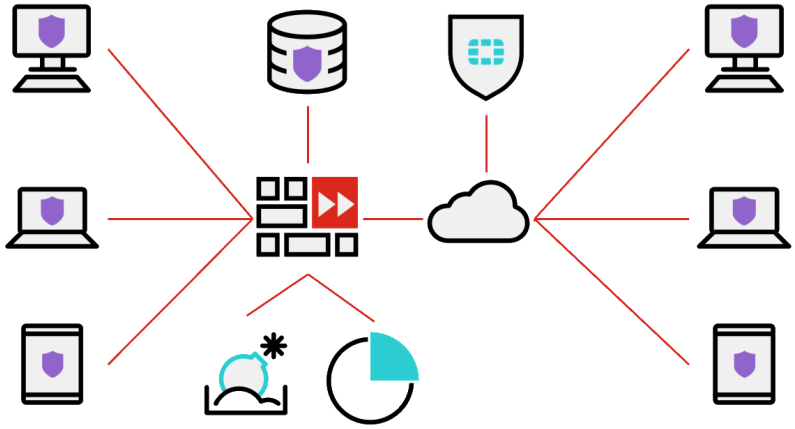
DATA SHEET

FortiClient 7.0

Единый клиент для обеспечения защиты и контроля конечных рабочих станций и серверов с технологией нулевого доверия и безопасным клиентом удаленного доступа VPN



Сбор телеметрии и интеграция FortiClient в архитектуру Fortinet Security Fabric обеспечивает максимальную видимость и гарантирует, что компоненты безопасности – FortiGate, FortiAnalyzer, EMS, FortiSandbox, управляемые точки доступа и коммутаторы – работают в едином контексте и обеспечивают контроль доступа, информирование, соблюдение требований и отчетность. FortiClient сочитает в себе технологии построения виртуальных частных сетей (VPN) и удаленный доступ в сеть с нулевым доверием (ZTNA). FortiClient защищает клиентов внутри корпоративного периметра и находящихся за его пределами.

Единый клиент для обеспечения защиты, соответствия требованиям и предоставления безопасного доступа.

Концепция нулевого доверия лежит в основе контроля и проверки безопасности каждой сессии используемых приложений.

Защита от эксплоитов и нацеленных атак (ATP) при поддержке лаборатории FortiGuard и интеграцией с песочницей FortiSandbox.

Централизованное управление и отчетность с помощью специализированного решения FortiClient EMS или FortiGate.

Возможности централизованного управления

- Простой и удобный интерфейс управления
- Удаленная установка агентов
- Инвентаризация установленного ПО
- Отчетность в режиме реального времени
- Интеграция с Active Directory
- Управление карантином
- Автоформирование групп управляемых рабочих станций
- Динамический контроль доступа
- Автоматизация оповещений
- Различные варианты использования платформы (локальная установка или облако)

Сервисы безопасности FortiGuard
www.fortiguard.com

Круглосуточная техническая поддержка FortiCare
support.fortinet.com

ПРЕИМУЩЕСТВА

Интеграция с Fortinet Security Fabric

FortiClient интегрирует защищаемые сервера и рабочие станции в Fortinet Security Fabric для раннего обнаружения и защиты от нацеленных атак. Интеграция обеспечивает видимость, контроль, соответствие требованиям, а также возможности по управлению уязвимостями и настройке автоматических действий для защищаемых систем. FortiOS и FortiAnalyzer используют собираемую FortiClient телеметрию для выявления признаков компрометации. Автоматическая изоляция и помещение в карантин подозрительных или явно скомпрометированных конечных точек позволяет предотвратить масштабные инциденты, остановив атаку на раннем этапе развития. Функции обеспечения соответствия требованиям и управления уязвимостями упрощают применение корпоративных политик безопасности и повышают уровень защищенности серверов и рабочих станций.

Web фильтрация и контроль SaaS приложений

FortiClient обеспечивает Web фильтрацию и безопасный доступ в Интернет на уровне конечной точки. Клиентский межсетевой экран уровня приложений детектирует используемые Web и SaaS приложения, защищает сервера и рабочие станции от компрометации и превращения в часть ботнет сетей.

Сетевой доступ с нулевым доверием (ZTNA)

FortiClient ZTNA использует встроенную функцию операционной системы FortiOS для обеспечения безопасного доступа к приложениям независимо от того, является ли пользователь локальным или удаленным. При каждом сеансе обмена данными используются защищенные туннели от FortiClient до прокси сервера FortiGate/FortiProxy, при котором выполняется обязательная проверка как пользователя, так и устройства. Только в случае успешного прохождения этих проверок безопасности предоставляется доступ для данного сеанса.

Цифровая гигиена конечных точек

FortiClient сокращает поверхность атаки путем сканирования установленных приложений на наличие известных уязвимостей и их автоматического исправления. В сочетании с принципами доступа с нулевым доверием этот подход повышает уровень цифровой гигиены конечных точек и безопасности организации в целом.

Защита от эксплойтов и вредоносного ПО

За счет интеграции с облачной песочницей и службой FortiGuard Threat intelligence агент FortiClient предотвращает заражение высокотехнологичным вредоносным ПО и позволяет блокировать использование уязвимостей на конечных точках. Все файлы, загружаемые на рабочую станцию с установленным агентом FortiClient, проходят проверку в облачной песочнице в режиме реального времени. Миллионы пользователей FortiClient и FortiSandbox по всему миру делятся информацией об известных и неизвестных вредоносных программах с облачной платформой FortiGuard Threat intelligence.

Виртуальные частные сети (VPN)

FortiClient предоставляет разнообразные возможности подключения к VPN. Поддерживается как технология SSL VPN, так и классический IPsec VPN. Возможность раздельного туннелирования для удаленных пользователей позволяет получить доступ в Интернет без необходимости перенаправлять весь трафик через корпоративный VPN сервер. Эта функция уменьшает временную задержку при передаче данных по сети, что положительно сказывается на скорости загрузки данных для пользователей. В то же время FortiClient включает средства защиты, гарантирующие, что данные из Интернет не смогут попасть обратно в VPN соединение и поставить под угрозу корпоративную сеть.

В дополнение к возможностям подключения FortiClient упрощает процессы автоматического подключения и динамического выбора VPN сервера. Вы также можете использовать многофакторную аутентификацию для обеспечения дополнительного уровня безопасности VPN соединений.

Защита от атак крипто-вымогателей (Ransomware)

В последнее время, количество атак с использованием крипто-вымогателей значительно возросло. Для предотвращения этих угроз в решении FortiClient была представлена новая технология защиты, которая позволяет вернуть рабочую станцию в изначальное состояние, до момента заражения.

СЕРВИСЫ

FortiClient Managed Services

Компания Fortinet предлагает свои услуги по первоначальной инсталляции, конфигурации и мониторингу агентов FortiClient. Это позволяет в кратчайшие сроки начать эффективно использовать решение FortiClient, опираясь на опыт и экспертизу сервисной команды Fortinet.

- **Первоначальное внедрение FortiClient Cloud**: совместно с командой заказчика мы спланируем и реализуем внедрение FortiClient Cloud, включая:
  - Формирование структуры дерева управляемых конечных точек
  - ZTNA
  - VPN
  - Управление уязвимостями установленных приложений
  - Настройка профилей и политик безопасности
  - Настройка правил контроля состояния конечных точек
  - Создание индивидуального установщика
- **Первоначальная установка агентов**: Сервисная команда Fortinet подготовит индивидуальный установщик FortiClient. Для последующей установки и регистрации агентов в системе управления FortiClient Cloud пользователям будут отправлены электронные письма с описанием необходимых действий.
- **Интеграция с Fortinet Security Fabric**: Будут выполнены необходимые работы по интеграции агентов FortiClient с Fortinet Security Fabric. Это позволит реализовать дополнительную автоматизацию и реагирование на инциденты, а также использовать архитектуру доступа с нулевым доверием (ZTNA).
- **Контроль критических уязвимостей**: Сервисная команда Fortinet проинформирует заказчика о факте обнаружения в их инфраструктуре конечных точек с высоким уровнем риска. Будут предоставлены рекомендации по устранению или минимизации рисков для данных систем.

Сервис лучших практик (BPS)

FortiClient Best Practices Service — это годовая подписка, предоставляющая доступ к специализированной команде экспертов, которая удаленно консультирует клиентов по вопросам установки, обновления и эксплуатации FortiClient. На основе информации, предоставляемой клиентами об их инфраструктуре и задачами, поставленными перед внедрением решения, эксперты сервиса BPS предоставляют консультации по развертыванию и настройке системы FortiClient. В рамках сервиса предоставляется дополнительная информация по лучшим практикам работы, ссылки на стороннее программное обеспечение и необходимые образцы программного кода. Данная команда не выполняет непосредственно администрирование системы и не имеет доступа к управлению конфигурациями у заказчика.

ОСОБЕННОСТИ

Централизованное управление агентами на операционных системах Windows, macOS, Linux, Chrome, iOS и Android. Сервер FortiClient EMS может быть развернут в инфраструктуре заказчика или оказываться в виде сервиса FortiClient Cloud.

Управление инвентаризацией отслеживает установленное программное обеспечение и осуществляет контроль его лицензирования. Используя данную инвентаризационную информацию, можно с легкостью обнаружить неиспользуемое или устаревшее ПО, что значительно снизит потенциальную площадь атаки на рабочие станции.

Интеграция со службой каталогов Microsoft Windows Active Directory позволяет синхронизировать используемую организационную структуру компании в консоль управления. Это позволит упростить управление и использовать идентичные группы, используемые в службах каталогов Windows.

Мгновенное предоставление текущей информации с агентов. События информационной безопасности и текущая активность на конечных точках отображаются в режиме реального времени.

Панель обнаруженных уязвимостей позволяет легко идентифицировать конечные точки, требующие дополнительного внимания со стороны службы информационной безопасности. Это в значительной мере снижает возможности злоумышленников по возможностям атаки на данные системы.

Централизованная система управления агентами FortiClient позволяет администраторам удаленно устанавливать, обновлять и конфигурировать клиентов системы, что значительно упрощает первоначальный этап развертывания агентов.

Интеграция с FortiSandbox определяет политику работы с подозрительными файлами и при необходимости отправляет их на дополнительный анализ. Детальная информация по предоставленным файлам будет доступна в консоли управления. Это позволит администраторам системы получить полное описание действий подозрительных файлов включая визуализацию дерева процессов.

FortiGate provides awareness and control over all your endpoints.

Телеметрия предоставляет информацию о клиентах в консоли FortiGate в режиме реального времени. Эта информация доступна всем компонентам Fortinet Security Fabric, что позволяет администраторам получить максимальную видимость происходящего в сети предприятия.

Динамический контроль доступа для обеспечения соответствия требованиям. FortiClient EMS создает виртуальные группы на основе состояния безопасности конечных точек. Данные виртуальные группы используется в FortiGate при определении политик. Это позволяет реализовать динамический контроль доступа клиентов в зависимости от их текущего состояния. Использование динамических групп помогает автоматизировать и значительно упростить соблюдение различных требований безопасности.

Карантин конечной точки позволяет быстро отключить скомпрометированный хост от сети предприятия и предотвратить возможность последующего распространения вредоносной активности.

Автоматическое реагирование позволяют настроить различные действия, включая изоляцию конечных точек без участия администраторов, что обеспечивает мгновенную реакцию на возникающие угрозы.

Раздельное туннелирование траффика приложений позволяет гранулировано определить, какие данные должны быть переданы через шифрованный туннель, а какие напрямую через сеть Интернет. Это положительно скажется на скорости передачи данных от указанных приложений.

Веб фильтрация контента по ключевым словам / фильтры YouTube. Блокировка веб-страниц, содержащих определенные слова или совпадения по регулярным выражениям, контроль данных с YouTube с возможностью ограничить определенный контент или канал, не блокируя при этом сервис целиком.

ВАРИАНТЫ ЛИЦЕНЗИРОВАНИЯ

ВАРИАНТЫ ЛИЦЕНЗИЙ FORTICLIENT	ZTNA	EPP / APT	MANAGED SERVICES	CHROMEBOOK
Сетевой доступ с нулевым доверием (ZTNA)	**Windows, macOS, Linux**	**Windows, macOS, Linux**	**Windows, macOS, Linux**	**Chromebook**
Zero Trust агент с мультифакторной аутентификацией	✓	✓	✓	
Централизованное управление с EMS или FortiClient Cloud	✓	✓	✓	✓
Централизованная отчетность	✓	✓	✓	✓
Динамический коннектор к Fortinet Security Fabric	✓	✓	✓	
Модуль поиска известных уязвимостей	✓	✓	✓	
SSL VPN с мультифакторной аутентификацией	✓	✓	✓	
IPSEC VPN с мультифакторной аутентификацией	✓	✓	✓	
Веб-фильтрация FortiGuard	✓	✓	✓	✓
Интеграция с FortiSandbox (локальной или сервисом)	✓	✓	✓	✓
Контроль подключаемых по USB устройств	✓	✓	✓	
Расширенные функции безопасности				
Антивирус на основе искусственного интеллекта		✓	✓	
Интеграция с Fortinet Cloud Sandbox[1]		✓	✓	
Автоматический карантин рабочей станции		✓	✓	
Межсетевой экран для приложений[1]		✓	✓	
Инвентаризация приложений		✓	✓	
Защита от крипто-вымогателей[2]		✓	✓	
Сервисы для решений FortiClient				
Установка агентов			✓	
Базовая конфигурация профилей безопасности			✓	
Интеграция с Fortinet Security Fabric			✓	
Мониторинг уязвимостей приложений			✓	
Мониторинг безопасности конечных точек			✓	
Дополнительные сервисы				
Сервис лучших практик (BPS)	Дополнение	Дополнение	Недоступно	Дополнение
Круглосуточная техническая поддержка	✓	✓	✓	✓
Локальная инсталляция/Изолированные сегменты	✓	✓		✓

1. FortiClient (Linux) не поддерживает данный функционал.
2. Только FortiClient (Windows) поддерживает данный функционал.

ФУНКЦИОНАЛ ПО ПЛАТФОРМАМ И ТРЕБОВАНИЯ

	WINDOWS	MACOS	ANDROID	IOS	CHROMEBOOK	LINUX
ZTNA						
Сбор телеметрии[1]	✓	✓	✓	✓	✓	✓
Динамические группы доступа и проверка соответствия требованиям[1]	✓	✓	✓	✓		✓
Сканирование установленного ПО на наличие известных уязвимостей	✓	✓				✓
Сбор событий и отчетность[2]	✓	✓		✓	✓	✓
IPSec VPN	✓	✓	✓			
SSL VPN[3]	✓	✓	✓	✓		✓
Удаленный доступ ZTNA	✓	✓				✓
Агент единого входа Windows AD	✓	✓				
Контроль подключаемых по USB устройств	✓	✓				✓
Расширенные функции безопасности						
Антивирус	✓	✓				✓
Cloud-based Threat Detection	✓	✓				
Интеграция с Sandbox (локальный)	✓	✓				✓[4]
Интеграция с Sandbox (облачный)	✓	✓				
Автоматический карантин	✓	✓				
Веб-фильтрация[5]	✓	✓	✓	✓	✓	
Защита от эксплойтов	✓					
Межсетевой экран приложений	✓	✓				

PLUS - добавьте подписку Sandbox Cloud для проактивной защиты от высокотехнологичных угроз.

1. Требуется EMS или FortiClient Cloud для централизованного управления FortiClient.
2. Требуется FortiAnalyzer.
3. Совместим с Windows mobile.
4. Без отправки файлов
5. Совместим с Chrome OS.

Таблица выше справедлива для последних версий ОС каждого типа.

FORTICLIENT
Поддерживаемые операционные системы*
Microsoft Windows 7 (32-бит и 64-бит)
Microsoft Windows 8, 8.1 (32-бит и 64-бит)
Microsoft Windows 10 (32-бит и 64-бит)
Microsoft Windows Server 2012 и выше
macOS 11+, 10.15, 10.14
iOS 9.0 и выше
Android 5.0 и выше
Linux Ubuntu 16.04 и выше, Red Hat 7.4 и выше, CentOS 7.4 и выше с KDE или GNOME
Возможности аутентификации
RADIUS, LDAP, локальная база данных, xAuth, TACACS+, сертификат (X509), FortiToken
Возможности подключения
Автоподключение VPN до входа в Windows
Конфигурация IKE для туннелей FortiClient IPsec VPN

FORTICLIENT EMS
Поддерживаемые операционные системы
Microsoft Windows Server 2012 и выше
Требования к клиентам
FortiClient 6.4 и выше, FortiClient для Windows и macOS X, 6.4 для iOS и Android
Системные требования
2.0 Ггц 64-бит процессор, 6 ядер CPUs, 8 ГБ RAM, 40 ГБ свободного места на диске, адаптер 10/100/1000BaseT
Сетевой Ethernet адаптер, Доступ в Интернет

ИНФОРМАЦИЯ ДЛЯ ЗАКАЗА

ТИП ЛИЦЕНЗИИ	ZTNA	EPP/APT	MANAGED	CHROMEBOOK
PaaS (EMS в облаке)				
25-хостов	FC1-10-EMS05-428-01-DD	FC1-10-EMS05-429-01-DD	FC1-10-EMS05-485-01-DD	FC1-10-EMS05-403-01-DD
500-хостов	FC2-10-EMS05-428-01-DD	FC2-10-EMS05-429-01-DD	FC2-10-EMS05-485-01-DD	FC2-10-EMS05-403-01-DD
2000-хостов	FC3-10-EMS05-428-01-DD	FC3-10-EMS05-429-01-DD	FC3-10-EMS05-485-01-DD	FC3-10-EMS05-403-01-DD
10 000 хостов	FC4-10-EMS05-428-01-DD	FC4-10-EMS05-429-01-DD	FC4-10-EMS05-485-01-DD	FC4-10-EMS05-403-01-DD
Локальная инсталляция				
25-хостов	FC1-10-EMS04-428-01-DD	FC1-10-EMS04-429-01-DD		FC1-10-EMS04-403-01-DD
500-хостов	FC2-10-EMS04-428-01-DD	FC2-10-EMS04-429-01-DD		FC2-10-EMS04-403-01-DD
2000-хостов	FC3-10-EMS04-428-01-DD	FC3-10-EMS04-429-01-DD		FC3-10-EMS04-403-01-DD
10 000 хостов	FC4-10-EMS04-428-01-DD	FC4-10-EMS04-429-01-DD		FC4-10-EMS04-403-01-DD
FortiCare сервис лучших практи (BPS)				
25-999 хостов		FC1-10-FCBPS-310-02-DD		
1000-9999 хостов		FC2-10-FCBPS-310-02-DD		
10 000+ хостов		FC5-10-FCBPS-310-02-DD		
Услуги по обучению				
Обучение с инструктором (класс или удаленно)		FT-FCT		
Доступ к лабораторным работам - окружения на портале обучения NSE (https://training.fortinet.com)		FT-FCT-LAB		
Ваучер для сдачи экзамена NSE5		NSE-EX-SPL5		

FORTINET®

www.fortinet.com