

ТЕХНИЧЕСКОЕ ОПИСАНИЕ

Кибербезопасность розничных сетей с Fortinet

Защита ритейлеров от продвинутых угроз
при обеспечении качественного
обслуживания клиентов



Основные положения

Fortinet предлагает ритейлерам широкий набор сетевых технологий и технологий безопасности, которые легко интегрируются и автоматизируются с помощью системы Fortinet Security Fabric. Торговым сетям, перед которыми стоят разнообразные задачи — от создания омниканальных магазинов до повышения эффективности бизнес-операций, — Fortinet предлагает пути решения основных вопросов сетевой инфраструктуры и безопасности. Высокопроизводительные решения Fortinet с лучшими в своем классе сетевыми функциями и функциями обеспечения безопасности справляются с широким спектром задач в области розничной торговли.

Благодаря глубокой интеграции с Fortinet Security Fabric, которая защищает все уязвимые для атак узлы в розничной торговле, а также с системой обнаружения угроз на базе искусственного интеллекта (ИИ) от Лаборатории FortiGuard, Fortinet анализирует данные в облачных хранилищах и на локальных носителях, от штаб-квартир до удалённых объектов и филиалов. Это обеспечивает ритейлерам прозрачную видимость, рабочие процессы безопасности в режиме реального времени, а также обмен информацией об угрозах. Такой уровень интеграции невозможен без автоматизации, которая в свою очередь позволяет сетевым службам и службам безопасности работать эффективнее и быстрее, а также снижать риски. Всё это — при низкой совокупной стоимости владения (ССВ).

Введение

Розничные сети — лакомая цель для киберпреступников. Данные платежных карт клиентов передаются по сети и оседают в публичных и частных облачных хранилищах. В то же время внедрение омниканального обслуживания клиентов создаёт сложности в филиалах сетей: клиенты ждут высокой производительности и безопасного соединения, в то время как ритейлеры собирают информацию о поведении клиентов, которую можно использовать для повышения вовлеченности. Столкнувшись с острой нехваткой кадров в области кибербезопасности, ритейлеры изо всех сил стараются закрыть все пробелы в безопасности. Распространение точечных продуктов безопасности и множество новейших угроз лишь усугубляют картину.

Кибербезопасность розничных сетей: ключевые особенности подхода в рамках Fortinet Security Fabric.

Fortinet позволяет ритейлерам решать проблемы с помощью Fortinet Security Fabric: эта система обеспечивает одновременно бесперебойную интеграцию всех аспектов безопасности, автоматизацию рабочих процессов и анализ угроз. Кроме того, предварительно сконфигурированные коннекторы Fabric Connectors дают ритейлерам возможность интегрировать решения сторонних производителей с экосистемой Fabric, а архитектура открытого программного интерфейса (API) Fortinet Security Fabric позволяет легко и быстро добавлять другие решения безопасности.

Ключевые характеристики решений Fortinet для кибербезопасности розничной торговли:

Видимость

Благодаря Fortinet Security Fabric ритейлеры получают централизованный обзор и контроль над всеми продуктами по обеспечению безопасности точек, развернутых в их сети. Встроенные коннекторы и открытая структура API позволяют интегрировать и управлять всеми инструментами безопасности.

Автоматизация

Решения Fortinet поддерживают автоматическое обнаружение угроз, детектирование в соответствии с прописанными правилами и формирование отчетов о соответствии нормативным требованиям. Всё это повышает эффективность работы ИТ-персонала розничной сети. Автоматизация включает в себя готовые рабочие процессы и отчетность в соответствии с отраслевыми стандартами, такими как: стандарт безопасности данных индустрии платежных карт (PCI DSS), стандарт безопасности Национального института стандартов и технологий (NIST), нормативы по защите от киберугроз (Cybersecurity Framework).



За прошедший год хотя бы одному злонамеренному вторжению подверглись 87% розничных компаний, а больше половины столкнулись с тремя вторжениями¹.

Согласно исследованию Fortinet, 11 из 13 ритейлеров, входящих в список 'Fortune 100', используют решения нашей компании для защиты своих сетей.

Проактивное распознавание угроз

Система распознавания угроз, работающая на базе ИИ и машинного обучения, передает информацию в систему информационной безопасности Security Fabric в режиме реального времени, останавливает быстро развивающиеся угрозы, которые развертываются в облаке, целятся на системы PoS и другую инфраструктуру розничной сети.

Высокая производительность

Межсетевые экраны следующего поколения FortiGate (NGFW) обеспечивают самую низкую в отрасли задержку и позволяют проводить глубокую проверку зашифрованного трафика на уровне защищенных сокетов (SSL)/безопасности транспортного уровня (TLS) с минимальным влиянием на производительность сети по скорости или пропускной способности². Для розничной торговли, где потребители ожидают высокую производительность от каждой точки взаимодействия с компанией, это очень важно.

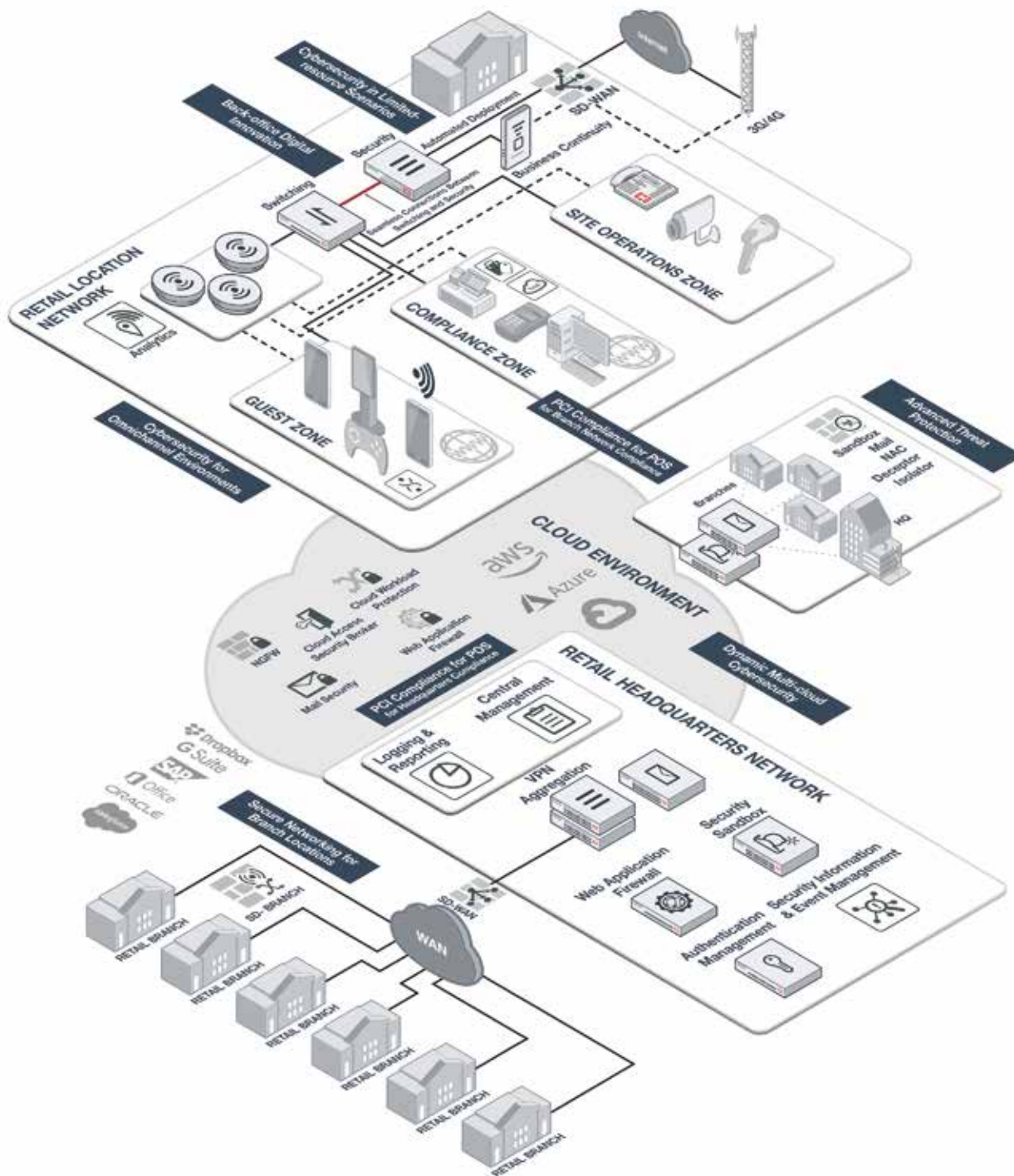


Рисунок 1: Решения Fortinet для кибербезопасности ритейла защищают всю сеть организации — от PoS-устройств до облачной инфраструктуры, — помогая поддерживать соответствие PCI DSS и другим нормам и стандартам.

Варианты использования

Решения Fortinet позволяют розничным сетям решать многие задачи. Среди них:

Кибербезопасность для омниканальной среды

Ритейлеры могут использовать Fortinet, чтобы обеспечить потребителям гибкий и персонализированный шопинг в магазине, сохраняя при этом сетевую безопасность и собирая ценную бизнес-аналитику. Гостевые беспроводные сети включают в себя портал для входа в социальные сети, а расширенная аналитика присутствия и позиционирования посетителей позволяет динамически размещать рекламу на основе местоположения.

Fortinet предлагает ритейлерам широкий портфель решений для защиты омниканальной среды, начиная с систем FortiGate Secure SD-WAN и Fortinet Secure SD-Branch, которые объединяют безопасность и сетевые технологии в филиалах сети в единое решение, обеспечивающее низкую совокупную стоимость владения при высокой производительности. FortiFone и FortiVoice предоставляют ритейлерам возможности автоматической настройки IP-телефонии (VoIP), которая подключена непосредственно к сети. FortiPresence позволяет мгновенно отправлять покупателю специальные предложения, основанные на анализе местоположения. FortiMail защищает учетные записи электронной почты клиентов и сотрудников, обеспечивая защиту систем от вирусов-вымогателей и других угроз, которые могут негативно сказаться на качестве обслуживания клиентов.

Кибербезопасность в условиях ограниченных ресурсов

Бывает, что магазины розничной сети находятся очень далеко друг от друга, у них могут быть разные потребности в безопасности и сетевом доступе. Масштабирование розничных операций при нехватке квалифицированных ресурсов для кибербезопасности требует большей эффективности за счет автоматизации и централизации.

В такой ситуации решения Fortinet позволяют ритейлерам обеспечить безопасность всех своих торговых точек без необходимости держать специалистов на местах. С помощью FortiDeploy можно предварительно настроить решения для обеспечения безопасности и завершить настройку автоматически, как только сеть и устройства безопасности окажутся на месте назначения. Межсетевой экран нового поколения FortiGate обеспечивает централизованный обзор и контроль над инфраструктурой безопасности в каждой конкретной точке. С помощью FortiManager и FortiAnalyzer ритейлеры получают полный обзор сетей, охватывающих более 10 000 точек, управляют конфигурациями и политиками безопасности распределенных розничных точек с помощью единого веб-интерфейса.

Соответствие точки продаж стандарту PCI

С Fortinet проще придерживаться стандарта PCI DSS. Централизованный обзор всех запущенных POS-устройств и предварительно настроенные шаблоны отчетности PCI DSS значительно снижают неавтоматизированные процессы и накладные расходы, связанные с демонстрацией соответствия нормативным требованиям. Fortinet Security Fabric предоставляет телеметрическую информацию в реальном времени для решений Fortinet и экосистемы партнеров Fabric с помощью встроенных коннекторов. Открытая платформа API предоставляет ритейлерам средства для быстрой и простой интеграции дополнительных решений сторонних партнеров в Security Fabric.

С помощью FortiManager и FortiGate NGFW ритейлеры могут автоматически находить и идентифицировать устройства в сети, а также централизованно управлять и обеспечивать соблюдение таких нормативных требований, как PCI DSS. FortiAnalyzer предоставляет готовые шаблоны отчетов PCI DSS и полную ретроспективную прозрачность сети. Это упрощает аудит и отчетность по PCI DSS и ряду других правил и стандартов.



Лаборатории FortiGuard ежедневно анализируют более 100 миллиардов нарушений безопасности³.



Типы атак на розничные сети⁴ (за последние 12 месяцев)

- Вредоносная программа: 50%
- Шпионское ПО: 44%
- DDoS-атаки: 36%
- Фишинг: 24%
- Внутренние угрозы: 23%
- Взлом мобильной связи: 23%
- Вирус-вымогатель: 23%
- Уязвимость нулевого дня: 17%
- Внедрение SQL-кода: 15%
- Атака через посредника: 11%

Влияние атак на розничную торговлю⁵ (за последние 12 месяцев)

- 42%: ухудшилась узнаваемость бренда
- 40%: перебои в работе, которые повлияли на доходы
- 39%: перебои в работе, которые повлияли на производительность
- 33%: перебои в работе, которые поставили под угрозу физическую безопасность
- 30%: потеря критически важных данных

Защищённая сеть для филиалов

Ритейлеры нуждаются в быстром и масштабируемом подключении для обеспечения бесперебойных операций по поддержке продаж, инвентаризации, закупок и других видов деятельности. Решения Fortinet предлагают высокоскоростную и надежную внутримагазинную сеть для поддержки надлежащего обслуживания клиентов, а также безопасную сеть SD-WAN для эффективной маршрутизации трафика между розничными торговыми точками и облачной инфраструктурой без ущерба для безопасности.

В дополнение к этому, ритейлеры могут повысить эффективность за счет консолидации архитектуры сети и безопасности, централизации обзора и управления устройствами и оптимальной маршрутизации более 5000 типов трафика приложений через FortiGate Secure SD-WAN и Fortinet Secure SD-Branch. Далее, такие решения для автоматической настройки, как FortiVoice и FortiFone, обеспечивают VoIP-коммуникацию непосредственно по сети. Для устойчивости бизнеса FortiExtender обеспечивает 100% бесперебойную работу подключения, используя резервное копирование 3G/4G, интегрированное с системой Secure SD-WAN.

Обнаружение продвинутых угроз

По данным исследования Fortinet, 87% розничных организаций пострадали от того или иного вторжения. Более того, анализ, проведенный лабораторией FortiGuard, показывает⁷, что до 40% новых вредоносных программ, обнаруженных в любой день, являются угрозами нулевого дня и/или неизвестными ранее. Ритейлеры, как обычно, должны выходить за рамки обнаружения угроз.

Лаборатория FortiGuard собирает данные об угрозах с помощью систем искусственного интеллекта и машинного обучения и передает её в систему информационной безопасности Fortinet Security Fabric в режиме реального времени, информируя службы безопасности на местах о новейших угрозах. FortiSandbox и FortiIsolator защищают сеть от потенциальных угроз, анализируя внешнее содержимое в изолированной среде перед входом в сеть. Системы FortiInsight и FortiDeceptor помогают ритейлерам находить внутренние угрозы на основе анализа поведения пользователей и организаций (UEBA), а также с помощью использования приманок, предназначенных для привлечения злоумышленников.

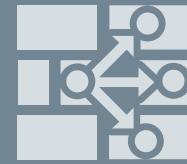
Цифровые инновации резервных систем

Многие ритейлеры используют интернет вещей (IoT) и технологии радиочастотной идентификации (RFID) для рационализации процессов, связанных с инвентаризацией и логистикой. Эти дополнительные – и зачастую небезопасные – сетевые узлы расширяют возможности для атак на компанию. Ритейлерам приходится искать компромисс между безопасностью сетевых расширений и сдерживанием неоправданного увеличения расходов.

Экономически эффективно будет использовать Fortinet Secure SD-Branch для параллельной работы деловых и гостевых сетей, что позволяет изолировать устройства IoT от общедоступной сети Wi-Fi. FortiNAC автоматически обнаруживает IoT-устройства в сетях и обеспечивает централизованный обзор, контроль и автоматическое реагирование на распространённые угрозы. FortiAP обеспечивает высокоскоростной и надежный доступ к сети со встроенной защитой, которой можно централизованно управлять с помощью FortiGate NGFW, а также централизованный мониторинг коммутаторов на уровне портов с помощью FortiSwitch.

Динамическая мультиоблачная кибербезопасность для розничной торговли

Ритейлеры управляют большими сетями географически разбросанных филиалов, что делает использование облачных сервисов логичным выбором. Однако сетевая инфраструктура, которая распространяется на частные облака, публичные облака и локальные центры обработки данных, часто создает очень разрозненную среду, которую трудно защитить. Розничным сетям, которые работают с несколькими облачными средами, подойдёт решение Fortinet cloud security для централизованного обзора, управления конфигурацией и применения политик нескольких поставщиков облачной безопасности (CSP).



Fortinet Secure SD-WAN – это самое низкое в отрасли время задержки, а совокупная стоимость владения в 8 раз ниже, чем у конкурентов⁶.



Лаборатория FortiGuard обнаружила более 720 угроз нулевого дня, что больше, чем у любого другого поставщика систем безопасности⁸.




79% крупных предприятий и 78% предприятий малого и среднего бизнеса перенесли рабочие процессы в облако. 81% крупных предприятий и 72% предприятий малого и среднего бизнеса считают, что безопасность является основой этих принципов работы⁹.


Кроме того, ритейлеры могут централизовать обзор, управление конфигурацией и контроль доступа в несколько облачных сред, развернув системы FortiCASB и FortiCWP. FortiGate NGFW доступен в облаке в виде виртуальной машины (VM) или программного обеспечения как услуги (SaaS); система обеспечивает интегрированную защиту облачных развертываний. Облачную электронную почту и веб-приложения можно защитить от атак, установив FortiMail и FortiWeb, которые используют новейшие технологии и данные от лаборатории FortiGuard для защиты от современных и быстро развивающихся угроз.

Заключение

Сети розничной торговли находятся под постоянной угрозой, независимо от того, пытаются ли злоумышленники украсть финансовые данные клиентов или подорвать работу ритейлера. По мере того, как розничные сети усложняются, переходят на мультиоблачную инфраструктуру и развертывание устройств IoT в разных точках, решения Fortinet и Fortinet Security Fabric помогают ритейлерам обеспечить централизованный обзор и контроль – они необходимы для защиты сетей от меняющихся угроз и для соответствия нормативам. Используя решения Fortinet, ритейлеры могут интегрировать сетевые инфраструктуры и инфраструктуры обеспечения безопасности, обеспечив тем самым высокоскоростное и надежное подключение точек розничной торговли, а также получать ценные сведения о бизнесе, которые можно использовать для дальнейшего улучшения обслуживания клиентов.



Fortinet девять раз входила в список компаний, рекомендованных «NSS Labs» – чаще, чем любой другой поставщик систем безопасности¹⁰.



Согласно отчётам консалтинговой компании Gartner, посвящённым корпоративным межсетевым экранам, Fortinet является «лидером» отрасли¹¹.

¹ Результаты основаны на серии исследований, проведенных 'Fortinet' среди представителей розничной торговли/гостиничного бизнеса/туриндустрии.

Отчет об исследовании готовится к выпуску.

² [«Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests»](#), Fortinet, October 14, 2019. Проверено 18 апреля 2020.

³ [«FortiGuard Security Services»](#), Fortinet, October 2019. Проверено 18 апреля 2020.

⁴ Результаты основаны на серии исследований, проведенных «Fortinet» среди представителей розничной торговли/гостиничного бизнеса/туриндустрии.

Отчет об исследовании готовится к выпуску.

⁵ Там же.

⁶ [«Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests»](#), Fortinet, October 14, 2019. Проверено 18 апреля 2020.

⁷ [«Using AI to Address Advanced Threats That Last-Generation Network Security Cannot»](#), Fortinet, June 8, 2019. Проверено 18 апреля 2020.

⁸ [«FortiGuard Security Services»](#), Fortinet, October 2019. Проверено 18 апреля 2020.

⁹ [«RightScale 2019 State of the Cloud Report»](#), Flexera, 2019. Проверено 18 апреля 2020.

¹⁰ [«Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests»](#), Fortinet, October 14, 2019. Проверено 18 апреля 2020.

¹¹ «Rajpreet Kaur, et al., [«Magic Quadrant for Network Firewalls»](#), Gartner, September 17, 2019. Проверено 18 апреля 2020.