DATA SHEET

FortiAnalyzer

Исполнение:

Устройство | Виртуальная машина | Облако

FortiAnalyzer - это аналитическая платформа для управления событиями, журналами и формирования отчетности. Решение облегчает и автоматизирует операционную деятельность подразделений безопасности, проактивно идентифицирует потенциальные риски, обеспечивает максимальную видимость поверхности атаки.

FortiAnalyzer интегрирован в архитектуру Fortinet Security Fabric, реализует функции аналитики безопасности и позволяет обнаруживать и предотвращать попытки проникновения на самых ранних стадиях атаки.

Объединяет инструменты безопасности, людей и процессы для эффективного управления событиями и инцидентами, быстрого обнаружения и реагирования.

Автоматизирует последовательность действий по блокированию атаки и устранению последствий. Интегрирован со средствами зашиты Fortinet Security Fabric и позволяет командам сетевой безопасности минимизировать затраты времени на инциденты, обеспечить выполнение SLA.

Реагирует на сетевые атаки, уязвимости, информацию о потенциальных компрометациях и угрозах, коррелирует события безопасности из сторонних источников, уведомляет о необходимости дополнительных защитных мер.

Особенности

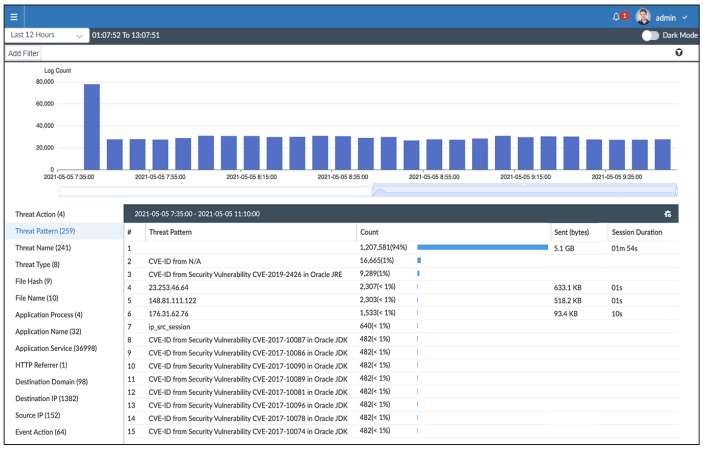
- Корреляция событий средств защиты Fortinet Security Fabric, сервис предоставления индикаторов компрометации (IOC) для противодействия нацеленным атакам
- Интеграция с FortiGate, FortiClient, FortiSandbox, FortiWeb, FortiMail и другими решениями для глубокой аналитики событий безопасности
- Высокая доступность (до 4 нод в кластере) с поддержкой геораспределенной архитектуры
- Автоматизация механизмов обнаружения и реакции на атаки за счет интеграции со средствами защиты на уровне API и специальных коннекторов
- Поддержка изолированных доменов управления (ADOM) для обеспечения изоляции пользовательских данных, аналитики и отчетности
- Исполнение в виде устройства, виртуальной машины, публичного облака или SaaS. Поддержка AWS, Azure и Google в качестве резервного облачного архива

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Обнаружение и управление инцидентами

Сетевой операционный центр (NOC) и Центр информационной безопасности (SOC)

Представление FortiSOC в FortiAnalyzer помогает командам SOC/NOC защищать сети, предоставляя доступ к журналам и данным об угрозах в режиме реального времени. Информация отображается в интерактивном формате, с поддержкой предопределенных и настраиваемых экранов, уведомлений и отчетов. Визуализация процессов операционной деятельности упрощает и ускоряет обнаружение аномалий и выполнение упреждающих действий по результатам корреляции нормальзованных событий информационной безопасности, полученных со средств защиты.

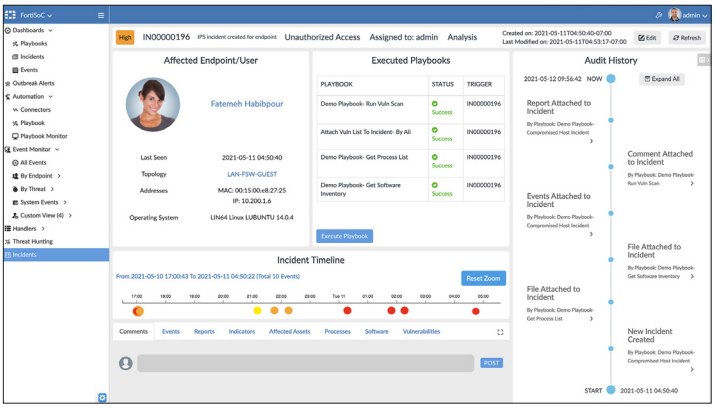


Управление событиями

Монитор Событий FortiAnalyzer позволяет отслеживать и управлять событиями из журналов безопасности. События обрабатываются и сопоставляются в легко читаемом формате, понятном для аналитика и достаточном для немедленного реагирования. Монитор Событий позволяет проводить расследования как ручным поиском, так и с использованием предопределенных или настраиваемых обработчиков событий для NOC и SOC. Система имеет преднастроенные обработчики для SD-WAN, VPN, беспроводной связи, сетевых операций, FortiClient и многих других категорий событий.

Управление инцидентами

Представлении FortiSOC позволяет управлять инцидентами на протяжения всего их жизненного цикла. Аналитики имеют возможность ознакомиться со всеми событиями, приведшими к инциденту, а также добавлять дополнительную информацию по результатам расследований, отслеживать выполнение автоматизированных сценариев реагирования.



Штатный коннектор FortiAnalyzer реализует интеграцию с FortiSOAR для дальнейшего расследования и работы по инциденту с возможностью выгрузки всех деталей через API.

Автоматизация операций

Автоматизированные сценарии реагирования (playbook) в FortiAnalyzer высвобождают ресурсы подразделений информационной безопасности и позволяют аналитикам сосредоточиться на более важных задачах.

Широкий набор предустановленных шаблонов автоматизированных сценариев реагирования доступен для тонкой настройки под инфраструктуру организации с помощью визуального редактора. Сценарии включают в себя оценку скомпрометированных хостов, обогащение данных известными индикаторами компрометации и т.д. Монитор сценариев позволяет отслеживать состояние их исполнения. Сценарии интегрированы с коннекторами Fortinet Security Fabric, что позволяет с их помощью взаимодействовать с FortiOS, EMS и другими элементами объединенной архитектуры. Сценарии автоматизации могут быть легко импортированы и экспортированы.

Сервисы безопасности

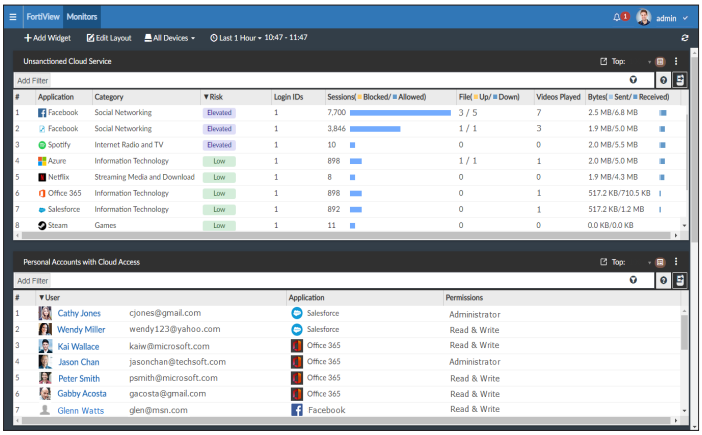
Подписка FortiSOC для FortiAnalyzer предоставляет функционал встроенного управления инцидентами и наборы автоматизированных сценариев реагирования (FortiSOC playbook).

Подписка FortiGuard Indicators of Compromise (IOC) предоставляет FortiAnalyzer доступ к информации о 500 тыс. индикаторах компрометации ежедневно. Это позволяет осуществлять поиск новых маркеров вирусных заражений, аномалий, атак злоумышленников в собранных с средств защиты событиях безопасности.

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Сервис мониторинга теневого ИТ позволяет обнаружить использование некорпоративных устройств и ресурсов, несанкционированных учетных записей, несогласованное использование SaaS, IaaS сервисов, API интеграций, приложений сторонних производителей и пользователей, несанкционированно использующих активы компании.

Сервис FortiGuard Outbreak alert автоматически загружает пакеты для обнаружения новых образцов вредоносного кода с описанием принципов их работы, информирует о возможностях противодействия с помощью компонентов Fortinet Security Fabric (например, какие сервисы FortiGate NGFW блокируют конкретную угрозу).



Аналитика Fortinet Security Fabric

Аналитика и отчетность

Командам информационной безопасности необходим инструмент проактивной аналитики и отчетности для обеспечения максимальной видимости сети, устройств и активности пользователей, способный обеспечить автоматизацию противодействия попыткам проникновения.

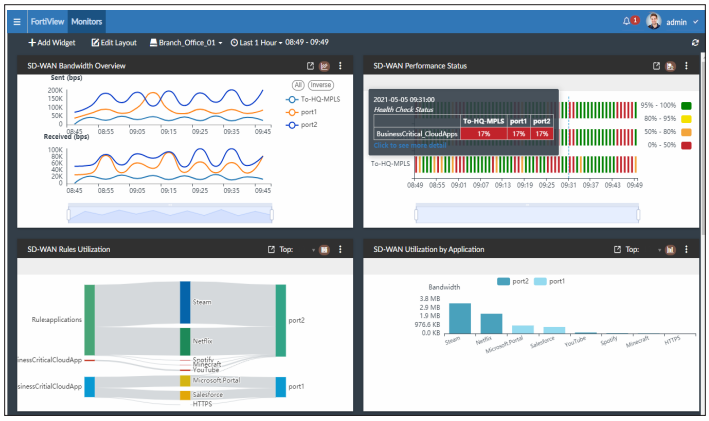
FortiAnalyzer сопоставляет данные журналов безопасности с информацией об угрозах и проводит анализ как в режиме реального времени, так и в исторической ретроспективе. FortiAnalyzer собирает воедино риски, сетевую активность, уязвимости, попытки атак, аномалии, мониторинг пользовательской активности, признаки теневого ИТ.

Управление активами

FortiAnalyzer предоставляет инструмент для идентификации и мониторинга активов, с которых собираются журналы событий операционной деятельности и безопасности. Наборы фильтров и алгоритмов корреляции событий связывают информацию и пользователях, устройствах, угрозах и атаках воедино.

FortiView - это продвинутое решение для мониторинга, визуализации и оперативной работы с событиями безопасности и оповещениями в реальном времени. Расширенные фильтры позволяют эффективно приоритезировать большой входящий поток данных о приложениях, SaaS сервисах, обнаруженных ботнетах и командных центрах, сетевой активности, стабильности работы VPN сервисов и т.д.

Тематические дашборды и виджеты NOC/SOC специально разработаны для отображения на разных широкоформатных экранах центров мониторинга и реагирования. В режиме реального времени отслеживается и визуализируется информация о проводной и беспроводной инфраструктуре, SD-WAN, VPN, приложениях, порталах, угрозах, теневому ИТ, инвентаризации ПО, уязвимостях.



Аналитики могут продолжить расследование инцидентов в разделе отображения деталей событий. Инструмент позволяет группировать устройства, источники информации, накладывать множественные расширенные фильтры, работать с форматированными и исходными сообщениями журналов, создавать собственные кастомизированные формы представления.

Лицензия FortiSOC позволяет в автоматическом режиме проводить нормализацию событий в рамках административных доменов внутри FortiAnalyzer.

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Отчеты FortiAnlayzer

FortiAnalyzer предоставляет более 60 шаблонов отчетов, более 800 наборов данных и более 750 диаграмм, готовых к использованию с примерами отчетов, включая направления SD-WAN, VPN, оценку рисков, ситуационную осведомленность, индикаторы рисков, пропускную способность и приложения, FortiClient, FortiMail, FortiSandbox, FortiDeceptor, соответствие требованиям и многие другие.

Аналитики могут легко настраивать, клонировать и изменять отчеты в соответствии со своими потребностями с помощью фильтров по устройствам, подсетям и типам, чтобы предоставлять конкретные бизнес-показатели целевым заинтересованным сторонам. Запланируйте запуск отчетов в непиковые часы или по требованию, определите профили для уведомлений и генерируйте отчеты в распространенных форматах, включая PDF, HTML, CSV и XML.

Варианты развертывания

Deploying FortiAnalyzer

FortiAnalyzer играет ключевую роль в архитектуре безопасности Fortinet и может быть развернут в различных конфигурациях, чтобы наилучшим образом удовлетворить потребности любой организации в аналитике, резервном копировании, аварийном восстановлении и хранении, доступности и резервировании, а также в сборе и пересылке журналов для распределенных сетей с большим количеством журналов событий.

FortiAnalyzer в режиме высокой доступности (HA)

FortiAnalyzer поддерживает инсталляцию в режиме высокой доступности. В случае сбоя основного (активного) FortiAnalyzer вторичный (пассивный) FortiAnalyzer (кластер до четырех узлов) немедленно перехватит на себя все функции основной ноды кластера, исключая сценарий единой точки отказа.

Мультитенантность с разграничением ресурсов

FortiAnalyzer поддерживает работу с множественными административными доменами, позволяет создавать древовидную ролевую модель управления с разграничением прав, квотами, политиками.

Режимы Analyzer и Collector

FortiAnalyzer поддерживает два режима работы: Analyzer и Collector. Основное назначение режима Collector - первичный сбор журналов, архивирование и перенаправление на ноду с ролью Analyzer. Такая архитектура существенно повышает производительность системы в целом, позволяя сосредоточить все ресурсы Analyzer ноды на аналитике, операционной деятельности и подготовке отчетов.

Помимо повышения производительности архитектура с множеством нод в режимах Analyzer и Collector реализует отказоустойчивость, расширение общего объема хранения журналов, а также снижает общее время реакции на инциденты со стороны команд эксплуатации.

Интеграции с решениями сторонних производителей

FortiAnalyzer позволяет перенаправлять журналы на сторонний syslog сервер, CEF сервер или другой FortiAnalyzer. При перенаправлении FortiAnalyzer также может сохранять и архивировать на себе локальную копию собираемых журналов. Журналы перенаправляются в режиме реального времени.

Доверенный аппаратный модуль (TPM) шифрования

Устройства FortiAnalyzer G серии имеют доверенный аппаратный модуль (TPM). Он представляет собой микроконтроллер для генерации, хранения и аутентификации криптографических ключей. Это позволяет обеспечить дополнительную аппаратную защиту от атак злоумышленников на систему аналитики и обработки журналов безопасности.

Облачные сервисы

FortiAnalyzer в облаке

FortiAnalyzer может поставляться в виде SaaS сервиса, реализуемого производителем. Сервис именуется FortiAnalyzer Cloud и реализует основной функционал стандартного FortiAnalyzer применительно к Fortinet NGFW и SD-WAN в облаке, не требуя приобретения программно-аппаратного комплекса или выделения ресурсов для виртуальной машины в среде виртуализации.

ВИРТУАЛИЗАЦИЯ

FortiAnalyzer VM

Виртуальные машины FortiAnalyzer представляют собой виртуальную версию аппаратного устройства и предназначены для работы на многих платформах виртуализации. Они позволяют организациям упростить централизованное управление журналами событий, автоматизировать рабочие процессы и помочь командам NOC и SOC выявлять угрозы и реагировать на них. Виртуальные машины FortiAnalyzer доступны как по подписке, так и по постоянным лицензиям.

FortiAnalyzer VM-S (подписка)

Подписочная модель лицензирования FortiAnalyzer объединяет в одну позицию стоимость виртуальной машины, технической поддержки FortiCare, сервисы индикаторов компрометации (IOC) и SOC (SOAR /SIEM), чтобы упростить покупку, обновление и продление продукта.

FortiAnalyzer-VM-S предоставляет организациям централизованный анализ событий безопасности, расследование инцидентов, отчетность, архивирование журналов, интеллектуальный анализ данных, карантин вредоносных файлов и оценку уязвимостей. Централизованный сбор, сопоставление и анализ географически и хронологически разрозненных событий безопасности с устройств Fortinet и сторонних производителей помогает организациям консолидировать и визуализировать информацию о текущем состоянии инфраструктуры информационной безопасности.

Подписки на виртуальные машины FortiAnalyzer лицензируют объем принимаемых журналов событий по 5, 50 и 500 Гбайт в день, позиции стекируются.

FortiAnalyzer VM (постоянная лицензия)

Fortinet предлагает постоянные лицензии на виртуальные машины FortiAnalyzer с дополнительными подписками на техническую поддержку 24x7 FortiCare и сервис поставки индикаторов компрометации FortiGuard (IOC).

Решение поддерживает широкий список платформ виртуализации.

ХАРАКТЕРИСТИКИ

FORTIANALYZER ВИРТУАЛЬНЫЕ УСТРОЙСТВА	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100	FAZ-VM-GB500	FAZ-VM-GB2000
Производительность						
Гбайт логов в день	+1	+5	+25	+100	+500	+2,000
Объем хранилища	+500 Гбайт	+3 Тбайт	+10 Тбайт	+24 Тбайт	+48 Тбайт	+100 Тбайт
Устройств/VDOM (максимум)	10,000	10,000	10,000	10,000	10,000	10,000
Удаленное управление устройством	✓	✓	✓	✓	✓	✓
Виртуальная машина						
Индикаторы компрометации FortiGuard (IOC)				✓		
SOC подписка				✓		
Виртуальная машина						
Поддержка гипервизоров	Актуальный список поддерживаемых гипервизоров приведен в Release notes. Перейдите по ссылке https://docs.fortinet.com/product/fortianalyzer/ для получения доступа к Release notes (внизу страницы). Перейдите в раздел "Product Integration and Support" → "FortiAnalyzer [version] support" → "Virtualization"					
vCPU (Минимум / Максимум)	4 / Неограничено					
Сетевые интерфейсы (Мин. / Макс.) [5]	1 / 4					
Память (Минимум / Максимум)	8 Гбайт / для 64-бит неограничено					

* Неограничено Гбайт в день при инсталляции в режиме Collector

ХАРАКТЕРИСТИКИ



УСТРОЙСТВА FORTIANALYZER	FAZ-150G	FAZ-300G	FAZ-800G
Производительность			
Гбайт логов в день	25	100	200
Установившаяся скорость обработки в режиме аналитки (событий в секунду)*	500	2,000	4,000
Установившаяся скорость обработки в режиме Collector (событий в секунду)*	750	3,000	6,000
Устройства/VDOMs (Максимум)	50	180	800
Максимальное количество дней в режиме аналитики**	90	28	50
Поддерживаемые опции			
Индикаторы компрометации FortiGuard (IOC)	✓	✓	✓
SOC подписка	✓	✓	✓
Сервис оповещений FortiGuard Outbreak Alert	✓	✓	✓
Enterprise комплект сервисов безопасности	✓	✓	✓
Hardware комплект поставки	✓	✓	✓
Характеристики аппаратной платформы			
Форм-фактор	Настольный	Монтаж в стойку, 1 RU	Монтаж в стойку, 1 RU
Всего сетевых интерфейсов	2 x RJ45 GE	4 x RJ45 GE	4 x RJ45 GE, 2 x SFP
Объем хранилища	4Тбайт (2× 2Тбайт)	8 Тбайт (2 × 4 Тбайт)	16 Тбайт (4 × 4 Тбайт)
Доступное хранилище (после сборки RAID)	2 Тбайт	4 Тбайт	8 Тбайт
Съемные жесткие диски	No	No	✓
Поддерживаемые RAID массивы	0/1	RAID 0/1	RAID 0/1,1s/5,5s/10
Тип RAID	Программный	Программный	Аппаратный / Горячая замена
RAID массив по умолчанию	1	1	10
Резырвный источник питания с горячей заменой	Нет	Нет	Опционально
Размеры			
Высота x Ширина x Длина (дюймы)	9.5 × 3.5 × 8	1.73 × 17.24 × 16.38	1.73 × 17.32 × 21.65
Высота x Ширина x Длина (см)	24.1 × 8.9 × 20.55	4.4 × 43.8 × 41.6	4.4 × 44.0 × 55.0
Вес	9.35 фунтов (4.24 кг)	22.5 фунтов (10.2 кг)	25.75 фунтов (11.68 кг)
Условия эксплуатации			
Источник питания	100–240В AC, 50–60 Гц	100–240В AC, 50–60 Гц	100–240В AC, 50–60 Гц
Потребляемая мощность (Средняя / Максимальная)	36Вт / 43Вт	90.1Вт / 99Вт	134Вт / 174.2Вт
Тепловыделение	147.4 БТЕ/час	337.8 БТЕ/час	594.4 БТЕ/час
Рабочая температура	32–104° F (0–40° C)	32–104° F (0–40° C)	32–104° F (0–40° C)
Температура хранения	-4–167° F (-20–75° C)	-13–167° F (-25–75° C)	-4–167° F (-20–75° C)
Влажность	от 5 до 95% без конденсата	от 20 до 90% без конденсата	от 5 до 95% без конденсата
Высота над уровнем моря	до 7,400 футов (2,250 м)	до 7,400 футов (2,250 м)	до 7,400 футов (2,250 м)
Соответствие требованиям			
Сертификаты безопасности	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB

* Установившаяся скорость обработки - Максимальная постоянная скорость обработки сообщений, которую FAZ устройство может поддерживать в течение 48 часов без деградации производительности системы и SQL базы.
** Максимальное количество дней сбора событий, постоянно поступающих с установившейся скоростью обработки. Значение будет больше, если среднее количество сообщений будет меньше.

ХАРАКТЕРИСТИКИ




УСТРОЙСТВА FORTIANALYZER	FAZ-1000F	FAZ-3000G	FAZ-3500G	FAZ-3700G
Производительность				
Гбайт логов в день	660	3,000	5,000	8,300
Установившаяся скорость обработки в режиме аналитки (событий в секунду)*	20,000	42,000	60,000	100,000
Установившаяся скорость обработки в режиме Collector (событий в секунду)*	30,000	60,000	90,000	150,000
Устройства/VDOMs (Максимум)	2,000	4,000	10,000	10,000
Максимальное количество дней в режиме аналитики**	34	30	38	60
Поддерживаемые опции				
Индикаторы компрометации FortiGuard (IOC)	✓	✓	✓	✓
SOC подписка	✓	✓	✓	✓
Сервис оповещений FortiGuard Outbreak Alert	✓	✓	✓	✓
Enterprise комплект сервисов безопасности	✓	✓	✓	✓
Hardware комплект поставки	✓	✓	✓	✓
Характеристики аппаратной платформы				
Форм-фактор	Монтаж в стойку, 2 RU	Монтаж в стойку, 3 RU	Монтаж в стойку, 4 RU	Монтаж в стойку, 4 RU
Всего сетевых интерфейсов	2 × 10GbE RJ45, 2 × 10GbE SFP+	2 x GE RJ45, 2× 25GE SFP28	2 x GE RJ45, 2× 25GE SFP28	2 × 10GE RJ-45 + 2 × 25GE SFP28
Объем хранилища	32 Тбайт (8 × 4 Тбайт)	64 Тбайт (16 × 4Тбайт)	96 Тбайт (24 × 4 Тбайт)	240 Тбайт (60 × 4 Тбайт) 3,5” HDD + 19.2 Тбайт (6 x 3.2 Тбайт) NVMe SSD
Доступное хранилище (после сборки RAID)	24 Тбайт	56 Тбайт	80 Тбайт	216 Тбайт
Съемные жесткие диски	✓	✓	✓	✓
Поддерживаымые RAID массивы	RAID 0/1,1s/5,5s/6,6s/10/50/60	RAID 0/1,1s/5,5s/6,6s/10/50/60	RAID 0/1,1s/5,5s/6,6s/10/50/60	RAID 0/1,1s/5,5s/6,6s/10/50/60
Тип RAID	Аппаратный / Горячая замена	Аппаратный / Горячая замена	Аппаратный / Горячая замена	Аппаратный / Горячая замена
RAID массив по умолчанию	50	50	50	50
Резырвный источник питания с горячей заменой	✓	✓	✓	✓
Размеры				
Высота x Ширина x Длина (дюймы)	3.5 × 17.2 × 25.6	5.2 × 17.2 × 25.5	7.0 × 17.2 × 26.0	7 × 17.2 × 30.2
Высота x Ширина x Длина (см)	8.9 × 43.7 × 65.0	13.0 × 44.0 × 65.0	17.8 × 43.7 × 66.0	17.8 × 43.7 × 76.7
Вес	34 фунтов (15.42 кг)	66.5 фунтов (30.15 кг)	90.75 фунтов (41.2 кг)	118 фунтов (53.5 кг)
Услови эксплуатации				
Источник питания	100–240В AC, 50–60 Гц	100-127В~/10А, 200-240В~/5А	100-240 В AC, 50-60 Гц	2000 Вт AC***
Потребляемая мощность (Средняя / Максимальная)	192.5Вт / 275 Вт	385 Вт / 500 Вт	629.5 Вт / 677.3Вт	850Вт / 1423.4 Вт
Тепловыделение	920 БТЕ/час	1350 БТЕ/час	2345.07 БТЕ/час	4858 БТЕ/час
Рабочая температура	50–95°F (10 – 35°C)	32 - 104°F (0 - 40°C)	41–95°F (5–35°C)	50–95°F (10–35°C)
Температура хранения	-40–140°F (-40–60°C)	-4 - 167°F (-20 - 75°C)	-40–140°F (-40–60°C)	-40–158°F (-40–70°C)
Влажность	от 8 до 90% без конденсата	от 5% до 95% без конденсата	от 8% до 90% без конденсата	от 8% до 90% без конденсата
Высота над уровнем моря	до 7,400 футов (2,250 м)	до 7,400 футов (2,250 м)	до 7,400 футов (2,250 м)	до 7,000 футов (2133 м)
Соответствие требованиям				

* Максимальная постоянная скорость обработки сообщений, которую FAZ устройство может поддерживать в течение 48 часов без деградации производительности системы и SQL базы.
** Максимальное количество дней сбора событий, постоянно поступающих с установившейся скоростью обработки. Значение будет больше, если среднее количество сообщений будет меньше.
***3700F должен быть подключен к электросети 200В - 240В.

ИНФОРМАЦИЯ ДЛЯ ЗАКАЗА

НАИМЕНОВАНИЕ	КОД ТОВАРА (SKU)	ОПИСАНИЕ
FortiAnalyzer	FAZ-150G	Устройство сбора и анализа логов — 2 x RJ45 GE, 4 Тбайт, до 25 Гбайт/день логов
	FAZ-300G	Устройство сбора и анализа логов — 4 x RJ45 GE, 8 Тбайт, до 100 Гбайт/день логов.
	FAZ-800G	Устройство сбора и анализа логов — 4 x GE, 2 x SFP, 16 Тбайт, до 200 Гбайт/день логов.
	FAZ-1000F	Устройство сбора и анализа логов — 2 × 10GE RJ45, 2 × 10GbE SFP+, 32 Тбайт, два блока питания, до 660 Гбайт/день логов.
	FAZ-3000G	Устройство сбора и анализа логов — 2 x GE RJ45, 2× 25GE SFP28, 64 Тбайт, два блока питания, до 3,000 Гбайт/день логов.
	FAZ-3500G	Устройство сбора и анализа логов — 2 x GbE RJ45, 2 x SFP28, 96 Тбайт, два блока питания, до 5,000 Гбайт/день логов.
	FAZ-3700G	Устройство сбора и анализа логов — 2 × 10GE RJ-45, 2 × 25GE SFP28, 240 Тбайт + 19.2 Тбайт NVMe SSD, до 8,300 Гбайт/день логов.
FortiAnalyzer-VM Subscription License with Support	FC1-10-AZVMS-465-01-DD	Подписка на централизованный сбор и анализ логов до 5 Гбайт/день. Включает поддержку 24×7 FortiCare, подписки IOC и SOC.
	FC2-10-AZVMS-465-01-DD	Подписка на централизованный сбор и анализ логов до 50 Гбайт/день. Включает поддержку 24×7 FortiCare, подписки IOC и SOC.
	FC3-10-AZVMS-465-01-DD	Подписка на централизованный сбор и анализ логов до 500 Гбайт/день. Включает поддержку 24×7 FortiCare, подписки IOC и SOC.
FortiAnalyzer-VM	FAZ-VM-GB1	Лицензия расширения, добавляет 1 Гбайт/день и 500 Гбайт емкости хранилища.
	FAZ-VM-GB5	Лицензия расширения, добавляет 5 Гбайт/день и 3 Тбайт емкости хранилища.
	FAZ-VM-GB25	Лицензия расширения, добавляет 25 Гбайт/день и 10 Тбайт емкости хранилища.
	FAZ-VM-GB100	Лицензия расширения, добавляет 100 Гбайт/день и 24 Тбайт емкости хранилища.
	FAZ-VM-GB500	Лицензия расширения, добавляет 500 Гбайт/день и 48 Тбайт емкости хранилища.
	FAZ-VM-GB2000	Лицензия расширения, добавляет 2 Тбайт/день и 100 Тбайт емкости хранилища.
FortiAnalyzer-Cloud*	FC-10-[Код модели FortiGate]-841-02-DD	360 Protection (FMG/FAZ Cloud, FortiCloud SOCaaS, IPS, AMP, App Ctrl, Web & Video Filtering, AS, Security Rating, IoT Detection, Industrial Security, SD-WAN Orchestrator, SD-WAN Cloud Monitoring, FortiConverter Svc и ASE FortiCare)
	FC-10-[Код модели FortiGate VM]-842-02-DD	360 Protection (FMG/FAZ Cloud, FortiCloud SOCaaS, IPS, AMP, App Ctrl, Web & Video Filtering, AS, Security Rating, IoT Detection, Industrial Security, SD-WAN Orchestrator, SD-WAN Cloud Monitoring, FortiConverter Svc и ASE FortiCare).
	FC1-10-AZCLD-463-01-DD	Increase FortiAnalyzer Cloud storage by 5 GB/Day for Central Logging & Analytics and FortiCloud SOCaaS. Include 24×7 FortiCare support, IOC and SOC subscription.
	FC2-10-AZCLD-463-01-DD	Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging & Analytics and FortiCloud SOCaaS. Include 24×7 FortiCare support, IOC and SOC subscription.
	FC3-10-AZCLD-463-01-DD	Increase FortiAnalyzer Cloud storage by 500 GB/Day for Central Logging & Analytics and FortiCloud SOCaaS. Include 24×7 FortiCare support, IOC and SOC subscription.
FortiAnalyzer - Backup to Cloud Service	FC-10-FAZ00-286-02-DD	Подписка на 1 год для FortiAnalyzer на коннектор к облачной системе хранения на 10 Тбайт.
FortiGuard Indicator of Compromise (IOC) Subscription	FC-10-[Код модели]-149-02-DD	Подписка на 1 год на индикаторы компрометации FortiGuard (IOC).
FortiAnalyzer SOC Subscription	FC-10-[Код модели]-335-02-DD	Подписка на функционал FortiAnalyzer SOC.
FortiAnalyzer-VM SOC Subscription Service	FC[Код Гбайт в день]-10-LV0VM-335-02-DD	Подписка на функционал FortiAnalyzer VM SOC.
FortiGuard Outbreak Alert Service	FC-10-[Код модели]-462-02-DD	Подписка на функционал FortiGuard Outbreak Alert Service.
FortiAnalyzer-VM Perpetual Outbreak Alerts Service	FC[Код Гбайт в день]-10-LV0VM-462-02-DD	Подписка на функционал FortiAnlayzer VM Perpetual FortiGuard Outbreak Alert Service.
Enterprise Protection Bundle	FC-10-[Код модели]-466-02-DD	Enterprise Protection (техническая поддержка 24×7 FortiCare, подписка на индикаторы компрометации FortiGuard и SOC).
Hardware Bundle	FAZ-[Модель устройства]-BDL-466-DD	Устройство, техническая поддержка 24×7 FortiCare, подписка FortiAnalyzer Enterprise Protection.

* Требует лицензию FortiCloud Premium Account. Смотрите сервисы для FortiGate (SOCaaS и другие облачные наборы).

FORTINET®

www.fortinet.com