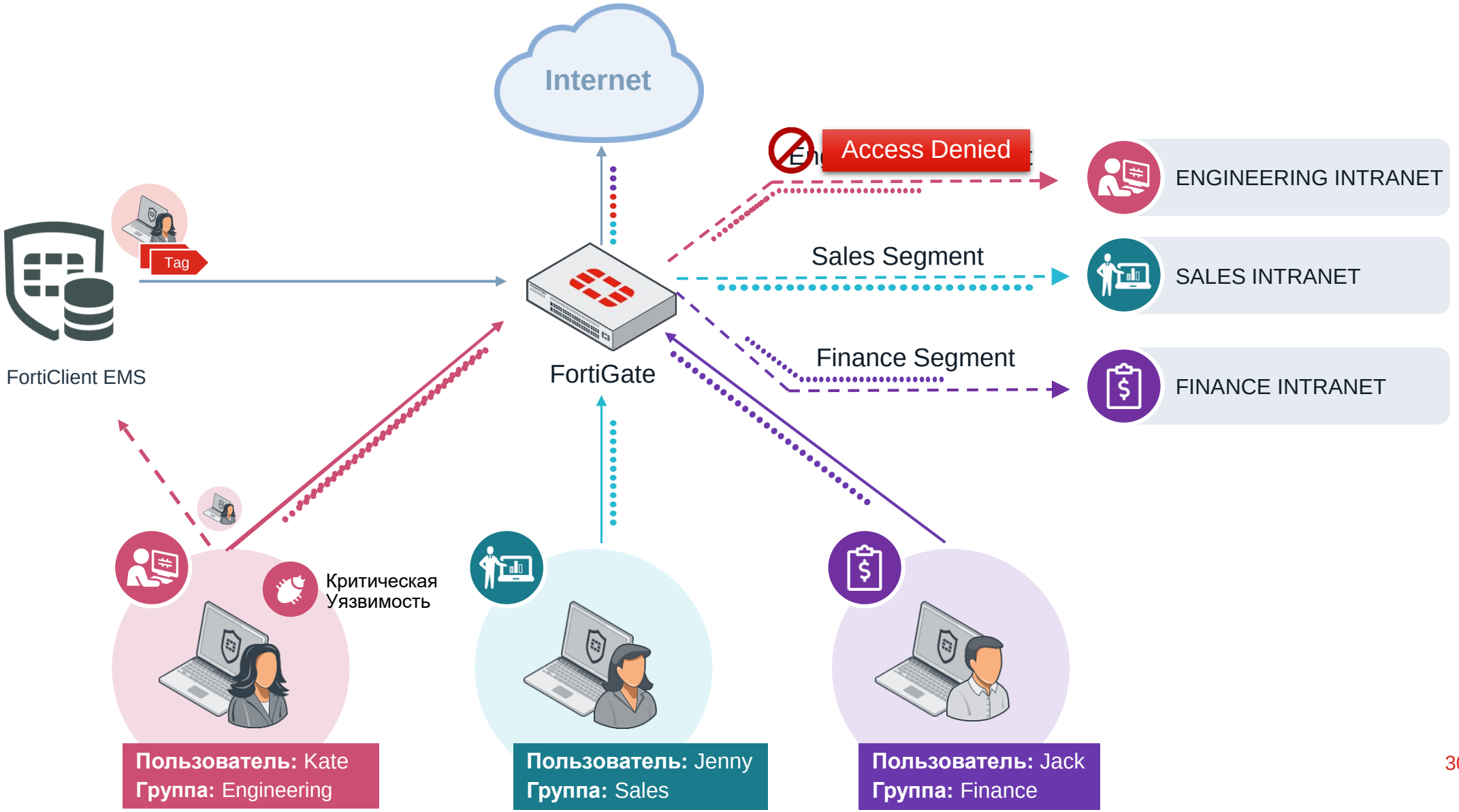
Что нового в 6.2

Расширенная интеграция с Sandbox



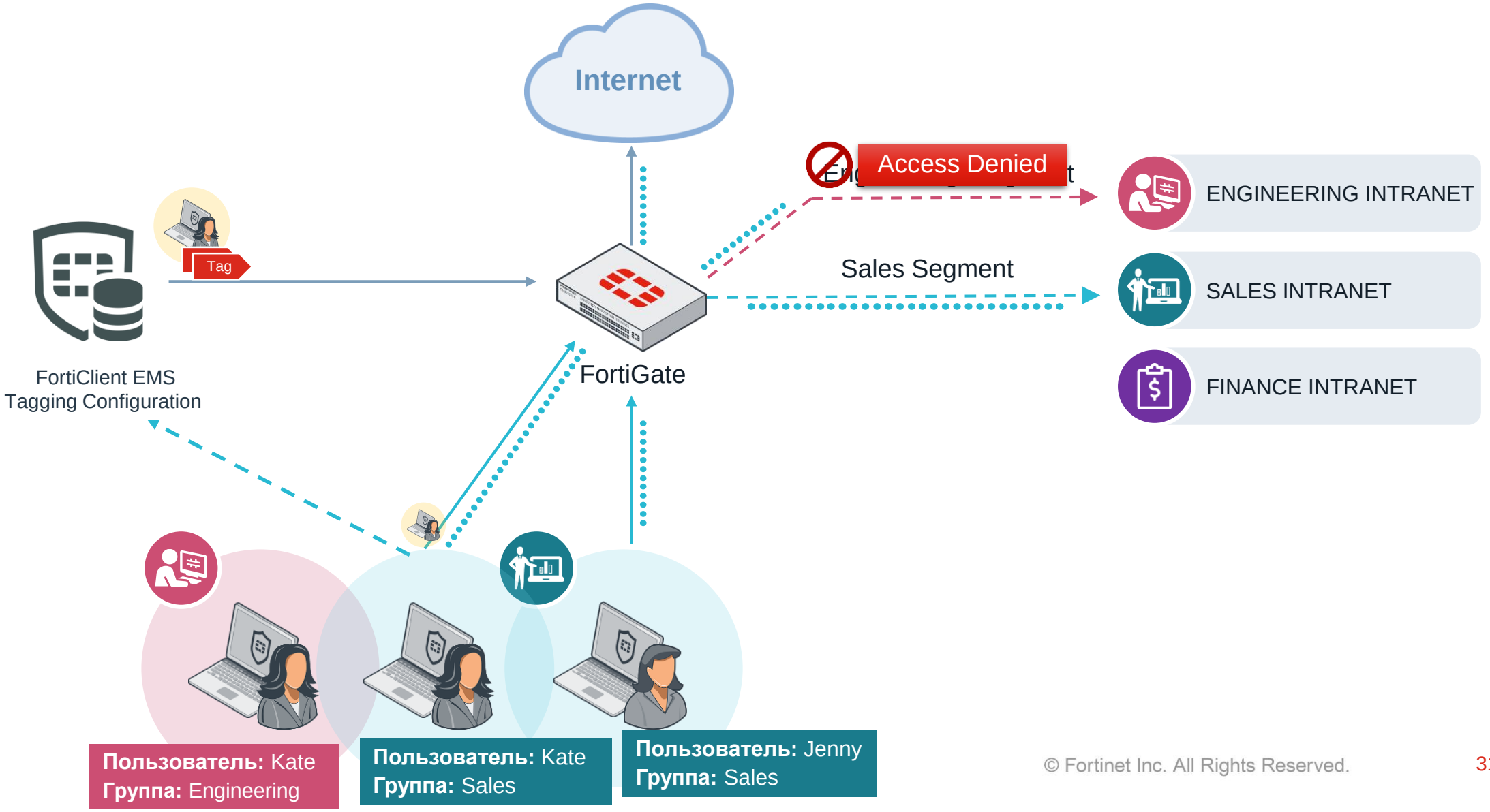
Динамический контроль доступа (Сегментация на основе намерений)

Пример: Блокировать доступ машин с риском к ресурсам компании



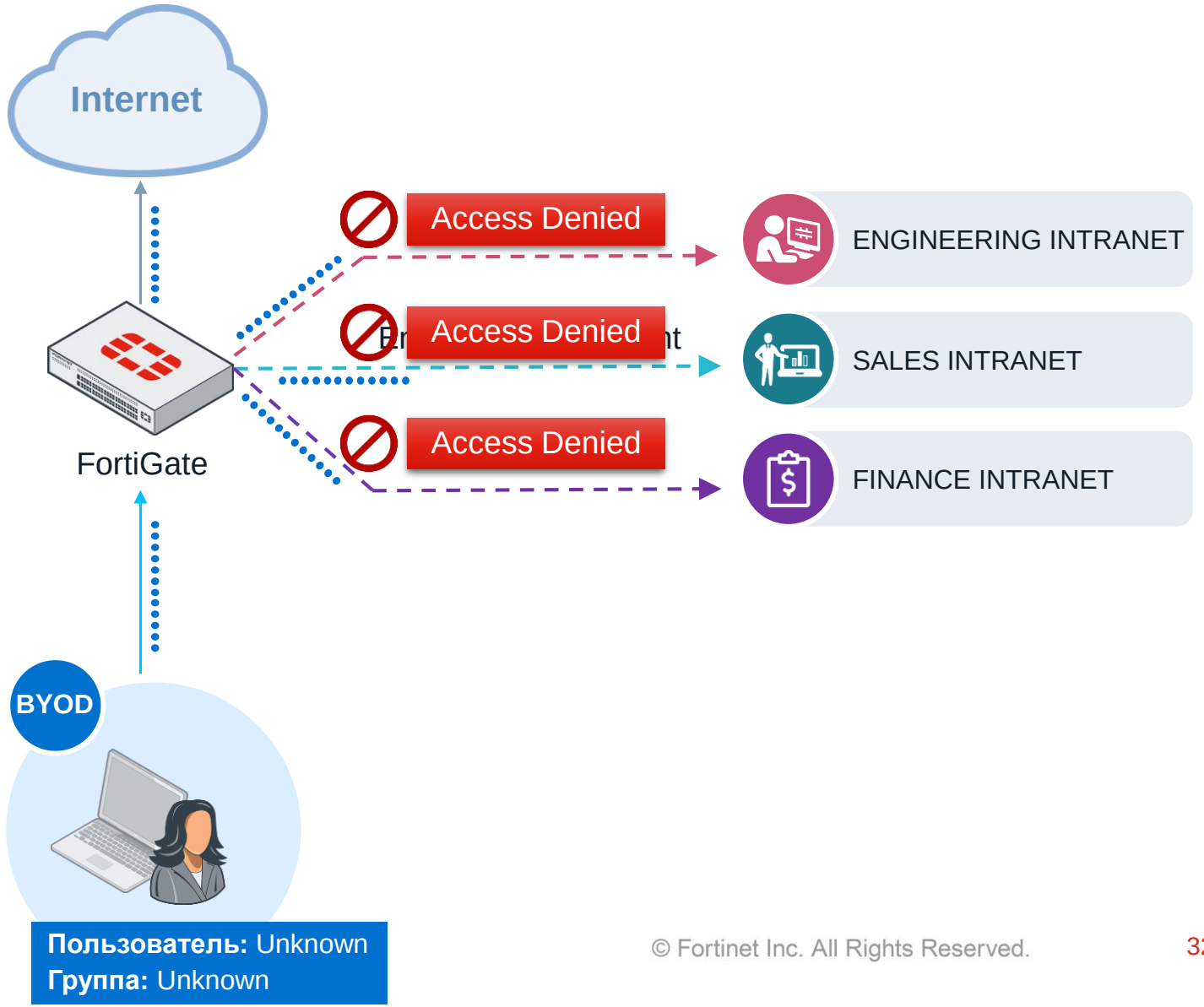
Динамический контроль доступа (Сегментация на основе намерений)

Пример: Доступ на основе членства в группе AD



Динамический контроль доступа (Сегментация на основе намерений)

Пример: Ограничение доступа неизвестных пользователей

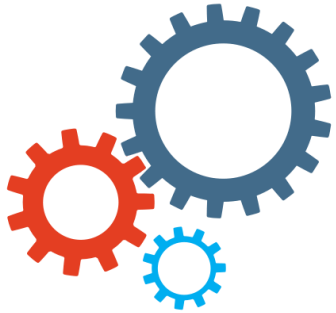


FortiClient 6.2

УЛУЧШЕНО ОБНАРУЖЕНИЕ УГРОЗ

- Расширенная интеграция с Sandbox
- Sandbox аналитические отчеты в EMS
- Облачное обнаружение в режиме реального времени новых угроз

FABRIC АВТОМАТИЗАЦИЯ



- Динамический контроль доступа
- Динамические виртуальные группы
- Поддержка политик FortiOS с использованием динамических групп

ОБЛАЧНОЕ УПРАВЛЕНИЕ

- FortiClient Cloud
- FortiSandbox Cloud интеграция

Проактивная защита конечных точек

- Antimalware—CPRL усиленный ML и AI
- Anti-exploit
- Web фильтрация
- Межсетевой экран приложений
- Интеграция с Sandbox

Проактивная защита конечных точек

Устранить уязвимости & Блокировать эксплойты	Обнаружение & Блокировка сложного вредоносного ПО	Интеграция & Автоматизация реакции
• Поиск уязвимостей • Установка обновлений • Защита от эксплойтов	new • Anti-malware new • Обнаружение malware не создающих файл • Обнаружение угроз в облаке • Anti-Exploit • Web фильтрация improved • МСЭ приложений • Интеграция с Sandbox	• Карантин файлов и устройств/ПК • Установка обновлений • Интеграция с Sandbox • Интеграция с SIEM

Видимость. Интеграция. Централизованное управление.

FortiClient – лицензирование, советы

FortiClient: при обновлении EMS не забудьте сконвертировать лицензию

Обновление версии лицензии FortiClient

- Поскольку вы можете приобрести несколько лицензий EMS FortiClient Fabric всегда указывайте что именно вы хотите сделать: объединить лицензии или использовать несколько разных EMS!
- При обновлении FortiClient EMS с 6.0 до 6.4.0 или 6.2.0, EMS сохраняет лицензию 6.0 после обновления. Однако из-за серьезных изменений в лицензировании, введенных в 6.2.0, вы все равно должны преобразовать лицензию в лицензию версии 6.4 или 6.2, вручную преобразовав лицензию на сайте обслуживания и поддержки клиентов до 31 августа 2020 г. или связавшись со службой поддержки Fortinet. После истечения срока действия конвертированной лицензии вы должны заказать и применить лицензии 6.2.

FortiClient: срок действия лицензий EMS

Добавление лицензии

- Новые лицензии добавленные к существующему EMS применяются в день когда истекает срок действия старой лицензии. Добавить новые лицензии можно в любой момент, если это не upgrade, при апгрейде лучше предварительно уточнить что лицензии обновлены до нужной версии.
- После истечения срока действия лицензии на EMS у вас будет 10 дней в течении которых клиенты FortiClient продолжат работать со всем функционалом (grace период), после истечения 10 дней лицензируемые функции EMS FortiClient будут выключены

FortiClient – Лицензирование

- **Упрощение** - FortiGate, на котором работает FortiOS 6.2, автоматически получает телеметрию от FortiClient 6.2 - Нет необходимости в отдельной лицензии на телеметрию/Compliance функционал для FortiGate
- **Небольшие пакеты** – Минимальная лицензия рассчитана на 25 клиентов
- Есть пакет, включающий интеграцию с FortiSandbox Cloud
- Схема лицензирования соответствует отраслевому стандарту, лицензирование FortiClient осуществляется по количеству устройств, централизованное управлением (EMS) включено в стоимость.
- Больше нет бесплатного полнофункционального FortiClient.
- Бесплатный ограниченный VPN-клиент

FortiClient 6.0 (для FortiOS 6.0 / 5.6)		FortiClient 6.2 (для FortiOS 6.2)
		FortiClient Fabric Agent with Sandbox Cloud: FC-15-EMS01-299-02-DD
FortiClient EMS SKU: FC1-15-EMS01-158-02-DD	→	FortiClient Fabric Agent SKU: FC-15-EMS01-297-02-DD
FortiClient Telemetry/compliance license for FortiGate: FC1-10-C1100-151-02-DD	→	Не требуется лицензии на FortiGate
EMS for Chrome: FC1-15-EMS02-158-02-DD	→	FortiClient Chromebook: FC-15-EMS01-403-02-DD

FortiClient 6.2 SKU

	Fabric Agent with Endpoint Protection and Sandbox Cloud	Fabric Agent with Endpoint Protection	FortiSandbox Cloud Subscription	FortiClient Chromebook
SKU	FC1-15-EMS01-299-02-DD	FC1-15-EMS01-297-02-DD	FC1-15-EMS01-298-02-DD	FC1-15-EMS01-403-02-DD
Security Fabric Components (Fabric Agent)	Yes	Yes	No	Limited (Telemetry only)
Endpoint protection (EPP)	Yes	Yes	No	Web filtering only
Sandbox agent for FortiSandbox integration	Yes	Yes	No	No
Secure remote access (VPN, SSL)	Yes	Yes	No	No
Sandbox Cloud Subscription	Yes	No	Yes	No
Centralized management	EMS	EMS	EMS	EMS

Zero-Trust Network Access

Многоуровневое лицензирование FortiClient. Версия 6.4

FortiClient Cloud

500-10,000
(500 pack)

0-499
(25 pack)

Лицензия доступна в пакетах по 500 и **значительно дешевле прейскурантной цены**

Лицензия доступна в упаковках по 25 и может стекироваться для увеличения количества конечных точек

On-Premise

10,000+
(10,000 pack)

500-10,000
(500 pack)

0-499
(25 pack)

Лицензия доступна в пакетах по 10 000 и **значительно дешевле прейскурантной цены**

Лицензия доступна в пакетах по 500 и **значительно дешевле прейскурантной цены**

Лицензия доступна в упаковках по 25 и может стекироваться для увеличения количества конечных точек

6.4: SKU новые лицензии

Новые лицензии

- FortiClient – Security Fabric Agent Subscription (FortiClient 6.2)
- FortiClient Tiered License
  - Добавляются пакеты для 25, 500 или 10K мест
  - Нет отличий в цене
  - Нет отличий в функционале
- FortiClient Cloud
  - Отдельный SKU
  - Не нужно покупать FortinetONE Premium лицензию
- FortiGuard Cloud – Off Fabric Endpoints
  - Появится в ближайшее время….. ☺

Вопросы?

- Что случилось с 6.0 лицензиями?
  - Заказать можно, но по запросу
  - Заказчики могут продлять 6.0 лицензии
  - Нет сообщений об отмене лицензий 6.0
- Можно ли использовать FortiClient Tiered SKU для FCT 6.2 → Да
- Лимит на FortiClient Cloud? → В настоящее время максимальное количество 5000. В ближайшее время увеличат.

Резюме

FortiClient

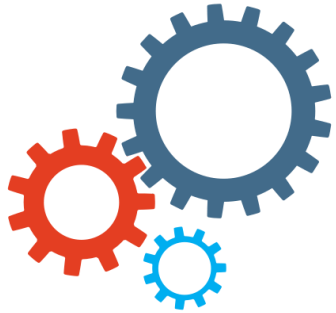
Видимость

- Расширенная видимость во всех ОС - Windows, Mac, Linux, Chromebook, Android и iOS
- Инвентаризация программного обеспечения
- Интегрированное управление уязвимостями с возможностью установки обновлений

Проактивная защита

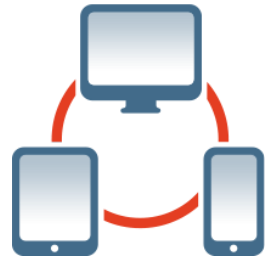
- CPRL обновляемый через FortiGuard ML
- Расширенная интеграция с Sandbox
- Sandbox аналитические отчеты в EMS
- Облачное обнаружение в режиме реального времени для новых угроз

Автоматизация



- Динамический контроль доступа
- Контроль соответствия политикам безопасности
- Security Fabric IOC Карантин
- Поддержка политик с FortiOS группами

Упрощенное управление



- Динамическая группировка устройств в зависимости от состояния
- Управление централизованным карантином
- Единая консоль для всех устройств
- Улучшенное удобство использования благодаря новой навигации
- Облачный вариант EMS

Что такое EMS.
Какие бывают EMS серверы

Архитектура решения FortiClient EMS

FortiClient EMS

EMS FortiClient как решение может включать следующие компоненты:

Основные компоненты

- База данных SQL. До 5000 клиентов достаточно SQL Express который устанавливается по умолчанию
- FortiClient EMS сервер устанавливаемый на Windows ОС
- FortiClient клиенты устанавливаемые на рабочие станции, сервера, мобильные устройства
- FortiAnalyzer как средство мониторинга, сбора логов, аналитики, задания обратной реакции

FortiClient EMS

EMS FortiClient как решение может включать следующие компоненты:

Опциональные компоненты

- FortiGate как VPN шлюз или NGFW шлюз совместно с которым работает EMS

FortiNAC	FortiSOAR	Другие продукты Fortinet
FortiSIEM	FortiGuard Cloud	
FortiManager	FortiSandbox	FortiAuthenticator
MDM системы	Endpoint клиенты сторонних производителей	
Другие решения партнеров Fortinet		

Система централизованного управления FortiClient

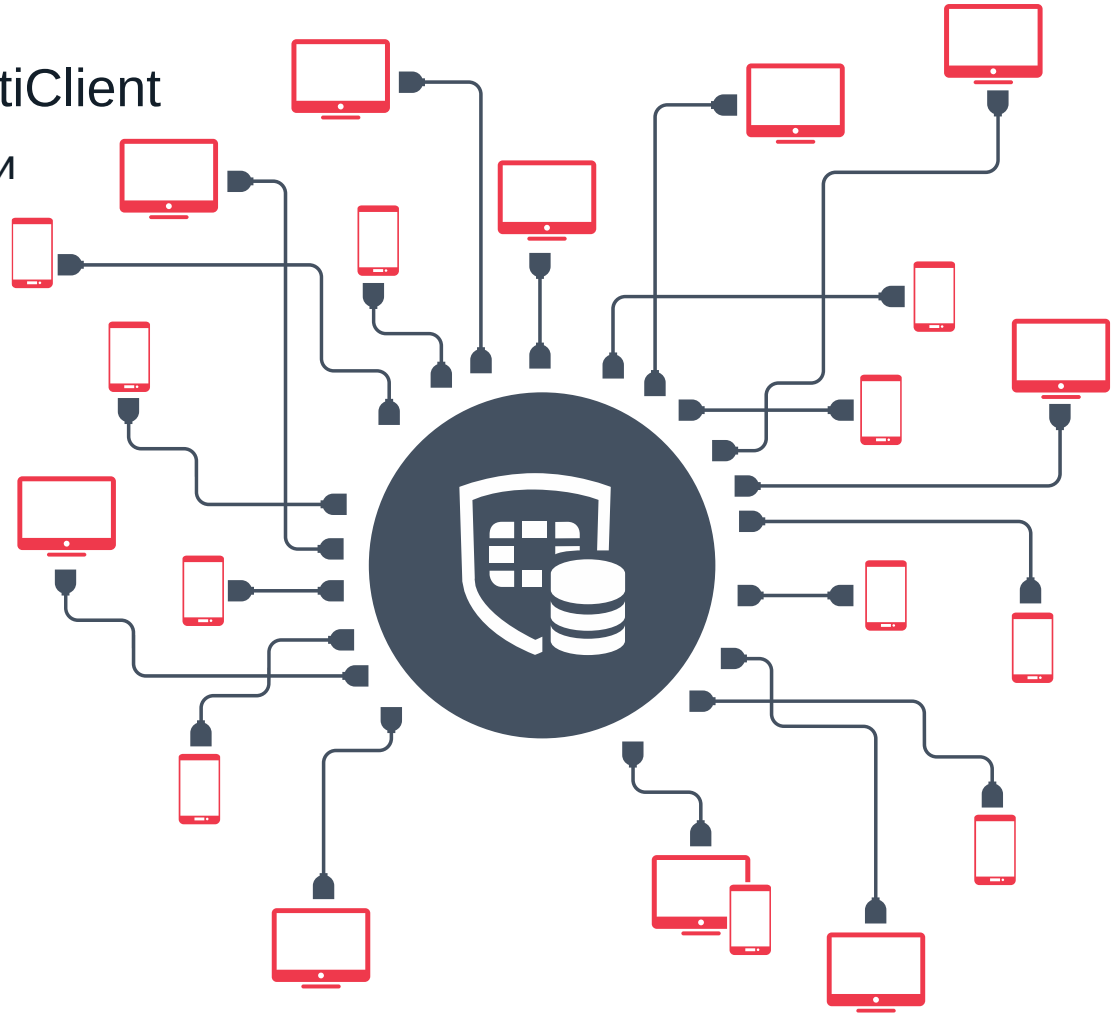
Enterprise Management System (EMS)

- EMS – программное обеспечение устанавливаемое на Windows сервер, использующее в качестве базы данных MS SQL сервер, обеспечивающее централизованного управления клиентами FortiClient устанавливаемых на ОС Windows, Linux, MacOS, Android, iOS, Chromebook , интегрируемый в Fortinet Security Fabric и обеспечивающий простое и эффективное управление угрозами предприятия, в том числе с использованием API
- EMS сервер бывает облачный Cloud EMS, в виде SaaS сервиса FortiClient Cloud и местный EMS сервер.
  - **Облачный EMS** сервер можно развернуть самостоятельно используя любое публичное облако, на котором будет развернут Windows сервер на который вы установите EMS сервер.
  - **SaaS сервис FortiClient Cloud** это EMS сервер развернутый в облаке Fortinet, который вы используете как сервис.
  - **On-prem EMS** это обычная установка на локальный Windows сервер

Система централизованного управления FortiClient

Enterprise Management System (EMS)

- Подготовка и развертывание дистрибутивов FortiClient
  - Интеграция с AD и другими корпоративными системами
- Оценка соответствия политикам безопасности
- Мониторинг клиентов в реальном времени
- Сводка по угрозам, оповещения
- Управление клиентами, в т.ч.
  - Сканирование на ВПО
  - Сканирование на уязвимости
  - Помещение в карантин
- Инвентаризация ПО
- Масштабируемое решение



FORTINET

FortiClient Cloud

FortiClient Cloud

EMS FortiClient сервер поставляемый как SaaS

- **Ограничения FortiClient Cloud EMS сервера по сравнению с локальным EMS сервером:**
  - FortiClient Cloud не поддерживает интеграцию с Active Directory
  - FortiClient Cloud не может управлять FortiClient для Chromebook
  - Максимальное количество клиентов FortiClient 5000 (в ближайшее время данное ограничение устранят)
  - Нет некоторых пунктов меню (резервное копирование/восстановление)
  - Поддержка версии FortiClient клиентов начиная с 6.2.1 и более поздних версий

- **Все остальные функции поддерживаются!**

FortiClient Cloud

EMS FortiClient сервер поставляемый как SaaS. Функционал:

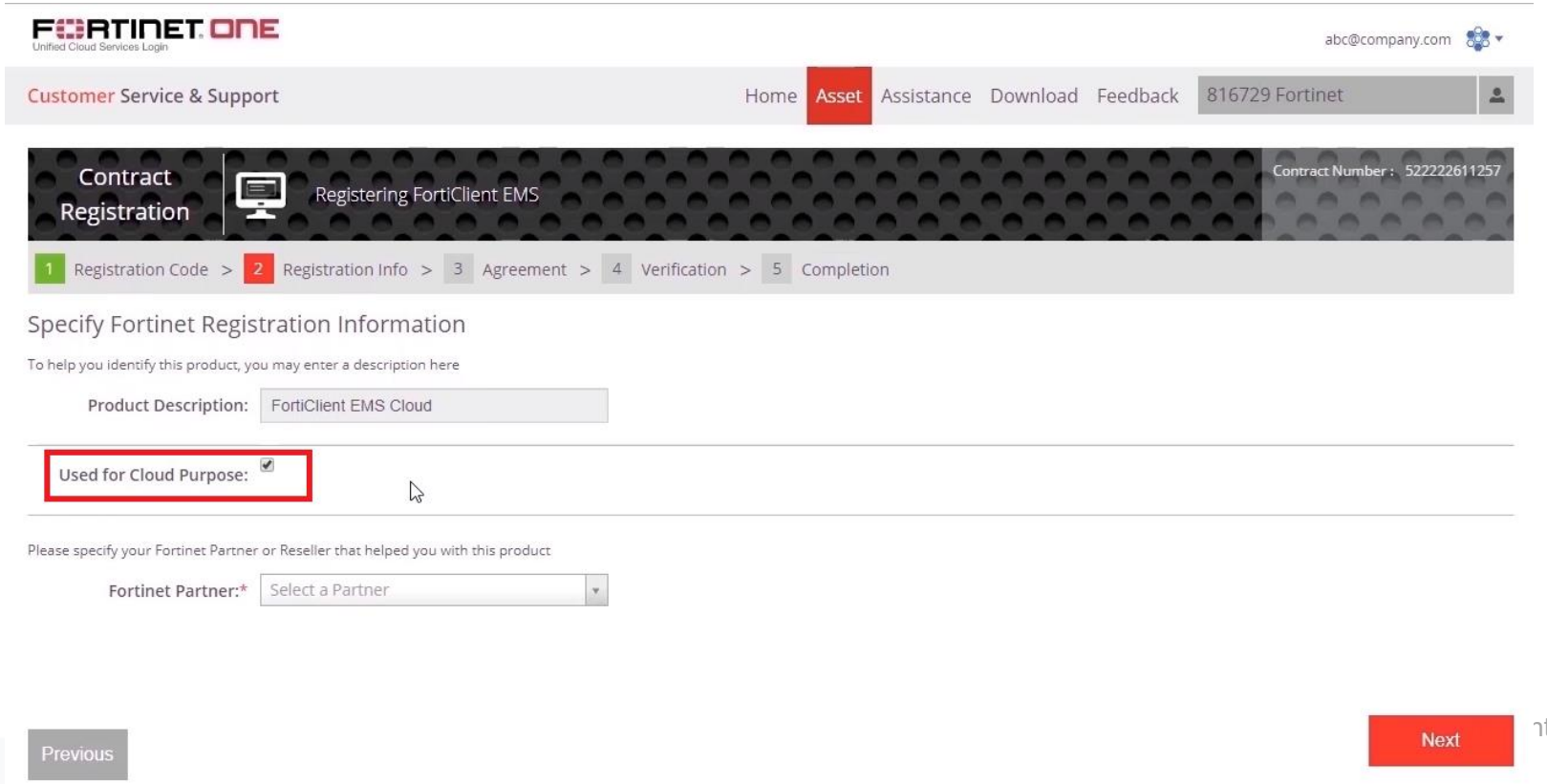
- Fabric Telemetry
- Antivirus real time protection
- Remote access (IPsec and SSL VPN)
- Sandbox Protection
- Web Filter
- Application Firewall
- SSO
- Cloud-based threat detection
- Anti-exploit engine
- USB device control
- Vulnerability management
- FortiGate Fabric connectors
- Software Inventory

Все остальные функции поддерживаются!

FortiClient Cloud

FortiClient Cloud. Как создать экземпляр:

1. Регистрация FortiClient Cloud подписки на свою учетную запись FortiCloud
2. Регистрация лицензии FortiClient на созданную учетную запись FortiCloud



FortiClient Cloud

FortiClient Cloud. Как создать экземпляр:

1. Регистрация FortiClient Cloud подписки на свою учетную запись FortiCloud
2. Регистрация лицензии FortiClient на созданную учетную запись FortiCloud

Видео. FortiClient Cloud быстрый старт.

https://vimeo.com/363936010

Документация FortiClient Cloud

https://docs.fortinet.com/document/forticlient-cloud/6.2.0/cloud-deployment/681910/introduction

Ресурсы

Дополнительные ресурсы

FortiClient EMS

Дистрибутив: https://www.forticlient.com/downloads

Активация пробной лицензии:
https://video.fortinet.com/latest/forticlient-trial-license

Бесплатный VPN клиент FortiClient

Онлайн инсталляторы: https://forticlient.com/downloads

Оффлайн инсталляторы: https://support.fortinet.com/

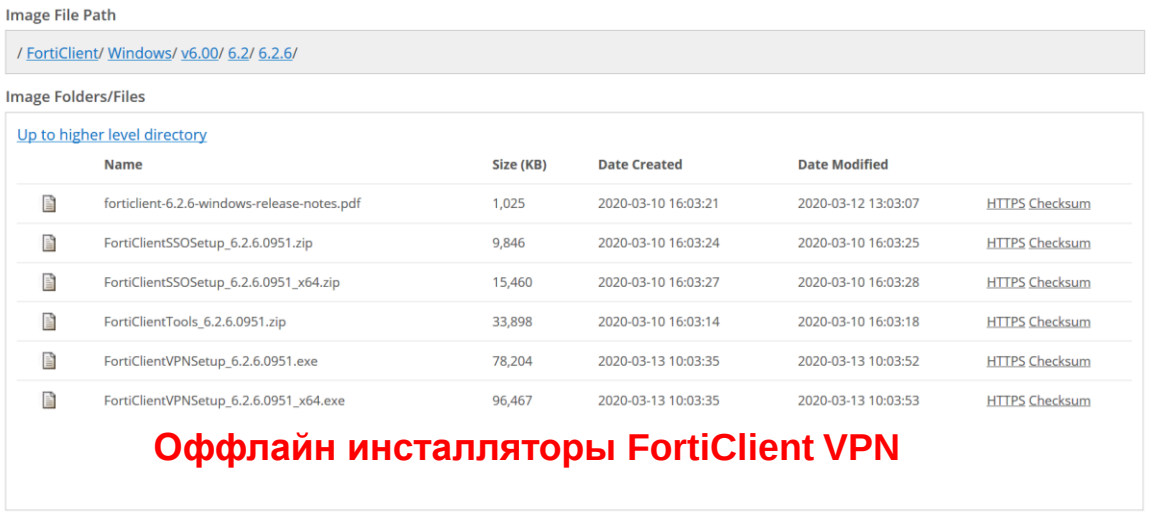


Image File Path

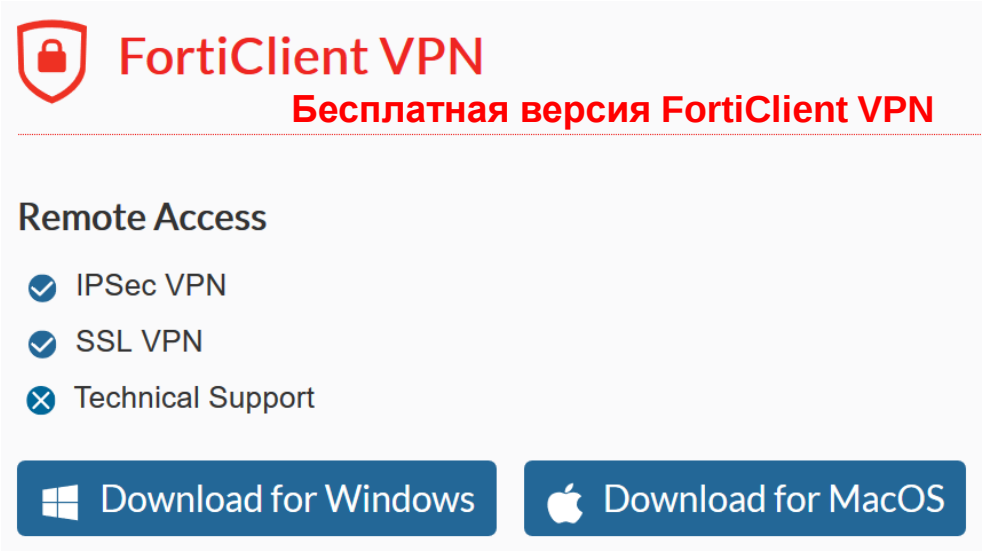
/ FortiClient/ Windows/ v6.00/ 6.2/ 6.2.6/

Image Folders/Files

Up to higher level directory

Name	Size (KB)	Date Created	Date Modified	
forticlient-6.2.6-windows-release-notes.pdf	1,025	2020-03-10 16:03:21	2020-03-12 13:03:07	HTTPS Checksum
FortiClientSSOSetup_6.2.6.0951.zip	9,846	2020-03-10 16:03:24	2020-03-10 16:03:25	HTTPS Checksum
FortiClientSSOSetup_6.2.6.0951_x64.zip	15,460	2020-03-10 16:03:27	2020-03-10 16:03:28	HTTPS Checksum
FortiClientTools_6.2.6.0951.zip	33,898	2020-03-10 16:03:14	2020-03-10 16:03:18	HTTPS Checksum
FortiClientVPNSetup_6.2.6.0951.exe	78,204	2020-03-13 10:03:35	2020-03-13 10:03:52	HTTPS Checksum
FortiClientVPNSetup_6.2.6.0951_x64.exe	96,467	2020-03-13 10:03:35	2020-03-13 10:03:53	HTTPS Checksum

Оффлайн инсталляторы FortiClient VPN



Как узнать о продукте FortiClient больше

- Просмотреть видеоролики ниже:
  - https://video.fortinet.com/products/forticlient/6.2/getting-started-with-ems-6-2-2-part-1
  - https://video.fortinet.com/products/forticlient/6.2/getting-started-with-ems-6-2-2-part-2
- Пройти курс обучения в институте Fortinet. Необходимо пройти короткую регистрацию:
  - https://training.fortinet.com/login/signup.php?

    Название курса «FortiClient EMS». Курс будет доступен всем желающим до конца 2020 года.
- **Fast Track** курс совместно с инструктором от Fortinet в виртуальной лаборатории Fortinet.

  Бесплатный курс позволяющий ознакомиться с функционалом FortiClient EMS в течении одного дня.
- Ознакомиться с документацией на сайте :
  - https://docs.fortinet.com/product/forticlient/6.4
  - https://docs.fortinet.com/product/forticlient-cloud/6.2

- Сформулировать вопросы и послать их по почте на адрес Russia@fortinet.com
- Запросить лицензии для тестирования написав по адресу Russia@fortinet.com , после регистрации оценочной лицензии через портал support.fortinet.com задать свой вопрос технической поддержке
- Поискать ответы на вопросы в базе знаний kb.fortinet.com

Как протестировать решение

Как развернуть пилот с использованием локального FortiClient EMS сервера

Для развертывания системы централизованного управления EMS FortiClient и клиентов FortiClient:

1. Пройти по ссылке: https://www.forticlient.com/downloads . Заполнить анкету, скачать дистрибутив сервера EMS.

2. Произвести установку сервера EMS.

3. Активировать триальную лицензию как показано в видеоролике по ссылке ниже: https://video.fortinet.com/latest/forticlient-trial-license

4. Развернуть решение и сделать первоначальную настройку указано в видео ниже:

   https://video.fortinet.com/products/forticlient/6.2/getting-started-with-ems-6-2-2-part-1

   https://video.fortinet.com/products/forticlient/6.2/getting-started-with-ems-6-2-2-part-2

5. Запросить необходимо количество лицензий в случае необходимости написав письмо на Russia@fortinet.com

Как развернуть пилот используя FortiClient Cloud сервера

Для развертывания системы централизованного управления FortiClient Cloud и клиентов FortiClient:

1. Просмотреть видео https://video.fortinet.com/products/forticlient-ems/6.2/forticlient-cloud-overview

2. Cloud EMS могут тестировать владельцы FortiCloud Premium Account подписки (FC-15-CLDPS-219-02-DD)

   Поэтому необходимо купить данную подписку или обратиться по адресу Russia@fortinet.com

3. Необходимо запросить лицензии FortiClient Security Fabric Agent написав по адресу Russia@fortinet.com указав количество клиентов. Отдельно необходимо указать количество клиентов Chromebook

4. После получения лицензий необходимо активировать подписку FortiCloud Premium Account и лицензии FortiClient Security Fabric как указано в видео выше

5. Дальнейшую настройку можно выполнив как указано в видеороликах доступных по ссылкам ниже:

   https://video.fortinet.com/products/forticlient/6.2/getting-started-with-ems-6-2-2-part-1

   https://video.fortinet.com/products/forticlient/6.2/getting-started-with-ems-6-2-2-part-2

Изменения

FortiClient

Совместимость между различными версиями продуктов

FortiClient	FortiClient EMS	FortiOS		FortiAnalyzer	FortiManager	FortiSandbox
		Endpoint control	IPsec VPN SSL VPN			
6.0.0	6.0.0+ 6.2.0+	5.6.0+ 6.0.0+	5.4.0+ 5.6.0+ 6.0.0+ 6.2.0+ 6.4.0	5.6.0+ 6.0.0+ 6.2.0+	5.6.0+ 6.0.0+ 6.2.0+	2.1.0+ 2.2.0+ 2.3.0+ 2.4.0+ 2.5.0+ 3.0.0+
6.0.1+						2.1.0+ 2.2.0+ 2.3.0+ 2.4.0+ 2.5.0+ 3.0.0+ 3.2.0
6.2.0	6.2.0+ 6.4.0	6.2.0+	5.6.0+* 6.0.0+* 6.2.0+ 6.4.0	6.0.0+ 6.2.0+	6.0.0+ 6.2.0+	2.5.0+ 3.0.0+ 3.1.0+ 3.2.0
6.2.1+				6.2.0+	6.2.0+	
6.4.0	6.4.0	6.2.0+ 6.4.0	6.0.0+ 6.2.0+ 6.4.0	6.4.0	6.4.0	

- Документ доступен на портале https://docs.fortinet.com

https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/25db317f-031e-11e9-b86b-00505692583a/fct-compatibility-chart.pdf

FortiClient: для изолированных сред

- Появилась возможность установки FortiClient и сервера EMS в изолированных средах, без доступа к Интернет
  - Включает **регистрацию** ForiClient и EMS для автономных сред
  - Полностью **автономный дистрибутив для** FortiClient EMS инсталлятора
  - Обновление версий FortiClient и **сигнатур** через FortiManager для изолированных сред
  - FortiClient поддержка для Windows **Server Core** 2019 и 2016

FortiClient: как можно протестировать

Доступны лицензии для тестирования большого количества клиентов

- EMS On-prem → EMS для **FortiCloud Account** позволяет использовать 30 дневную лицензию на 10 клиентов
  - Используя FortiCare учетную запись можно получить **одну** EMS пробную лицензию самостоятельно
- EMS **On-Prem или Cloud**: 60 дней, неограниченное количество клиентов
  - Доступна версия FortiClient с облачной и местной песочницей и поддержкой FortiClient для Chromebook, Linux, MacOS, Windows, Mobile OS (Android, iOS)
  - Для тестирования FortiClient совместно с облачным вариантом сервера EMS Cloud, необходимо выбрать EMS Cloud вариант при **регистрации лицензии FortiClient**. Требуется наличие **FortiOne Premium учетной записи**, купить можно используя SKU FC-15-CLDPS-219-02-02

Угрозы с которыми сталкиваемся при обслуживании конечных устройств

Проблемы с которыми сталкивается каждая компания

Ponemon INSTITUTE

63% всех компаний не могут контролировать конечные устройства вне сети, более половины не могут определить состояние соответствия конечных устройств

ОТСУТСТВИЕ ВИДИМОСТИ

verizon

4%
людей участвуют в любой фишинговой кампании, нажимая все подряд

ДОВЕРЧИВЫЕ ПОЛЬЗОВАТЕЛИ

99% эксплуатируемых уязвимостей известны специалистам по безопасности и ИТ-специалистам

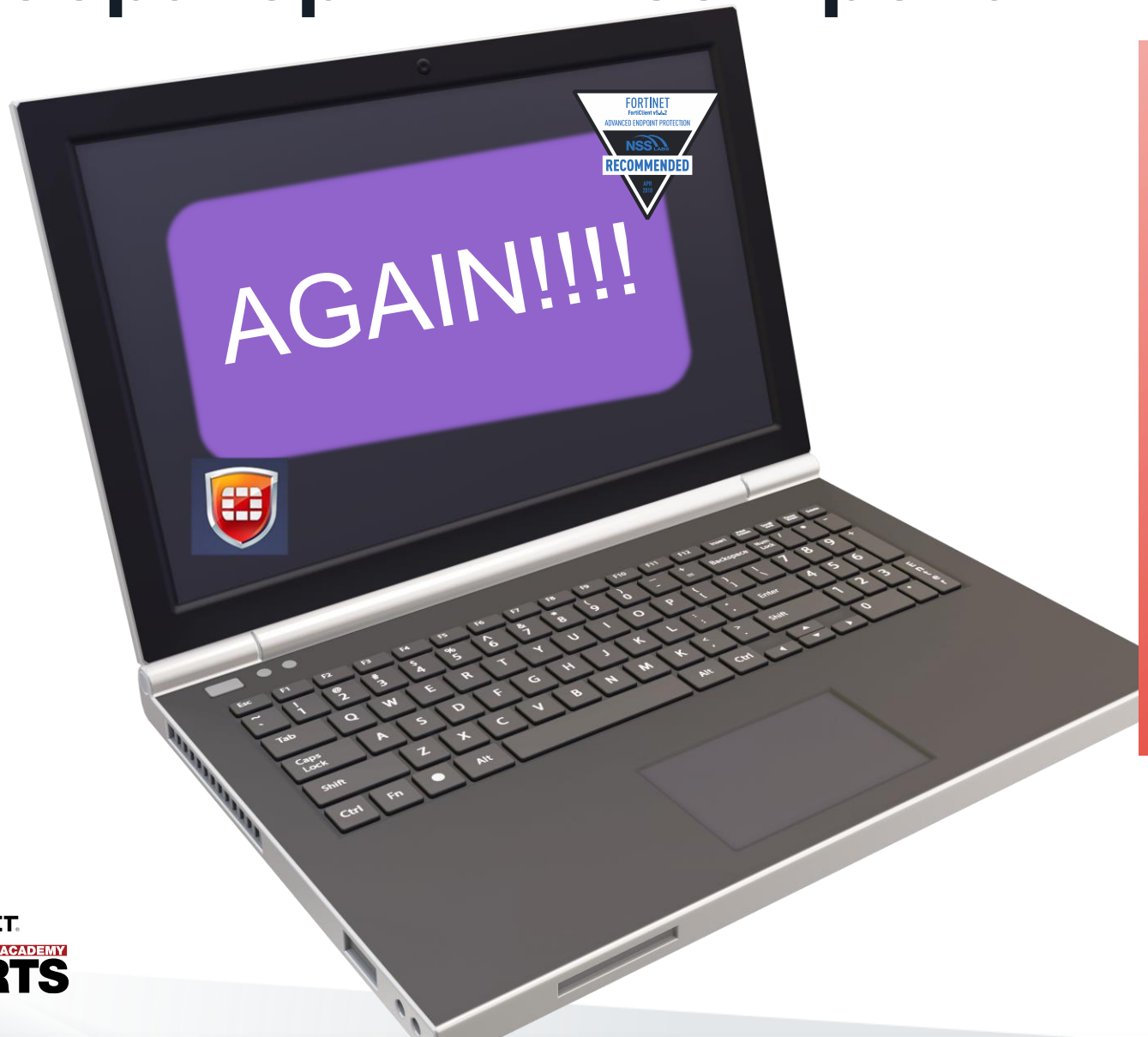
УЯЗВИМЫЕ УСТРОЙСТВА

Источники:

1. Стоимость небезопасных конечных устройств, Ponemon Institute, 2017
2. Гартнер, «Как реагировать на угрозу 2018 года», Грег Янг, 28 ноября 2017 года
3. Отчет о расследовании нарушений, Verizon, 2018

Результаты независимых тестирований!

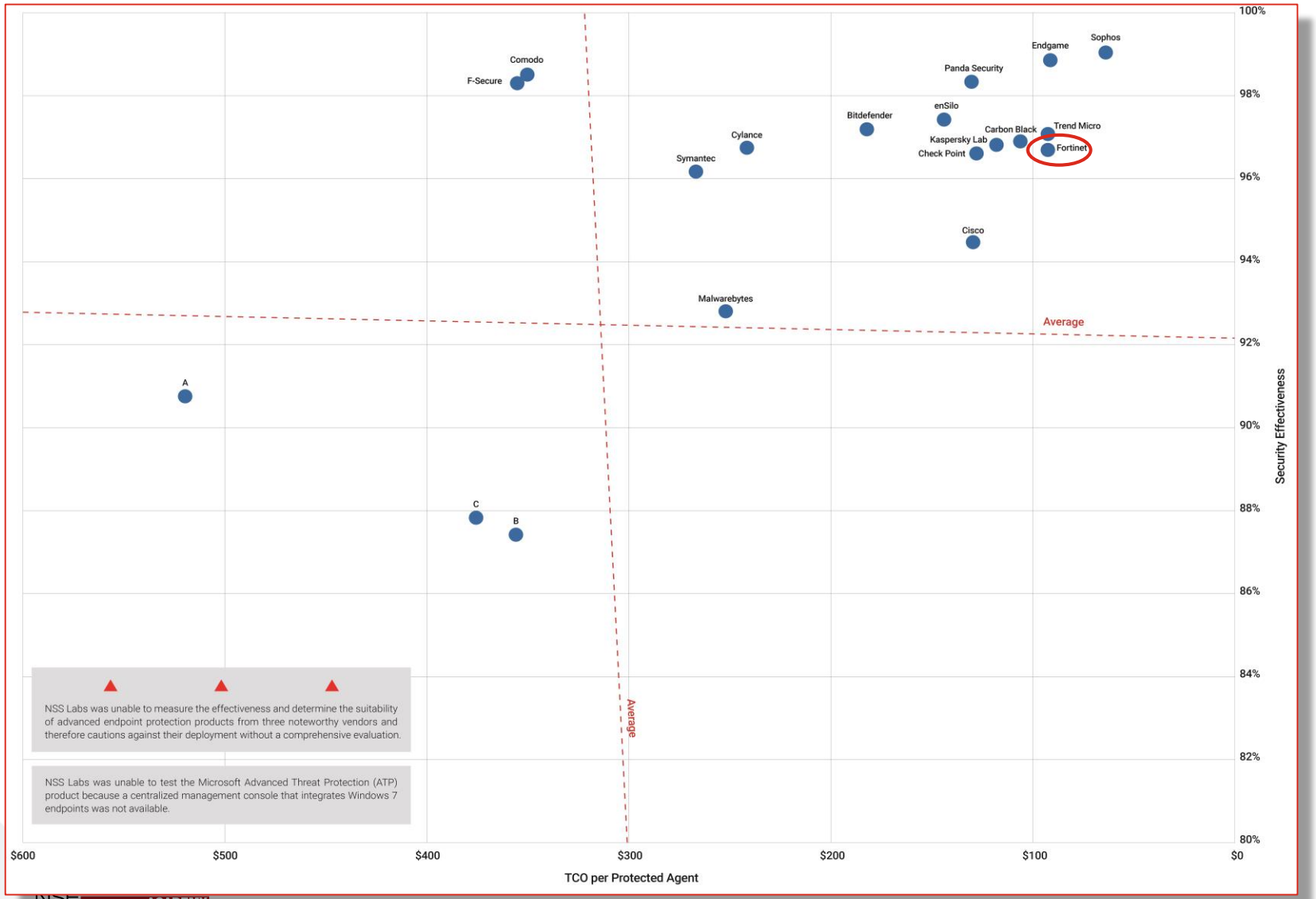
FortiClient рекомендован ведущими лабораториями тестирования



- 4 года подряд
- Лучшая стоимость ТСО при использовании облачной песочницы
- Один из лидеров в квадрате
- Усиление позиции на рынке

FORTINET NSE ACADEMY XPERTS

AEP 3.0 Security Value Map 2019



FORTINET
FortiClient v5.6.2
ADVANCED ENDPOINT PROTECTION
NSS LABS
RECOMMENDED
APR 2018

21 продукт тестировался

19 вендоров показано

14 рекомендовано

2 Security рекомендованы

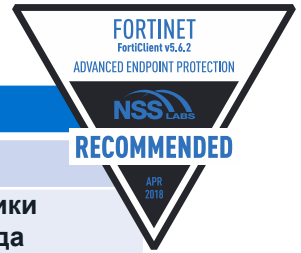
3 продукта не прошли тест

Security эффективность 87.4 - 99.1%

6 вендоров пропустили хотя бы одну технику обхода, уязвимость

NSE ACADEMY
XPERTS

FortiClient Рекомендован



Продукт						3-летний TCO – 2500 агентов (US$)		
Fortinet FortiClient v. 6.0.3 с EMS						$44,009		
	HTTP	Email	Документы & Скрипты	Offline Угрозы	**Неизвестные Угрозы**	**Эксплойты**	Смешанные Угрозы	**Техники обхода**
Уровень блокирования	100%	98.5%	91.9%	93.3%	**100%**	**100%**	50%	**100%**
Дополнительный уровень обнаружения	0%	.3%	6.5%	6.7%	**0%**	**0%**	%	**0%**
Итого	**100%**	98.8%	98.4%	**100%**	**100%**	**100%**	50%	**100%**

Общий бал за функционал
97.5

Security эффективность:
96.7%

FORTINET NSE ACADEMY XPERTS

Самые сложные и опасные угрозы блокируются 100%

Malware

33,653 Unique Variants

6,405 Different Families

13.7 Variants Seen per Firm

Эксплойты

8,309 Unique Exploit Detections

1,218 Exploits Seen per Firm

54% Firms who saw Severe Exploits

FORTINET NSE ACADEMY XPERTS

Дополнительная информация

Security Эффективность

Блокировка и обнаружение:

100% Эксплойты
100% Неизвестные угрозы
100% Техники обхода
100% Http malware
100% off line угрозы

В каких проверках были пропуски

Документы и скрипты 98.4% (1/62)
Смешанные угрозы 50% (7/14)

Нет 100% защиты для Endpoint
Глубокая защита и интеграция имеют решающее значение

Примеры вендоров кто пропустил угрозы

ESET Endpoint Protection
G DATA Endpoint Protection
McAfee Endpoint Protection
Palo Alto Networks Traps
SentinelOne
Fire Eye

Security эффективность в пределах 87.4% - 99.1%
6 вендоров пропустили одну или более техник обхода

FORTINET NSE ACADEMY XPERTS

FortiClient – результаты независимых тестирований

Результаты тестирования NSS LABS AEP 4.0 FortiClient

25 февраля, 2020

- NSS labs изменила свой метод отчетности для теста Advanced Endpoint Protection (AEP). Вместо Security Value Map (SVM), теперь NSS labs указывает для каждого участника уровень рейтинга от AAA, AA, A, BBB, BB до B.

- Первый раунд: **12+ участников** производителей AEP. FortiClient v6.2.2 был присвоен уровень A. Для FortiEDR был присвоен уровень AA.

- FortiClient заблокировал **97.37% угроз** с **0.6% ложных** срабатываний.

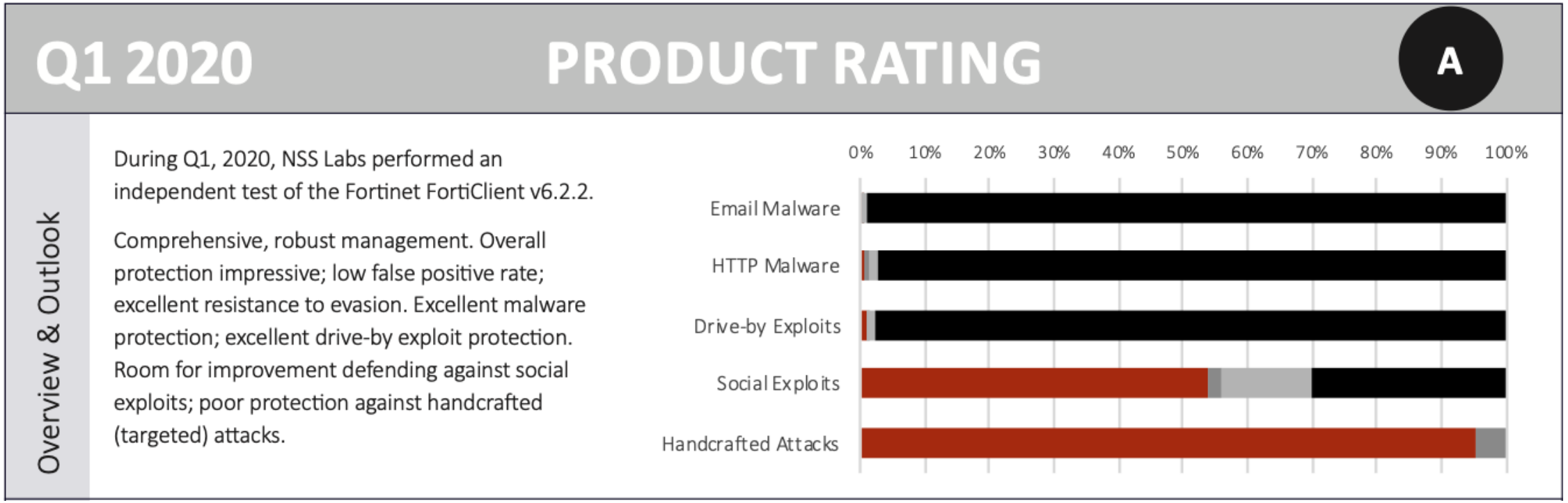
- Среди участников, Kaspersky, Bitdefender, Checkpoint, PAN Traps….и т.д.

- Тестирование продолжается. Рейтинги будут меняться со временем

- Большая выявленных проблем FCT уже исправлена, окончательное исправление будет в версии 6.4.1 которое выйдет в середине июля.

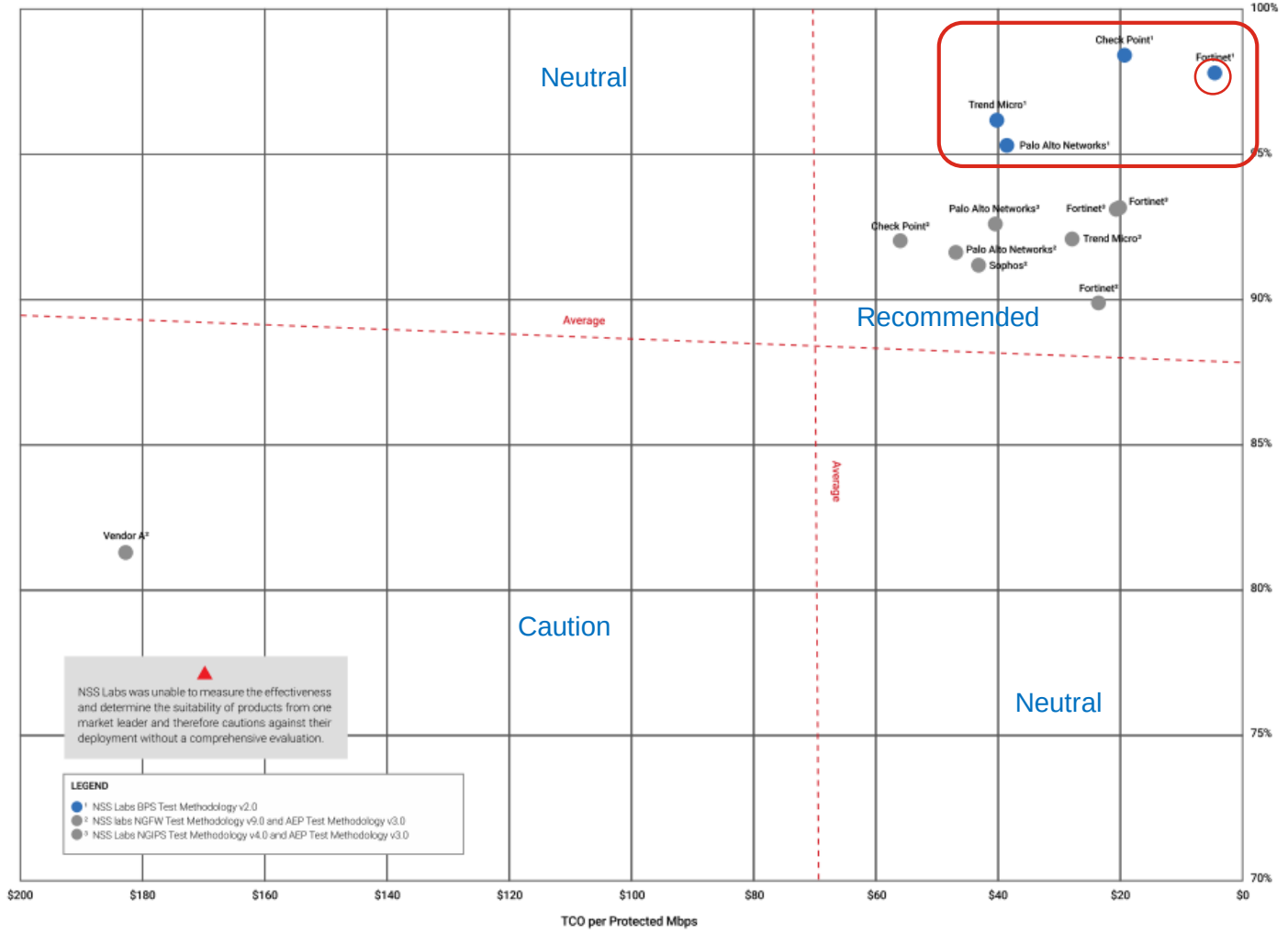
Результаты тестирования NSS LABS AEP 4.0 FortiClient

25 февраля, 2020



Security Value Map (SVM), Декабрь 2019

- Рекомендованы решения 4 вендоров:
  - **Check Point** Software Technologies Next Generation Threat Prevention Appliance + Endpoint Security
  - **Palo Alto Networks** PA-5220 + Traps
  - **Trend Micro** TippingPoint 8200TX Appliance + Deep Discovery Analyzer + OfficeScan
  - **Fortinet** Fortinet FortiGate 500E + FortiClient + FortiSandbox (AWS BYOL)



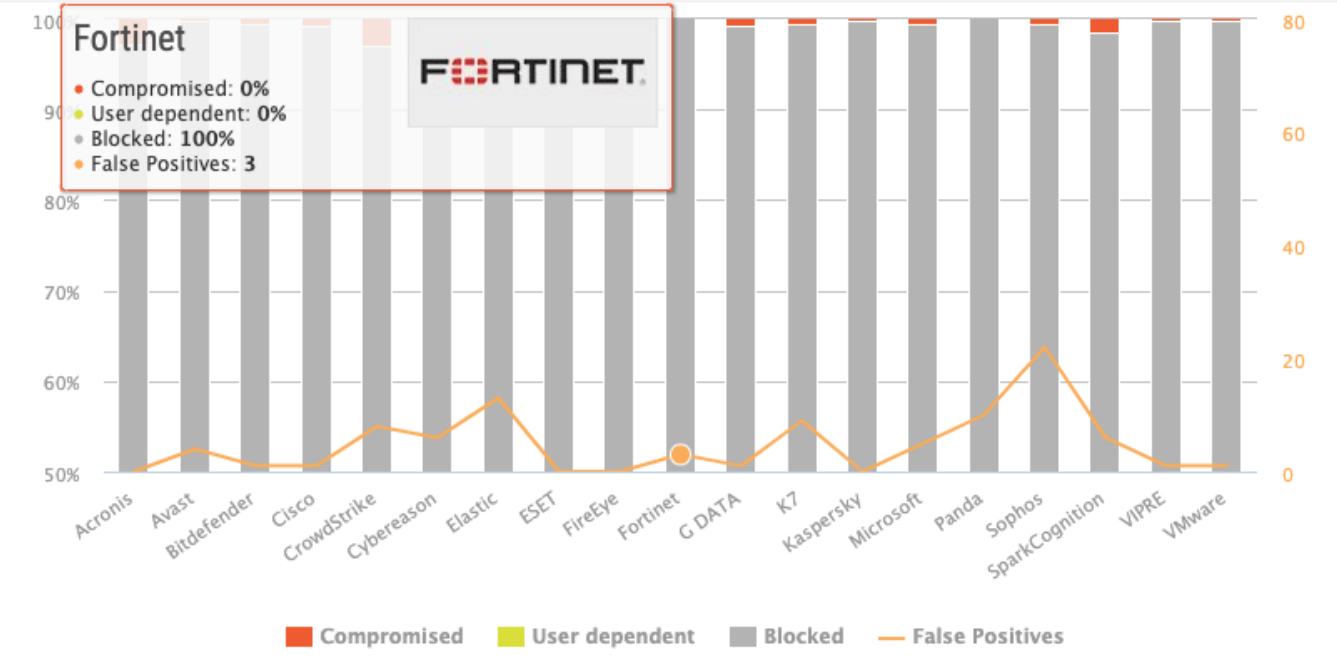
NSS Labs BPS SVM, **Dec 2019**

AV-Сравнительный отчет, март/апрель 2020

Test Results

Real-World Protection Test (March-April)

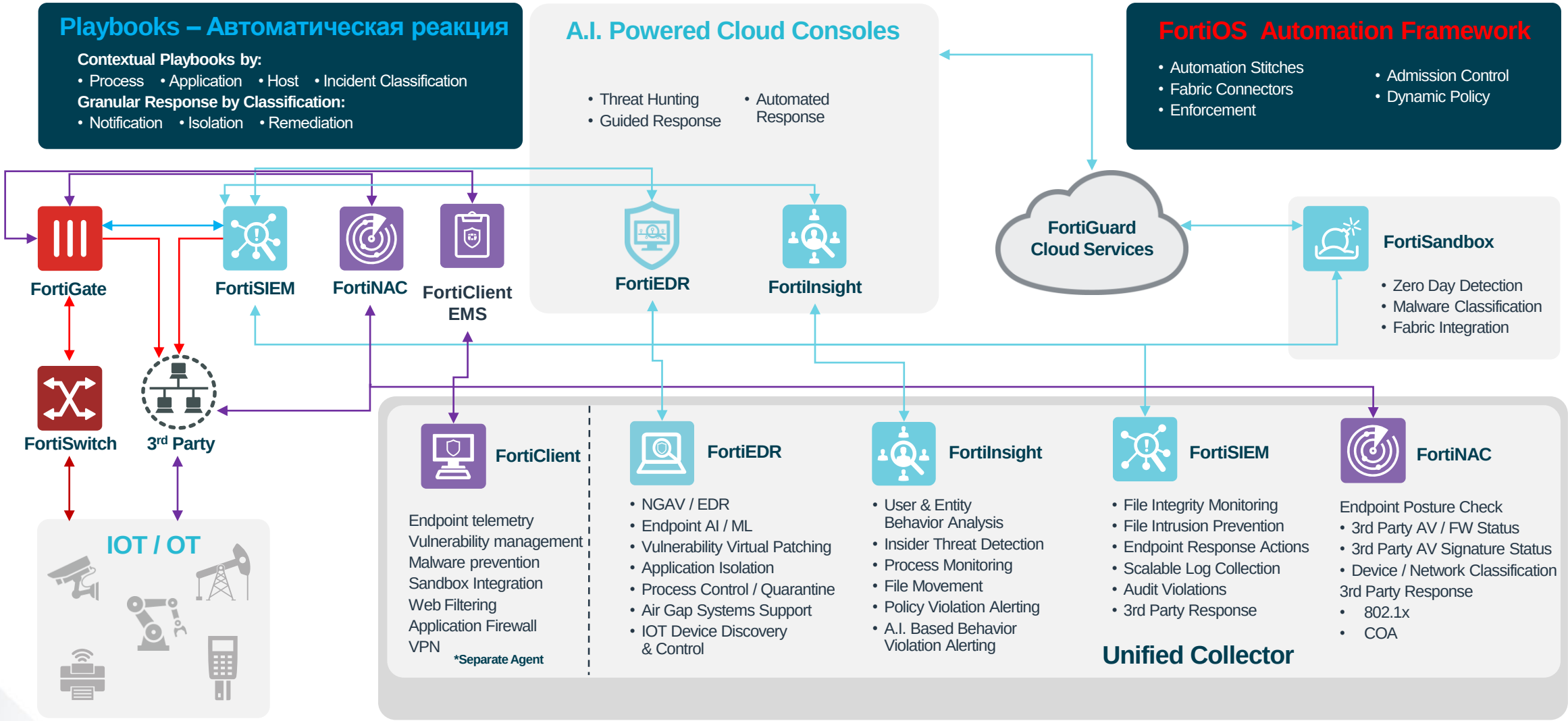
This fact sheet gives a brief overview of the results of the Business Real-World Protection Test run in March and April 2020. The overall business product reports (each covering four months) will be released in July and December. For more information about this Real-World Protection Test, please read the details available at https://www.av-comparatives.org. The results are based on a test set consisting of **403** test cases (such as malicious URLs), tested from the beginning of March till the end of April.



- **Участники**: очень большая группа…
- Fortinet и Panda **Заняли первое место #1** среди всех участников.
- **Решение Fortinet** : FortiEDR, FortiClient и FortiSandbox.
- https://www.av-comparatives.org/tests/business-security-test-march-april-2020-factsheet/

Fortinet Endpoint Security Архитектура

Архитектура Fortinet Endpoint Security



6.2.3+ новый функционал

Новый функционал добавленный в 6.2.3+

Расширение Security Fabric

- **FortiClient Cloud лицензия**
  - FortiCloud Cloud лицензия необходима для использования облачного EMS сервера
  - Постоянная лицензия для тестирования продукта. Не для продуктива. Одна лицензия на одну учетную запись FortientOne

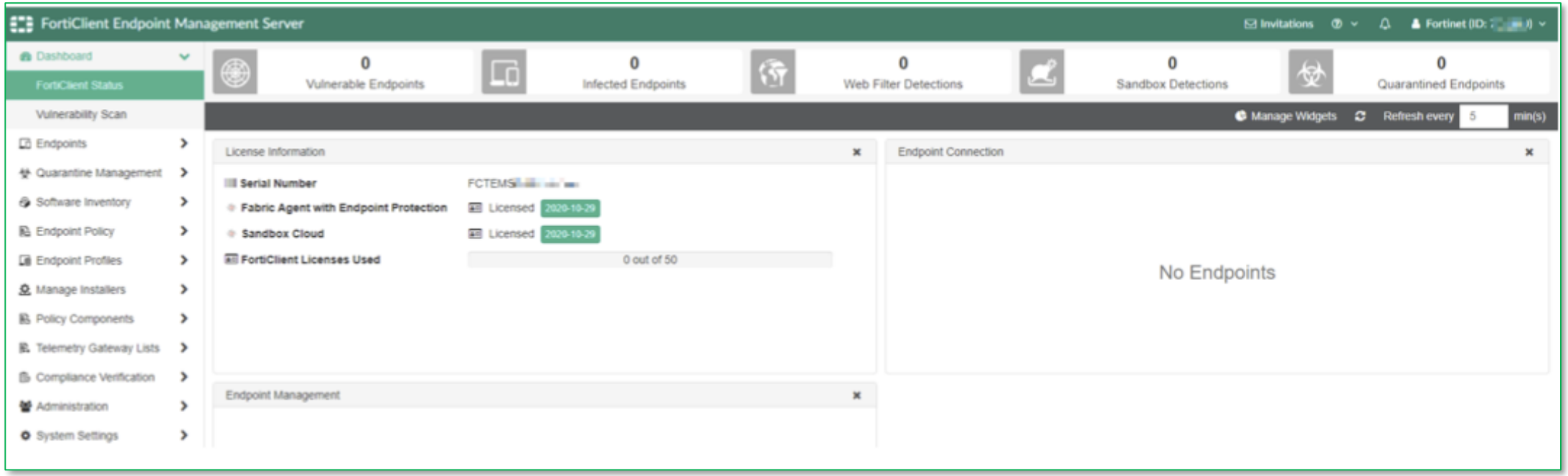
Интерфейс

- **SSL VPN on GUI FortiClient**
  - GUI для SSL VPN

FCT 6.2.3+: Изменения

FortiClient Cloud лицензия заменяет обе позиции ниже

- FortiCloud premium лицензия необходима для запуска FortiClient Cloud экземпляра
- Необходим контракт EMS FortiClient Fabric.



FCT 6.2.3+: лицензирование

Продлен срок действия триальной лицензии FortiClient с 30 дней до постоянной лицензии

- Каждая учетная запись FortientOne может иметь только **один тестовый экземпляр EMS**
- Ограничена **3 рабочими станциями,** Sandbox не включен в тестовую лицензию.
- **Нельзя использовать** для EMS с истекшим сроком лицензии
- Может быть Cloud или On-prem EMS

FCT 6.2.3+: некоторые замечания

Важно:

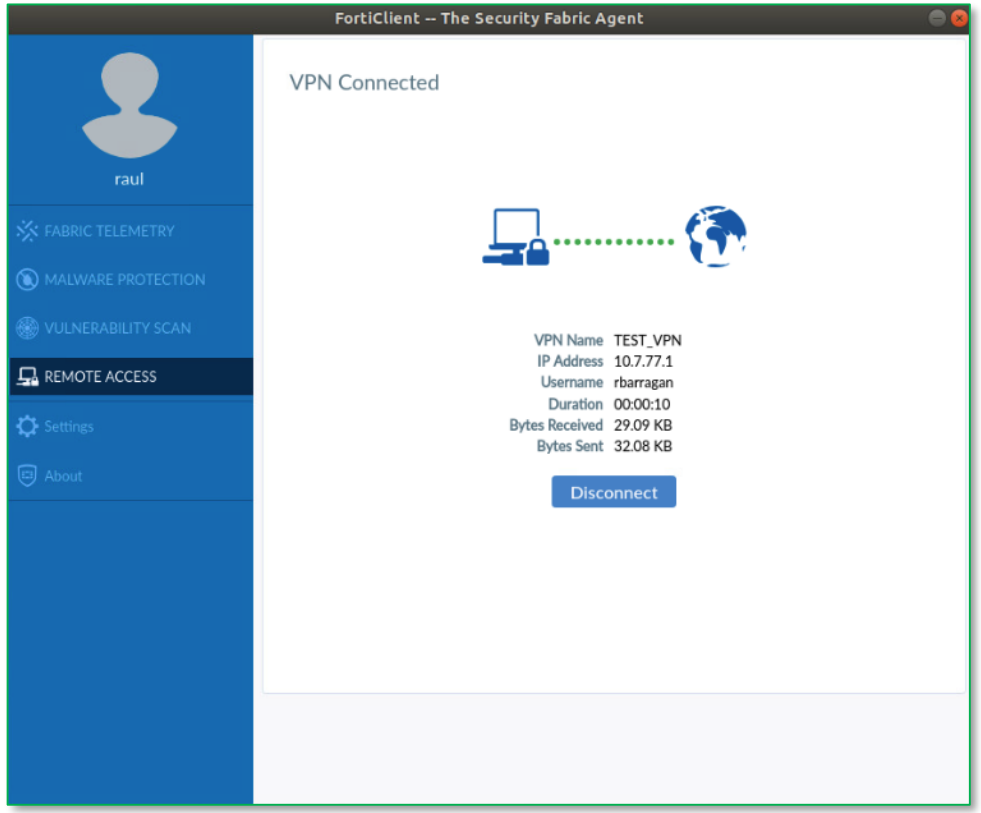
- Если на сервере уже установлена более новая версия Visual C ++ (VC) 2015, установка завершится неудачно
  - https://support.microsoft.com/en-us/help/4092997/vc-2015-redistributable-install-error-1638-when-newer-version-present

- **Заказчики с количеством рабочих станций более 5000**
  - Установить SQL Server Enterprise.
  - Рекомендуется использовать SQL Server 2017 или более позднюю версию.
  - https://docs.fortinet.com/document/forticlient/6.2.3/ems-administration-guide/665097

6.2.4 SSL VPN доступен через GUI FortiClient

FortiClient Linux

- SSL VPN поддерживается в GUI FortiClient Linux
- Команды Host check на данный момент не поддерживаются
- GUI Free VPN Linux клиент так же доступен
- 2FA пока реализован не полностью



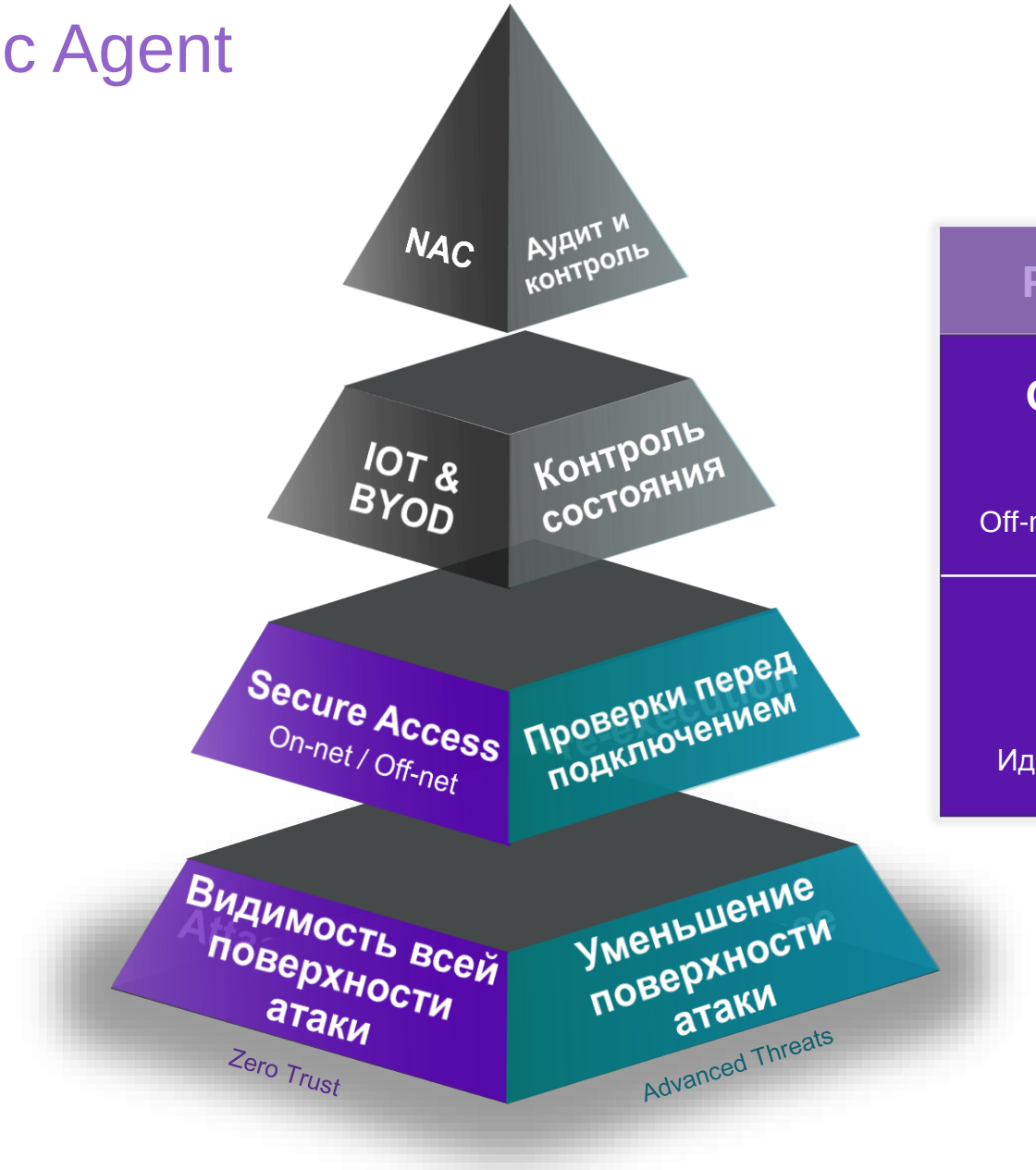
Новое в FotiClient 6.4

6.4.0

Fortinet Security Fabric обеспечивает цифровые инновации

Zero Trust Network Access

Fabric Agent



FABRIC AGENT	FABRIC AGENT
On-net / Off-net Контроль доступа 2FA аутентификация. Off-net профили безопасности	**EPP** Anti-Malware защита Защита от бестелесных угроз Sandboxing Web фильтрация
Видимость Пользователь Устройство Идентификаторы соц.сетей	**Уязвимость** Определение Автоматическое обновление

Zero-Trust Network Access

Сетевой доступ с нулевым уровнем доверия

Zero-Trust Network Access

Antimalware Scan Interface (AMSI) защита для Windows

Бестелесное злонамеренное ПО использует скрипты которые которые как правило зашифрованы или обфусцированы для предотвращения сканирования с целью загрузки исполняемого кода непосредственно в память без размещения файла в ФС рабочей станции. AMSI engine позволяет FortiClient сканировать все скрипты и файлы, загруженные непосредственно в память.

Пример поддерживаемых скриптов:

- PowerShell
- JScript
- VBScript
- JavaScript
- .NET Assembly loading
- WMI

Zero-Trust Network Access

Antimalware Scan Interface (AMSI) защита для Windows

Бестелесное злонамеренное ПО использует скрипты которые которые как правило зашифрованы или обфусцированы для предотвращения сканирования с целью загрузки исполняемого кода непосредственно в память без размещения файла в ФС рабочей станции. AMSI engine позволяет FortiClient сканировать все скрипты и файлы, загруженные непосредственно в память.

Пример поддерживаемых скриптов:

- PowerShell
- JScript
- VBScript
- JavaScript
- .NET Assembly loading
- WMI

Zero-Trust Network Access

Защита конечных точек с использованием AI/ML

Новый AV Engine (антивирусный механизм) усиленный механизмами AI (искусственный интеллект) и ML (машинное обучение) теперь включен в FortiClient. Механизм ML используется для обнаружения и предотвращения запуска вредоносных программ с акцентом на новые или неизвестные вредоносные программы. Новый механизм ML использует алгоритмы для анализа файлов Windows PE (exe,dll,sys и т.д.) и прогнозирования их безопасности или вредоносности.

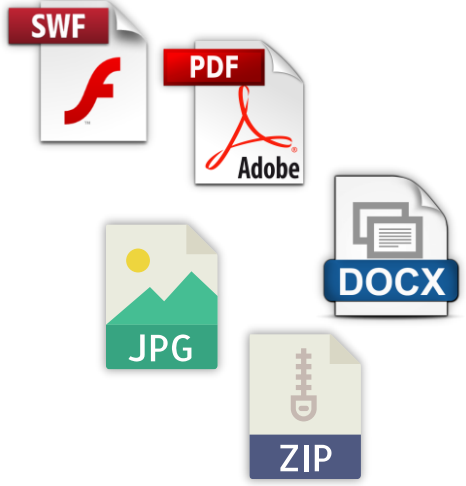
Это решение не использует проверку подписи приложений.

Zero-Trust Network Access

FortiSandbox Cloud поддержка для Mac

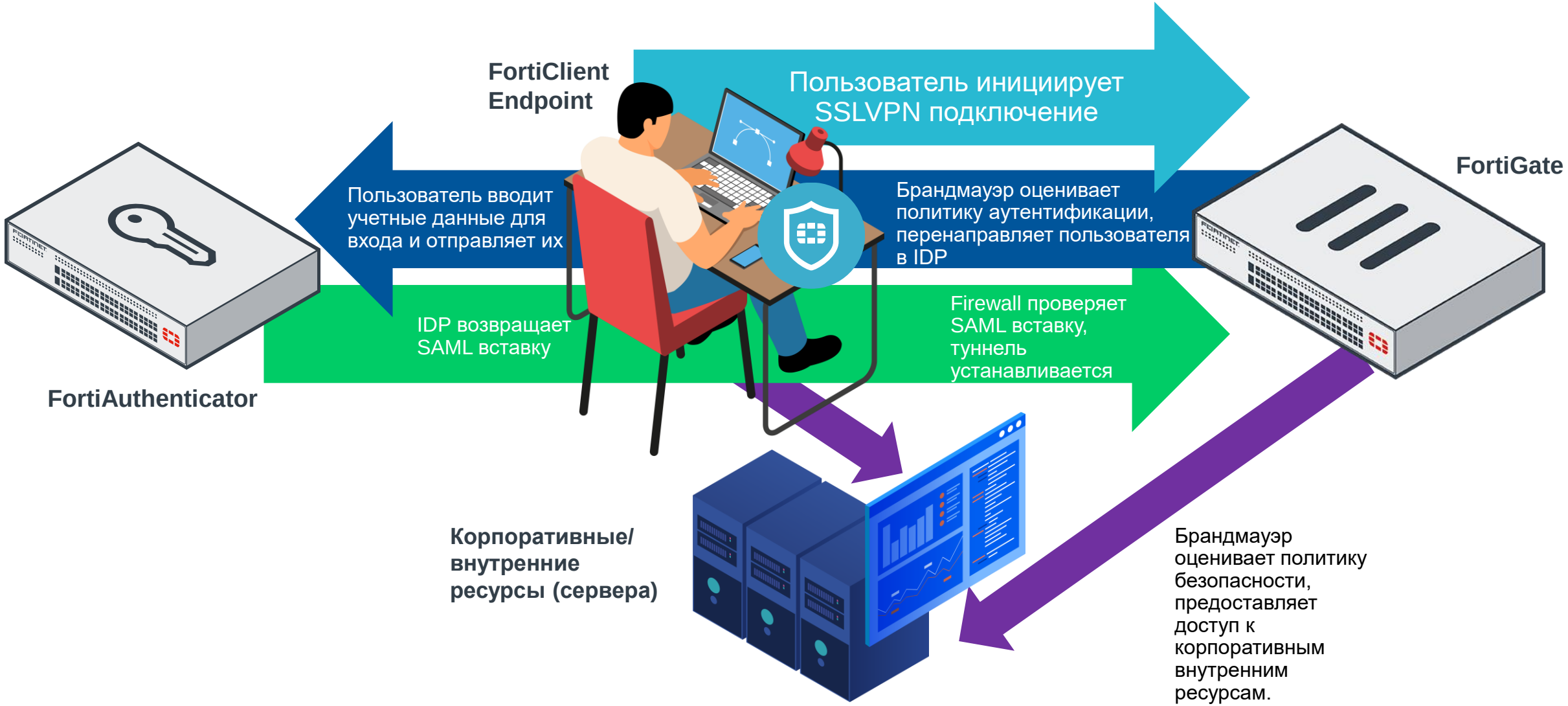
FortiClient Mac теперь поддерживает отправку загруженных файлов с высоким уровнем риска на FortiSandbox Cloud. Типы поддерживаемых файлов:

- PDF
- SWF
- DOC/DOCX/XLS/PPT
- JPG/PNG
- ZIP/RAR/TNEF



Zero-Trust Network Access

Поддержка SAML для SSLVPN



Zero-Trust Network Access

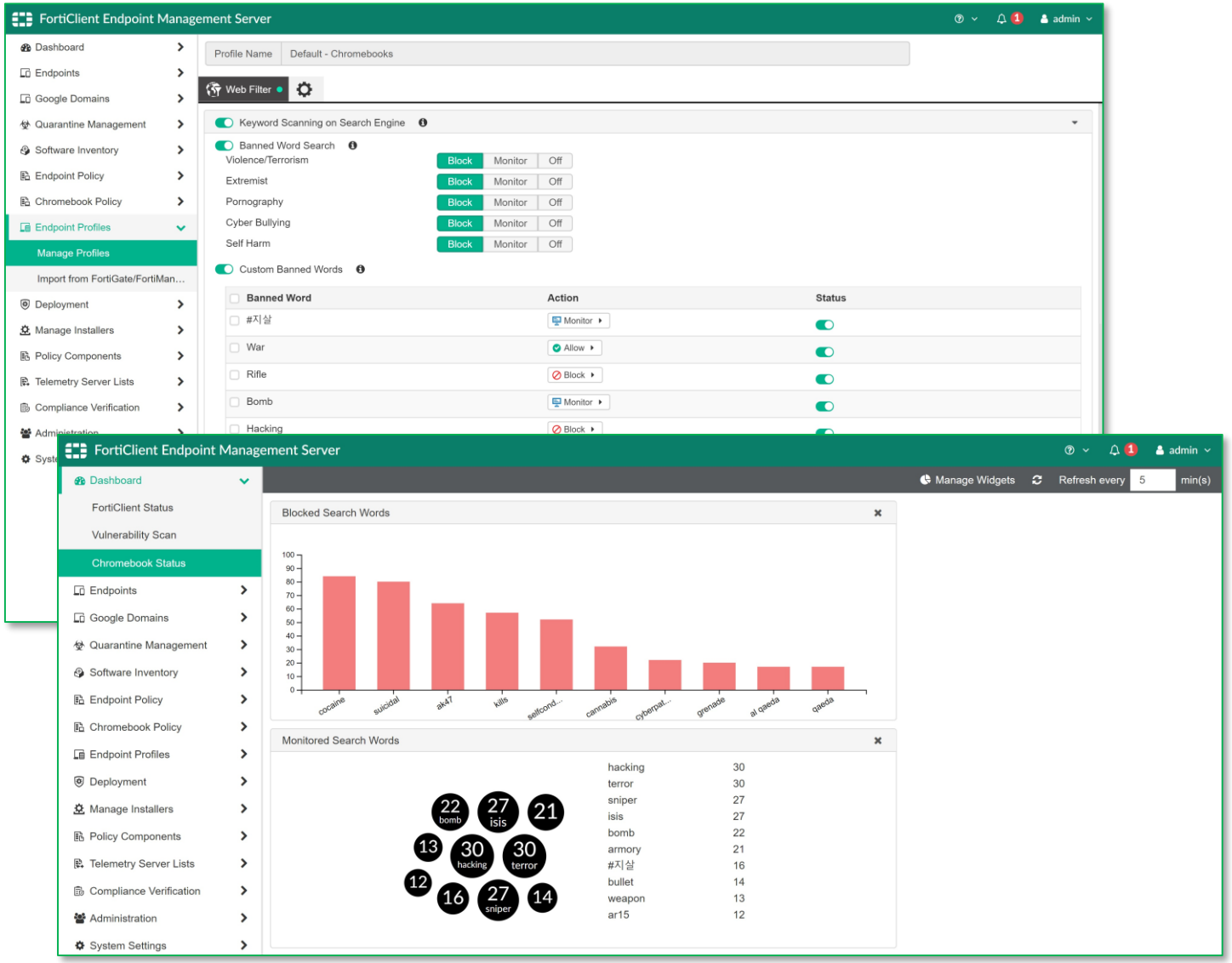
Content SafeGuard для Chromebook

Сканируется поисковое слово в популярных поисковых системах, чтобы заблокировать доступ к категориям:

- Cyber Bullying (кибер запугивание)
- Self Harm (причинение себе вреда)

- Поддержка Google, Yahoo, Bing, Youtube, Facebook, Twitter

- Статистика о самых популярных словах в поисковых запросах

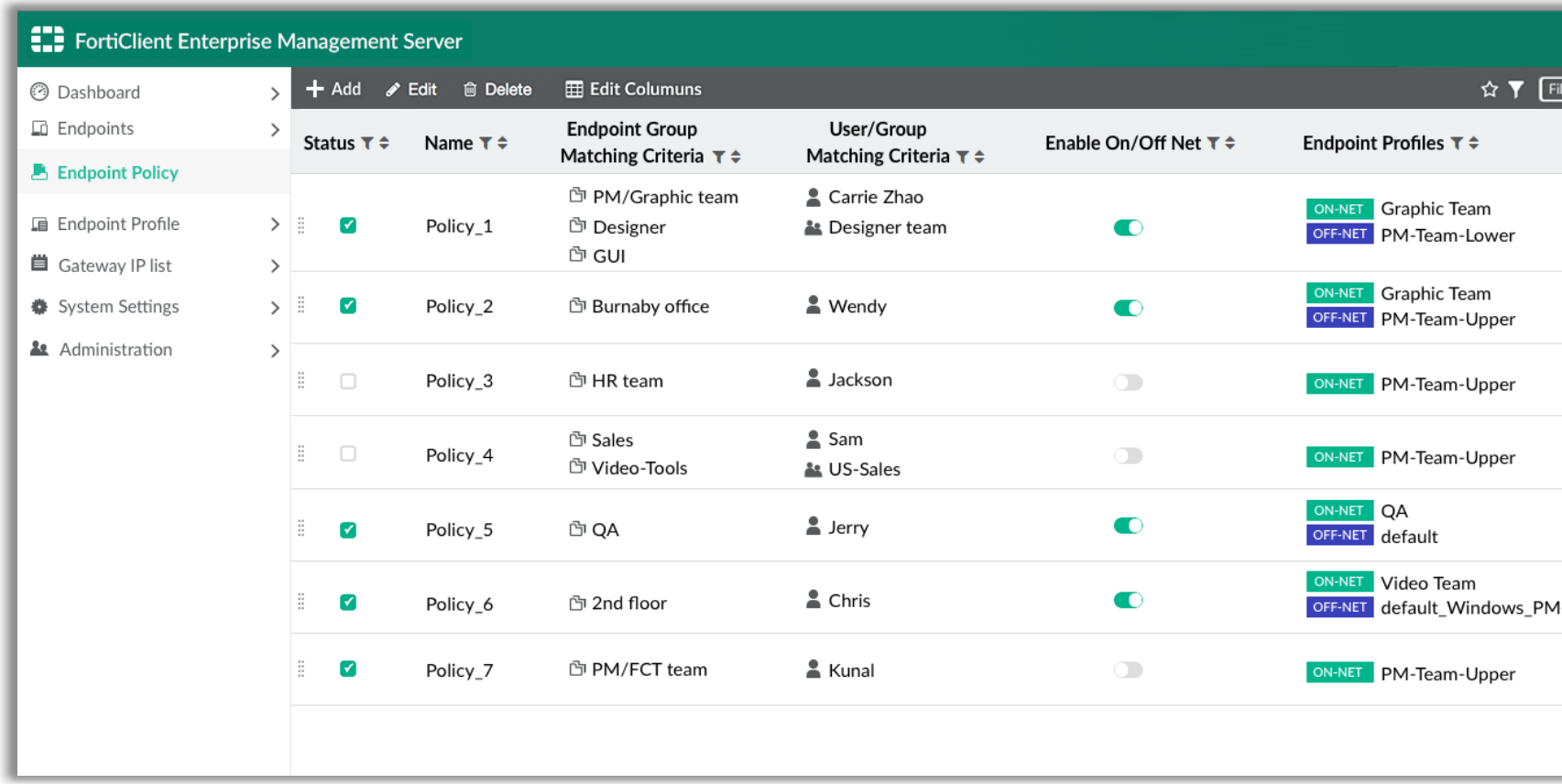


Zero-Trust Network Access

EMS поддерживает управление устройствами в зависимости от пользователя

FortiClient EMS теперь можно использовать для управления конечными точками на основе зарегистрированных пользователей, а не компьютеров.

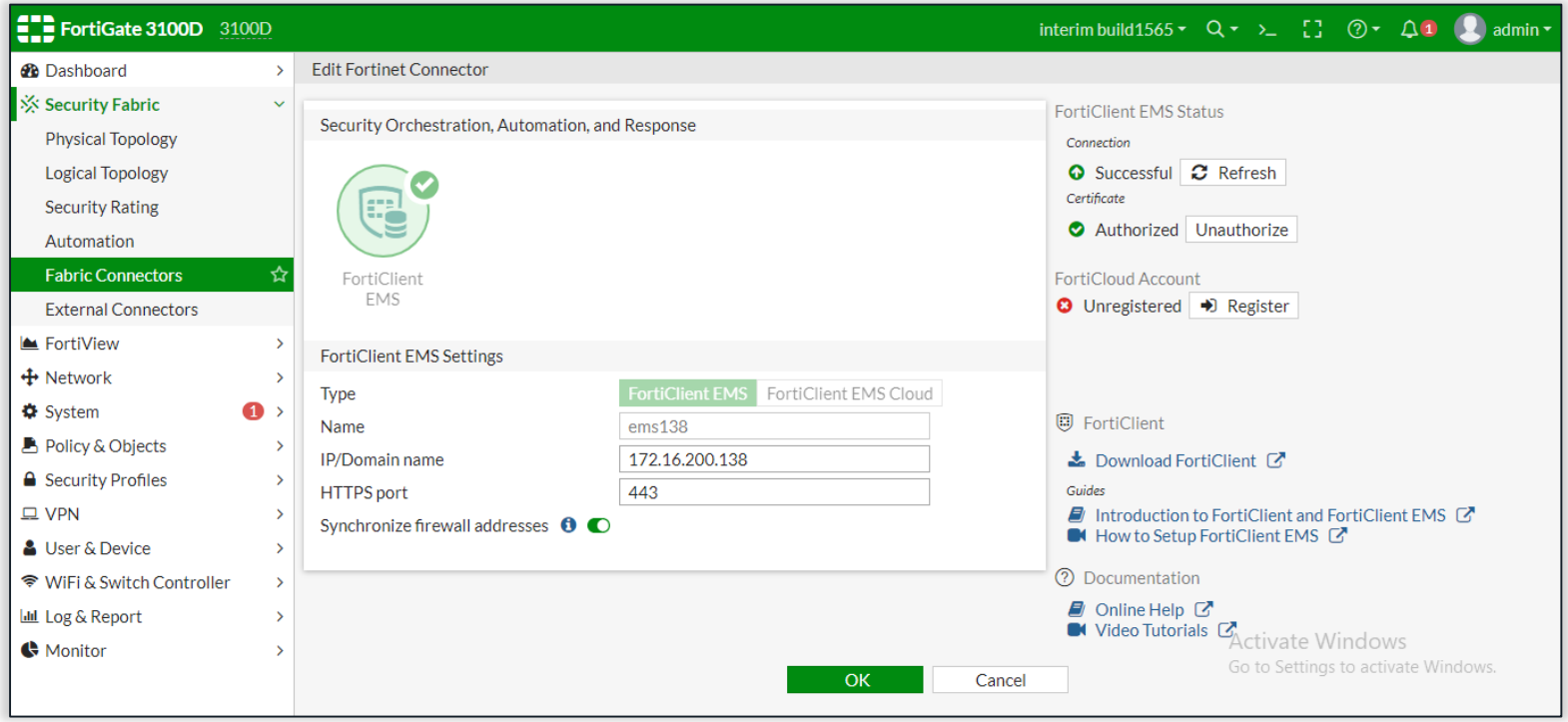
EMS может синхронизировать пользователей AD и группы безопасности, чтобы их можно было использовать для предоставления профилей безопасности конечных точек.



Fabric Management Center

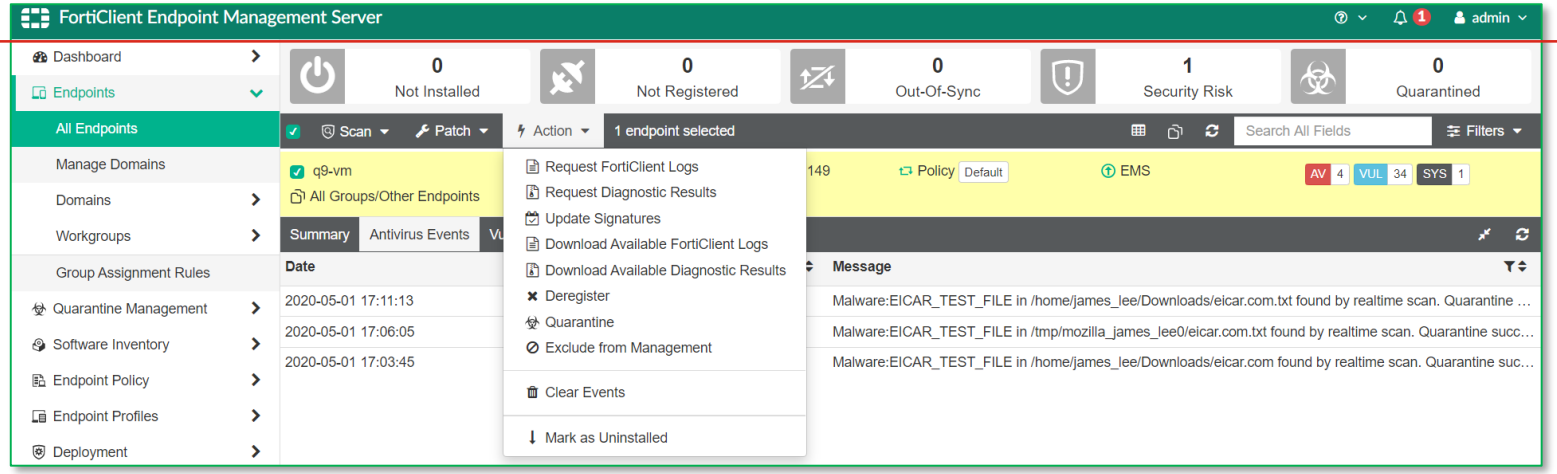
Упрощенный коннектор EMS на FortiOS

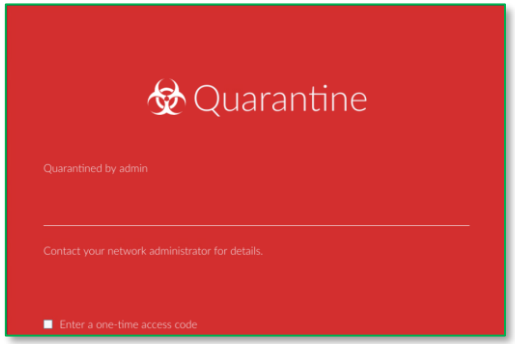
- Предоставление информации о машине пользователя
  - Операционная система
  - Сетевой интерфейс, IP/MAC адреса
  - Имя машины и Домен
  - Текущий пользователь
  - Аватар и Social ID идентификатор
- Состояние безопасности
  - AV статус
  - AV версия сигнатур
  - Состояние функции безопасности Windows
  - Обнаруженные уязвимости
- Контроль соответствия ПК политикам
  - Динамические теги для ПК
  - Соответствие на основе состояния безопасности, запущенных приложений, уязвимостей, запущенных процессов, разделов реестра, вошедшего в систему пользователя и т.д.
- Удаленные действия



6.4 другие улучшения

Linux Endpoint карантин

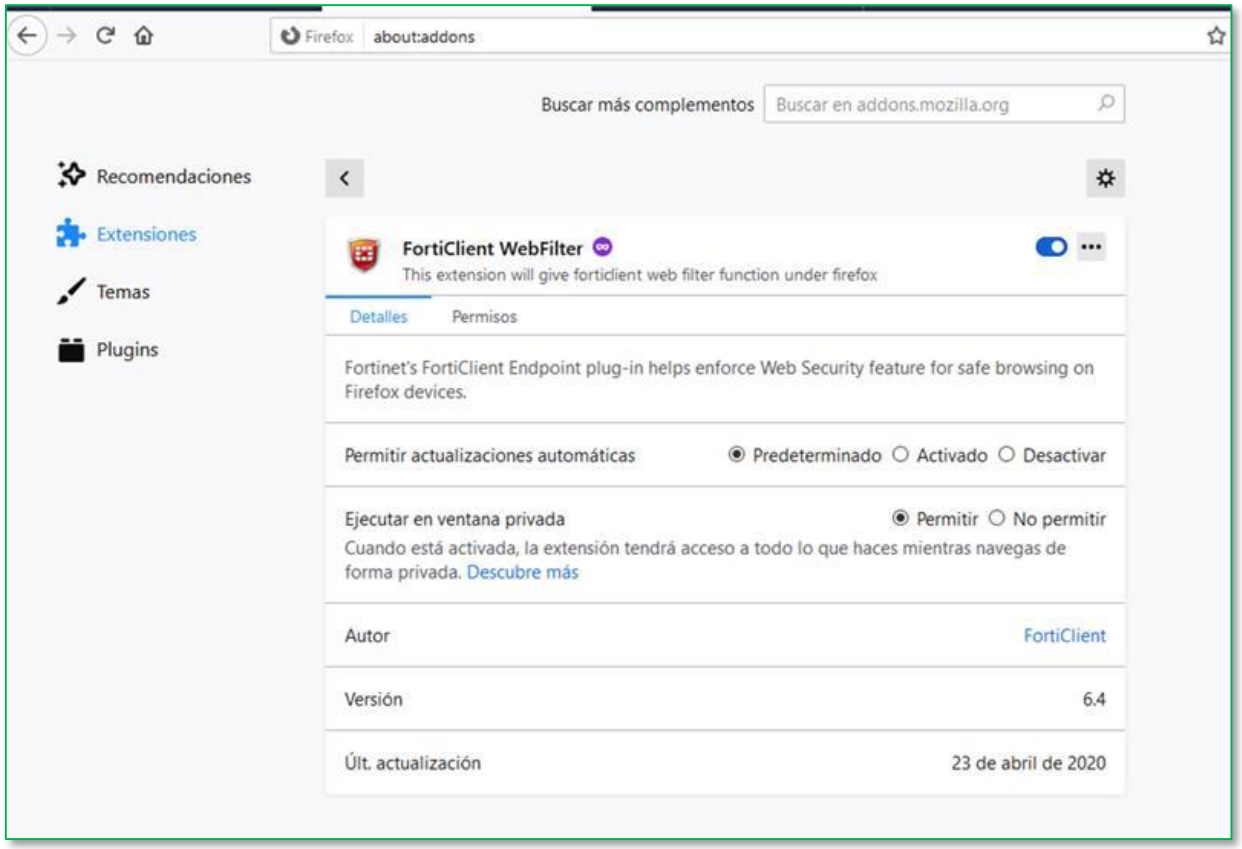


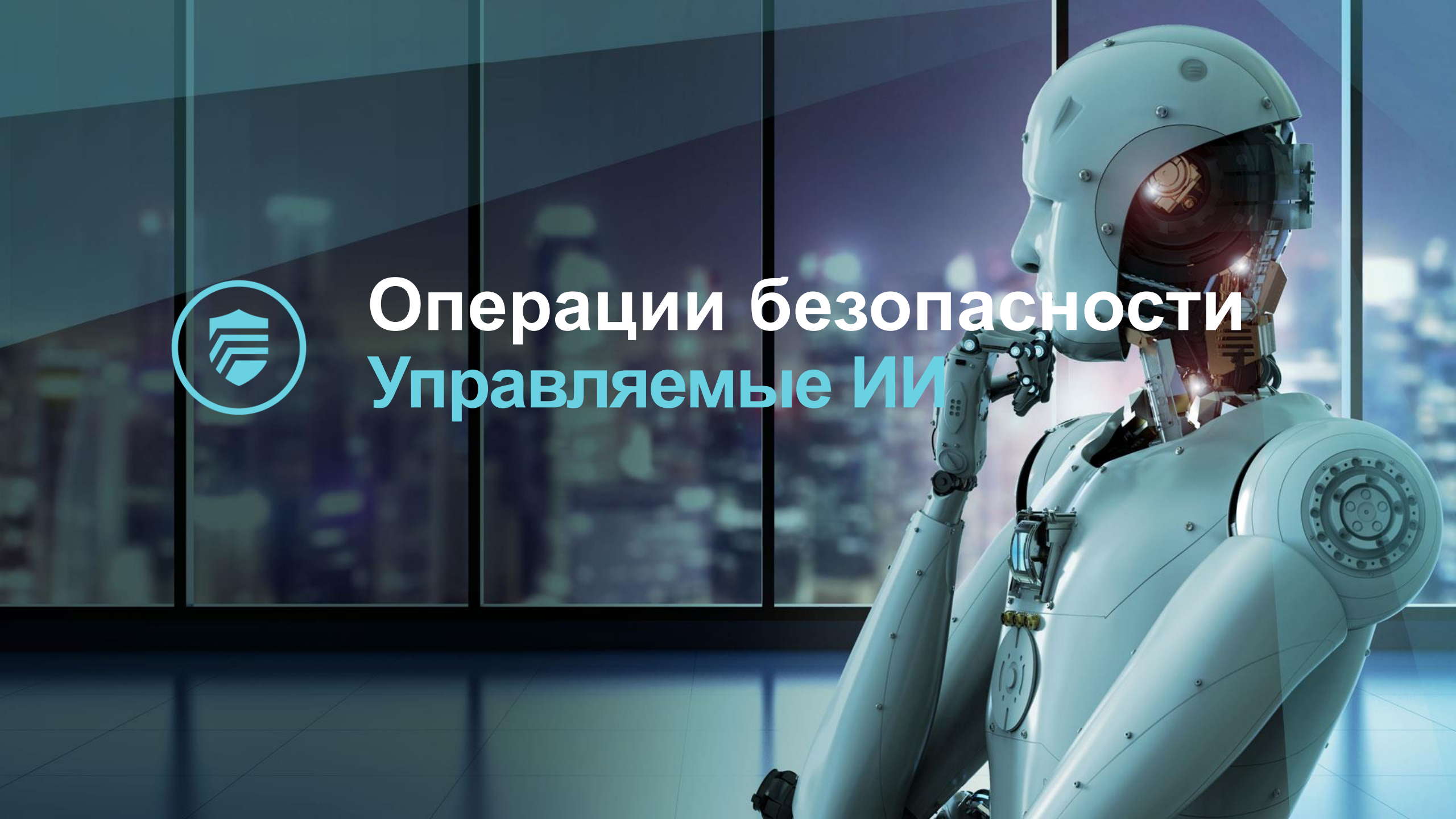


Плагин для браузера FireFox

- FireFox Browser плагин
- Ранее уже был для Chrome
- HTTPS инспекция для Web фильтрации

- Плагин для IE/Edge → будет в 6.4.1
- Для других браузеров → Позже





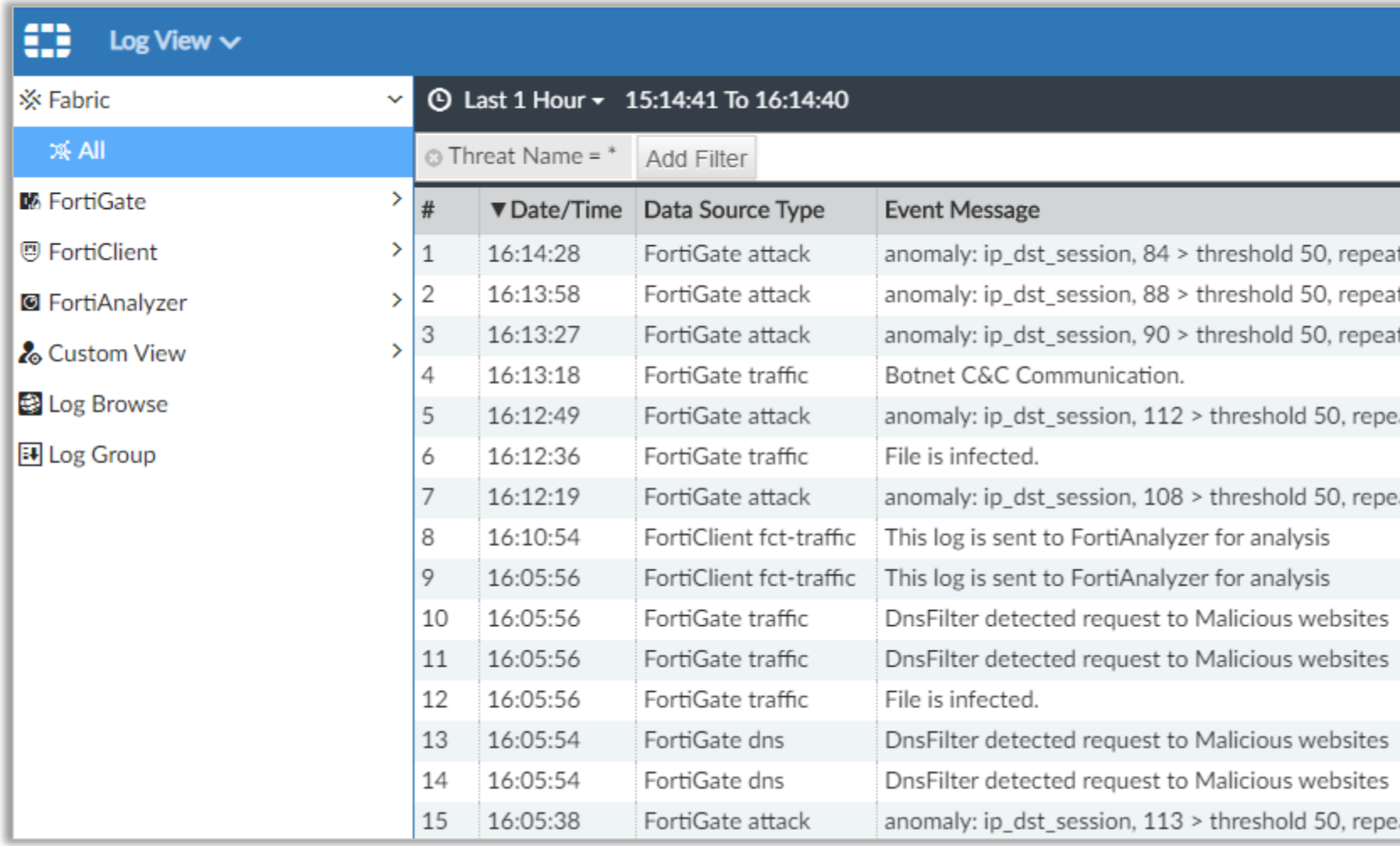
Операции безопасности
Управляемые ИИ

Управляемый ИИ анализ угроз

Расширенная телеметрия для агентов Security Fabric

FortiClient теперь также может извлекать журналы событий ОС и делиться ими с FortiAnalyzer вместе с журналами FortiClient. Поддерживается автоматическая отправка:

- Windows OS Event логов
  - События безопасности
  - События приложений
  - События системы
- Системные события MacOS
- Системные события Linux

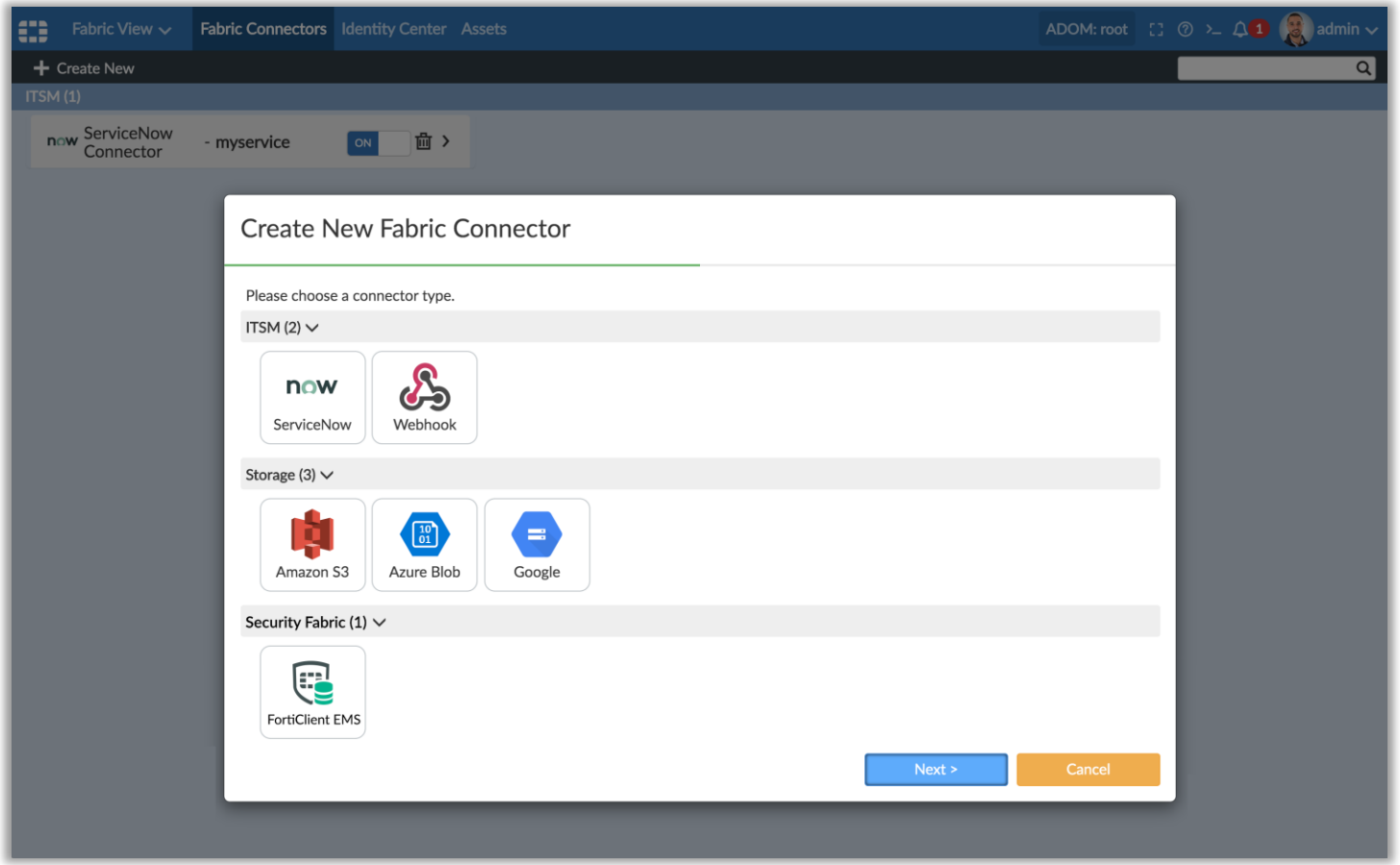


#	Date/Time	Data Source Type	Event Message
1	16:14:28	FortiGate attack	anomaly: ip_dst_session, 84 > threshold 50, repeat
2	16:13:58	FortiGate attack	anomaly: ip_dst_session, 88 > threshold 50, repeat
3	16:13:27	FortiGate attack	anomaly: ip_dst_session, 90 > threshold 50, repeat
4	16:13:18	FortiGate traffic	Botnet C&C Communication.
5	16:12:49	FortiGate attack	anomaly: ip_dst_session, 112 > threshold 50, repe
6	16:12:36	FortiGate traffic	File is infected.
7	16:12:19	FortiGate attack	anomaly: ip_dst_session, 108 > threshold 50, repe
8	16:10:54	FortiClient fct-traffic	This log is sent to FortiAnalyzer for analysis
9	16:05:56	FortiClient fct-traffic	This log is sent to FortiAnalyzer for analysis
10	16:05:56	FortiGate traffic	DnsFilter detected request to Malicious websites
11	16:05:56	FortiGate traffic	DnsFilter detected request to Malicious websites
12	16:05:56	FortiGate traffic	File is infected.
13	16:05:54	FortiGate dns	DnsFilter detected request to Malicious websites
14	16:05:54	FortiGate dns	DnsFilter detected request to Malicious websites
15	16:05:38	FortiGate attack	anomaly: ip_dst_session, 113 > threshold 50, repe

Управляемый ИИ анализ угроз

Появился коннектор EMS на FortiAnalyzer

- Информация о конечной точке
- Установленное ПО
- Информация о найденных уязвимостях
- Действие по удаленному исправлению
- Шаблоны (Playbook-и) ответных действий на инциденты
- Доступ в режиме реального времени к запущенным процессам и сетевым соединениям на конечных точках

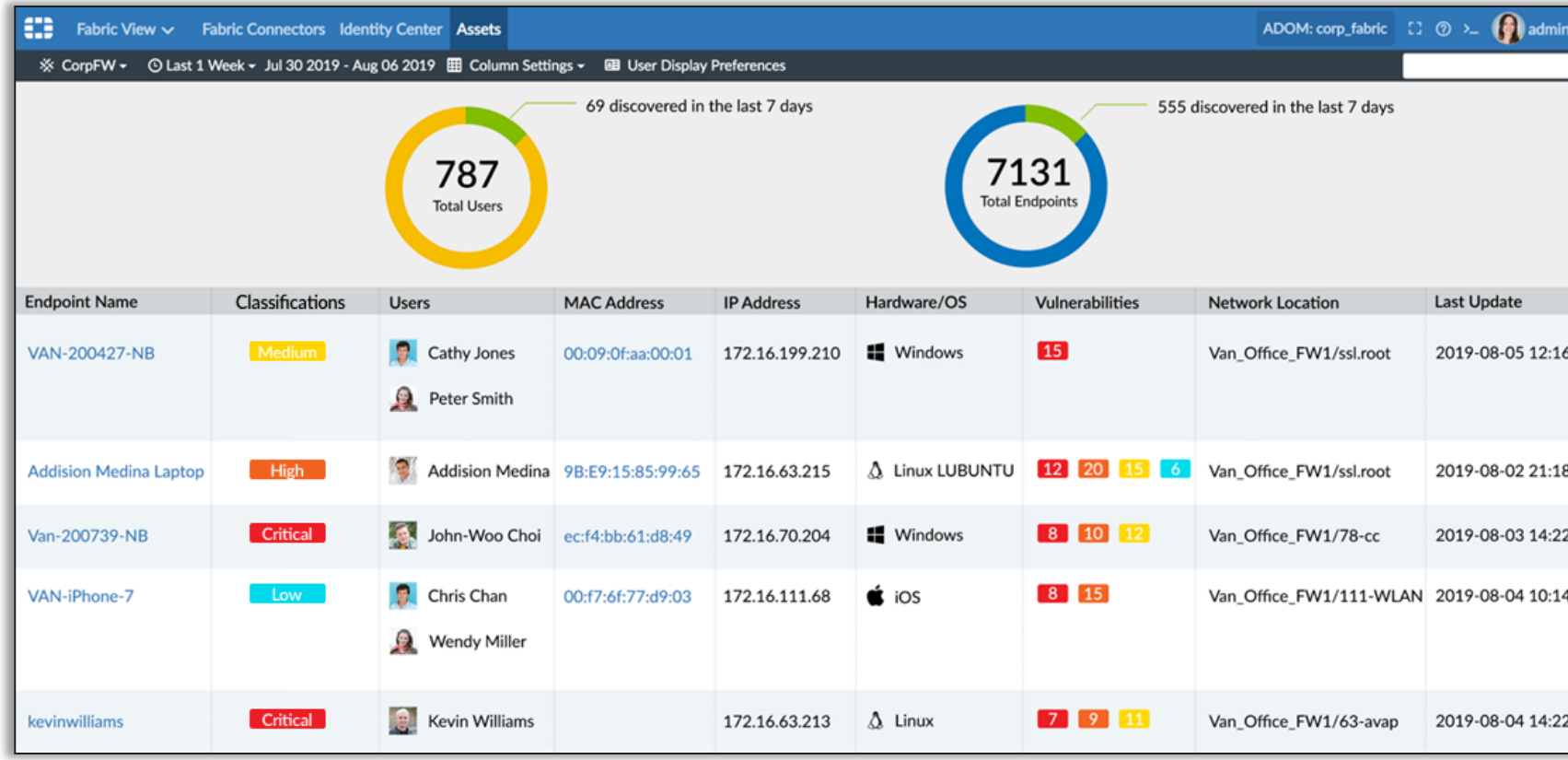


Управляемый ИИ анализ угроз

Информация о конечных точках в центре активов FAZ Assets

Центр активов обеспечивает в режиме реального времени просмотр всех корпоративных компьютеров конечных точек, их состояние безопасности и информацию о пользователях, вошедших в систему.

Информация о конечной точке теперь может быть получена с помощью EMS Connector и используется для обогащения центра активов в FortiAnalyzer более точными сведениями о конечной точке.

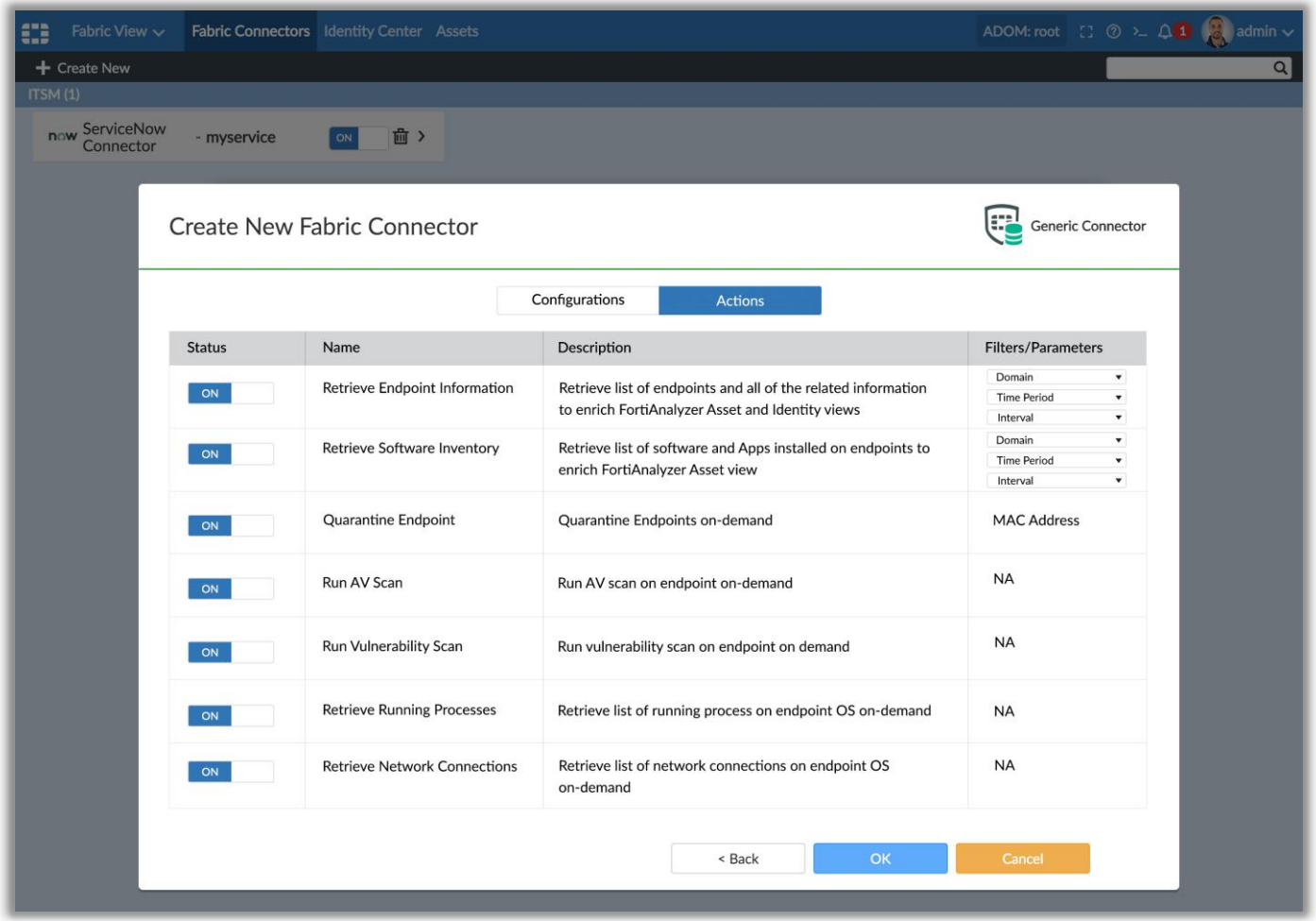


Управляемый ИИ анализ угроз

FortiAnalyzer SOC Playbook Actions

При возникновении инцидента, playbook-и можно использовать для получения информации о конечных точках в режиме реального времени из EMS и сопоставления ее с другими событиями сети фабрики для получения полной картины. Эти сопутствующие события затем могут быть использованы для выполнения соответствующих действий по исправлению

EMS поддерживает двунаправленные действия для обогащения или локализации инцидентов.



6.4 vs 6.2: Основные архитектурные отличия

EMS 6.2

- FGT – EMS имеет 2 конфигурации:
  - Элемент Security Fabric
  - Connector → Использование FSSO
- Пересечение с другими FSSO конфигурациями в той же политике (Пользователи, группы)
  - например отдел Маркетинга в AD и динамическая группа FCT TAG для VPN
- Ограничение - 3 FortiGate шлюза на EMS

EMS 6.4

- FGT – EMS
  - Использует API
  - Улучшена безопасность: Требуется действующий EMS сертификат
- Новый коннектор с FAZ
  - Автоматизация с использованием SOC
- Новый коннектор с FNAC
  - В основном для получения информации
- Обновление в режиме реального времени

Demo Time

Демонстрация функционала 6.4

Содержимое

Пошаговые инструкции для трех новых функций, представленных в выпуске FortiClient/EMS 6.4:

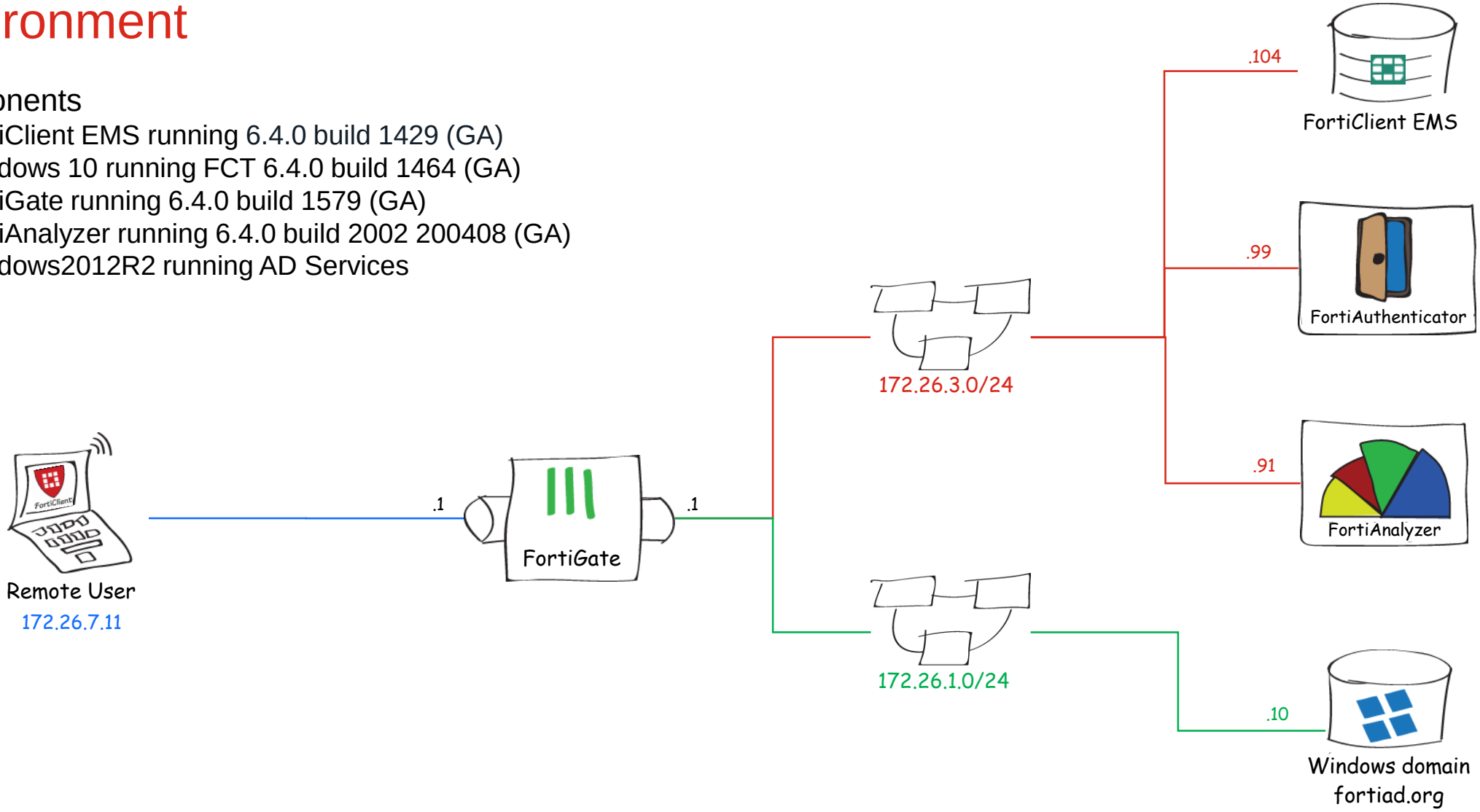
- Профили пользователей FortiClient на основе групп пользователей
- Новая интеграция - EMS, FGT, FAZ
- Аутентификация SSL-VPN с использованием SAML

Demo Lab

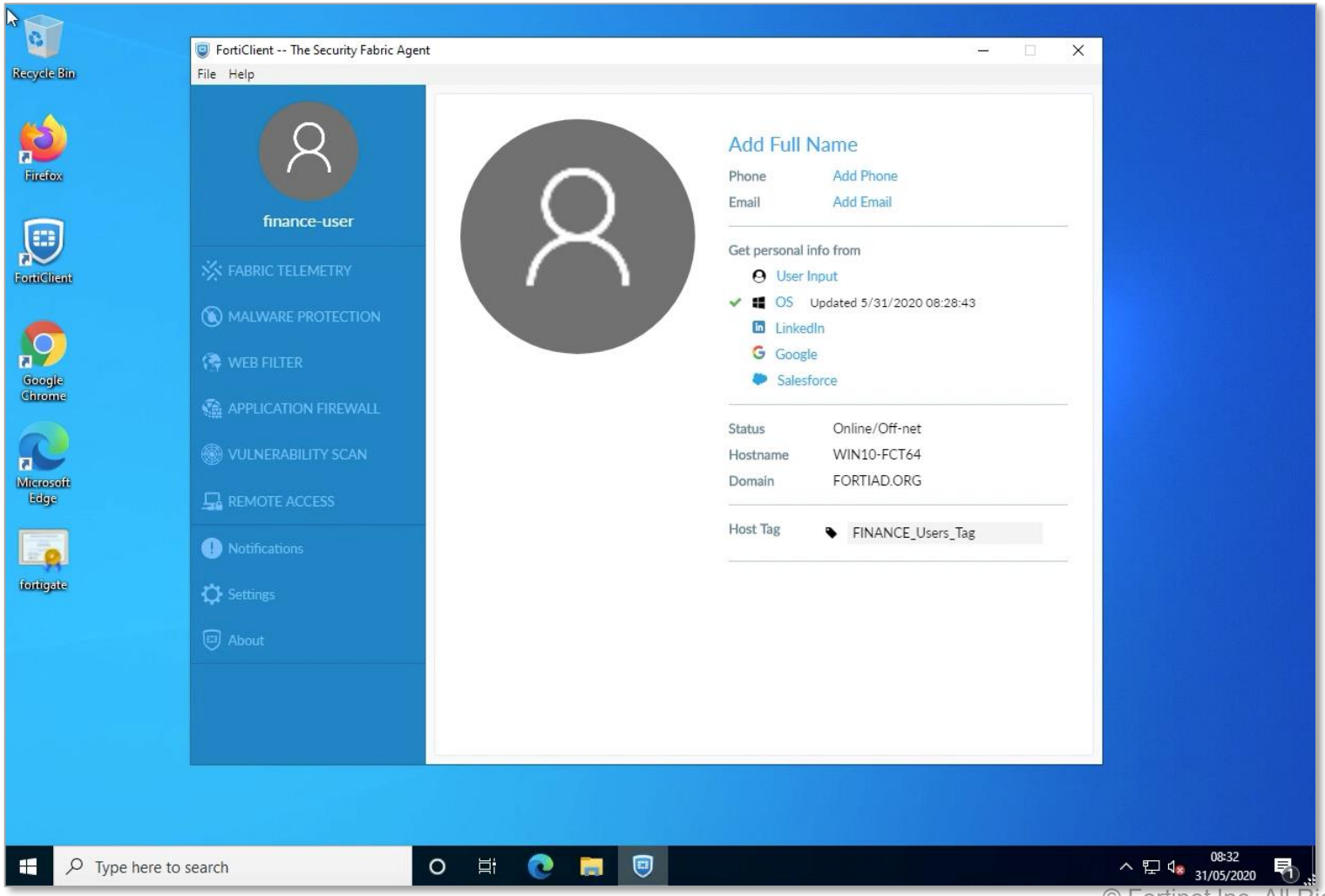
Environment

Components

- FortiClient EMS running 6.4.0 build 1429 (GA)
- Windows 10 running FCT 6.4.0 build 1464 (GA)
- FortiGate running 6.4.0 build 1579 (GA)
- FortiAnalyzer running 6.4.0 build 2002 200408 (GA)
- Windows2012R2 running AD Services

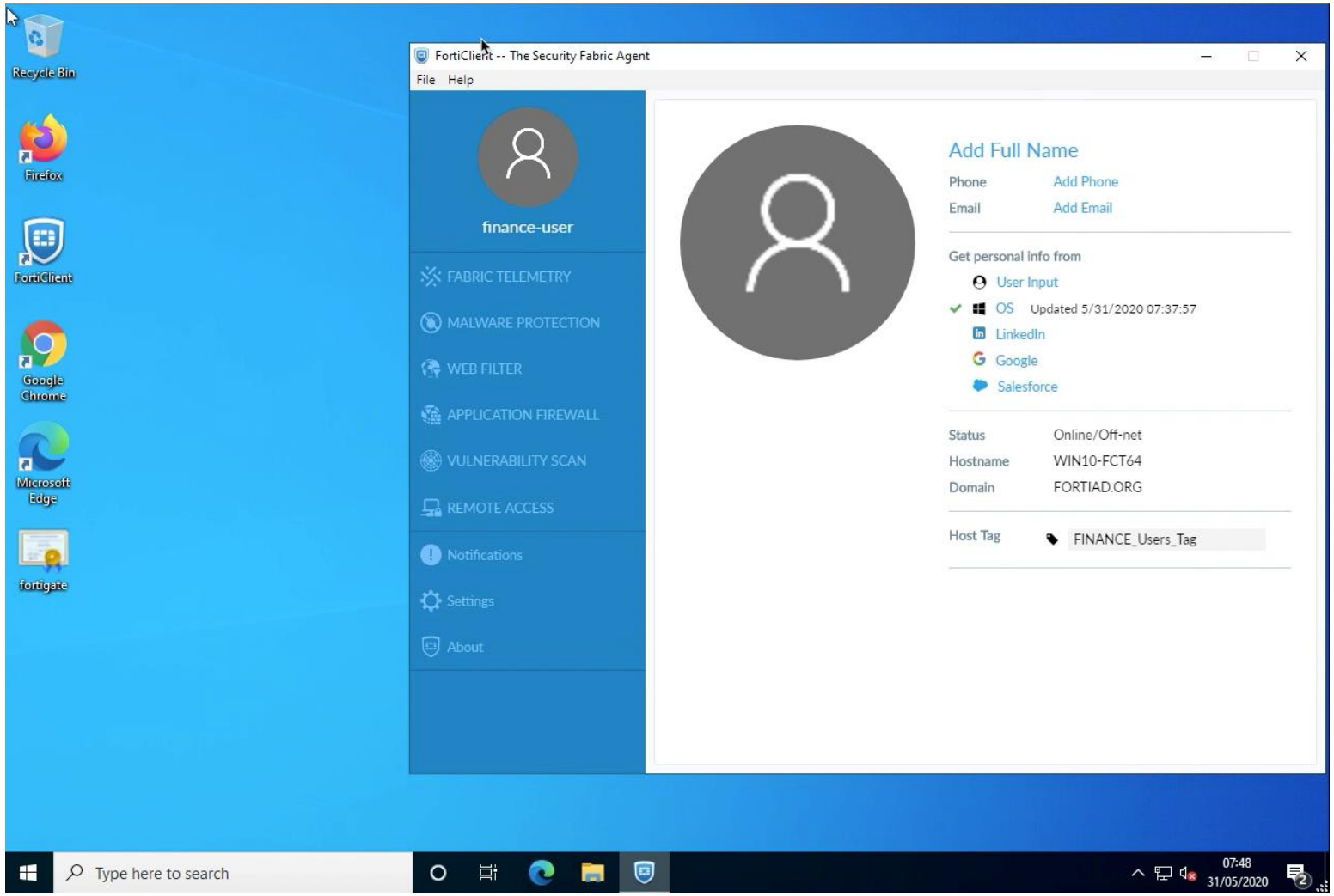


FortiClient применение профилей к группам пользователей



EMS-FGT Fabric интеграция

DEMO → UNTRUSTED 3				
FCTEMS0000108120_SALES_Users_Tag	all	always	ALL_ICMP	DENY
FCTEMS0000108120_SALES_Users_Tag	all	always	ALL	ACCEPT
FCTEMS0000108120_FINANCE_Users_Tag	all	always	ALL	ACCEPT



SSL-VPN SAML аутентификация