

РАЗРАБОТАНО для БЕЗОПАСНОЙ УДАЛЁННОЙ РАБОТЫ

Следующее поколение сетевого взаимодействия
и безопасности



Основание компании: ноябрь 2000 г.

Выпуск первого продукта: май 2002 г.

Fortinet IPO: ноябрь 2009 г.
NASDAQ: FTNT

Головной офис: Саннивейл,
Калифорния

Число сотрудников: 7,756

Прибыль за 2019 г.: \$2.16 млрд.
Обороты по счетам за 2019г.: \$2.60 млрд.

Прибыль за 2-й квартал 2020:
\$616 млн.

Обороты по счетам за 2-й квартал 2020: \$711 млн.

Прибыль на акцию за 2-й квартал 2020 (GAAP): \$0.68

Прибыль на акцию за 2-й квартал 2020 (Non-GAAP): \$0.82

Рыночная капитализация (30 июня 2020): \$22.2 млрд.
\$1.63 млрд. наличных средств без задолженностей

Объем поставленной продукции до настоящего времени: более 5.9 млн.

Количество клиентов: свыше 465,000

Клиенты, внедрившие SD-WAN: свыше 21,800

Международные патенты (31 марта 2020)

Выдано патентов: 682
На рассмотрении 195

Обзор

Миссия компании Fortinet заключается в создании инновационных и высокопроизводительных средств сетевой безопасности для защиты и упрощения информационно-технологической инфраструктуры клиентов. Мы являемся ведущим мировым поставщиком решений сетевой безопасности и SD-WAN, коммутации и беспроводного доступа, контроля доступа к сети, аутентификации, безопасности в публичном и частном облаках, безопасности конечных точек и усовершенствованных решений защиты от угроз на основе искусственного интеллекта для операторов связи, центров обработки данных, предприятий и распределенных офисов.



Цена акций

	1-й год	3-й год	5-й год	С момента IPO*
Позиция FTNT	1-я	1-я	1-я	1-я
FTNT	79%	267%	232%	2,096%
СНКР	-7%	-2%	35%	224%
PANW	13%	72%	31%	447%

Динамика цен на акции до 30/06/2020, Источник: FactSet

* FTNT IPO на 18/11/2009 - \$6.25; PANW IPO на 20/07/2012 - \$42. показатели СНКР с момента выхода FTNT на IPO.

Рост операционной маржи

Операционная прибыль - в среднем за четыре квартала



Источник: данные компании.

2-й квартал 2020:

Выручка от продаж решений сетевой безопасности SD-WAN впервые превысила 10% от общей выручки – во втором квартале этот показатель составил 12%.

Азиатско-Тихоокеанский регион 21%

Прибыль по регионам

2-й квартал 2020

Европа, Ближний Восток и Африка 37%

*Продажи FortiGate 100 серии в настоящее время классифицируются как Mid-range диапазон

Средняя ценовая категория* 44% Компании

Обороты по счетам FortiGate по сегментам

2-й квартал 2020

Высокая ценовая категория 35% Крупные компании, телеком, поставщики услуг

Базовые продукты* 21% МСБ, филиалы, ритейл

АТР 15%

Затраты на персонал по регионам

2-й квартал 2020

ЕБВА 27%

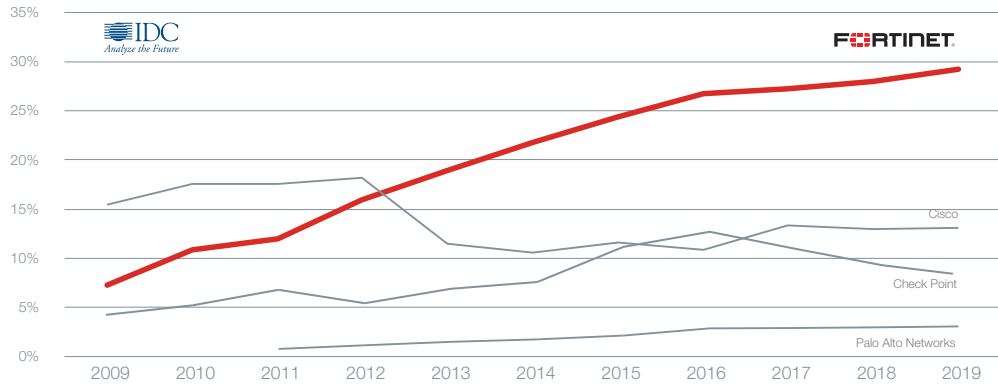
Северная и Южная Америка 58%

компания #1 ПО кибербезопасности В МИРЕ

#1 Самое большое количество проданных решений сетевой безопасности

~ 30 % всех поставок межсетевых экранов и решений UTM

Источник: IDC Worldwide Security Appliance Tracker, апрель 2020 г. (основано на ежегодных отгрузках межсетевых экранов, решений класса UTM и VPN)

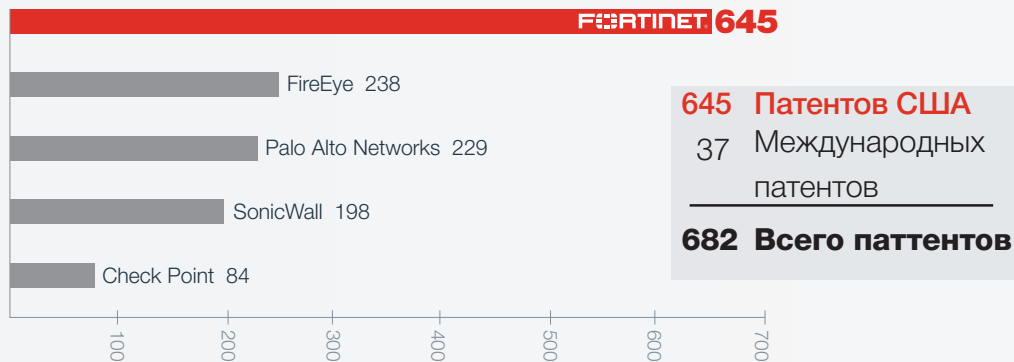


Источник: IDC Worldwide Security Appliance Tracker, апрель 2020 г. (основано на ежегодных отгрузках межсетевых экранов, решений класса UTM и VPN)

#1 В области инноваций

В 3 раза больше патентов, чем у других компаний по сетевой безопасности

Источник: Патентное ведомство США, по состоянию на 31 марта 2020 г.



#1 Самый широкий охват решений информационной безопасности

От Интернета Вещей до облака

Источник: оценки Fortinet, основанные на недавних аналитических исследованиях. Прогнозы на 2024 год.

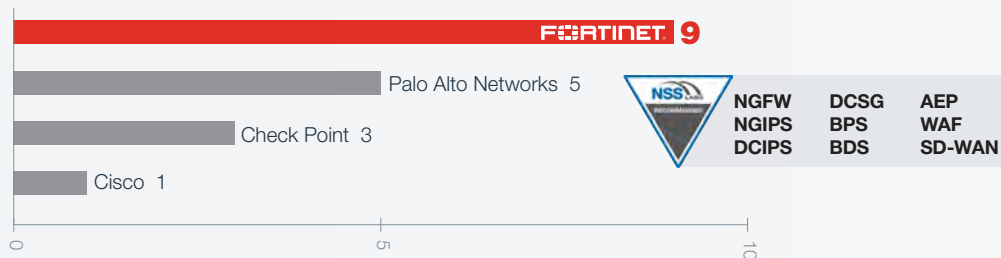


Общий объем целевого рынка: \$44 млрд. в 2020 г., прогнозируется рост до \$63 млрд. к 2024 г.

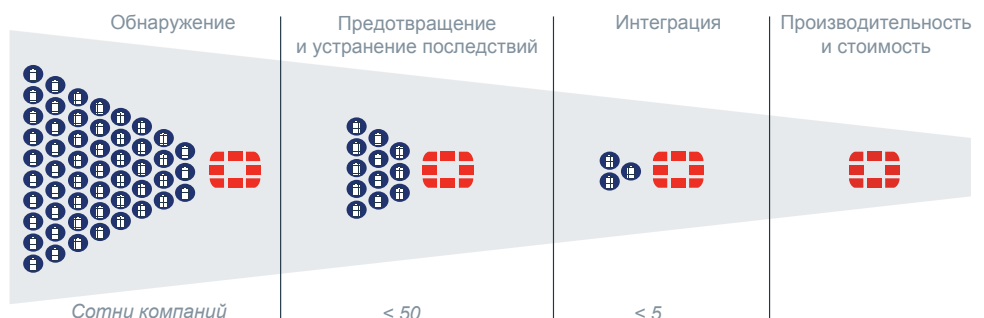
#1 Признанный лидер международных лабораторий

NSS Labs, ISCA, VB и др.

Источник: последние результаты испытаний NSS Labs по состоянию на июль 2020 года. Дополнительные сведения см. на страницах 10 и 11.

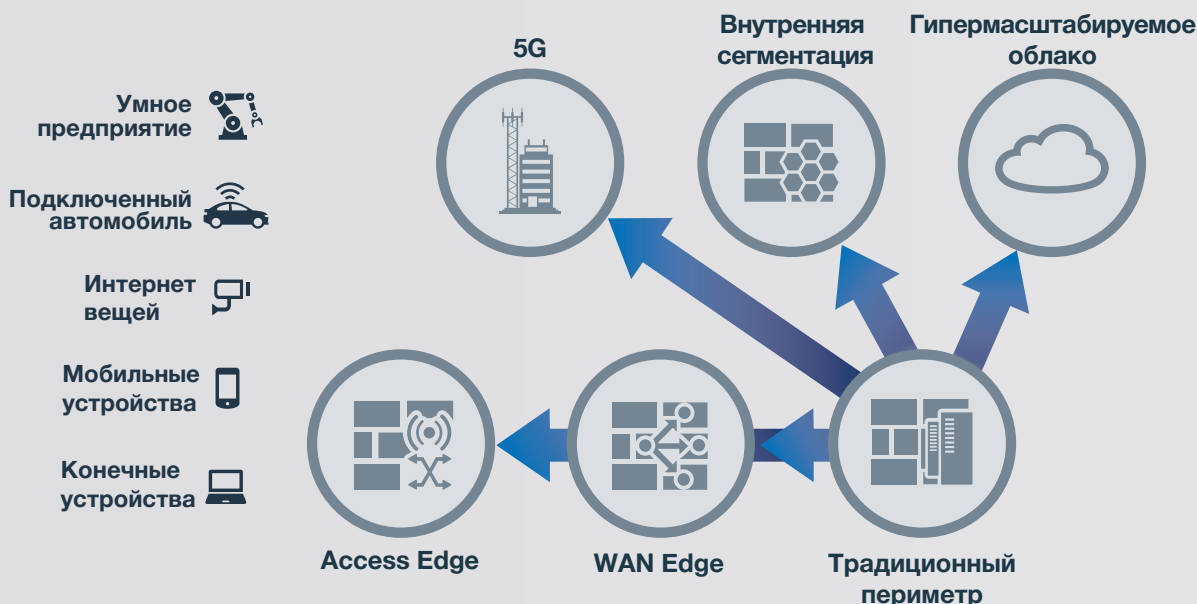


Единственная компания, занимающая ведущие позиции во всех ключевых аспектах сетевой безопасности



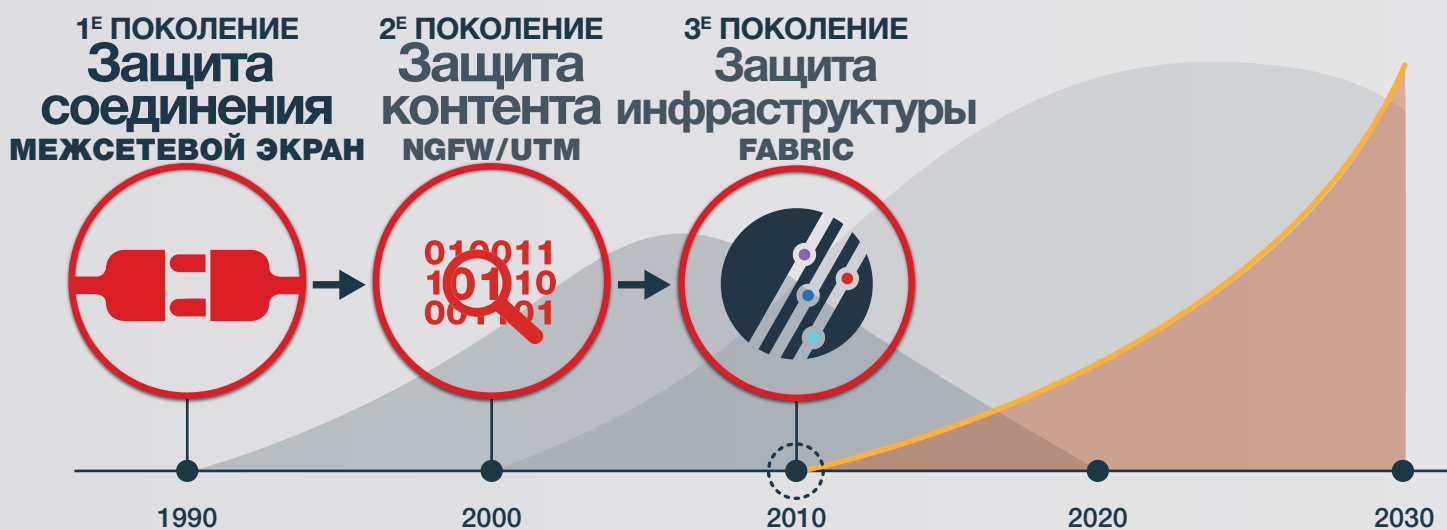
В ОСНОВЕ ЦИФРОВЫХ ИННОВАЦИЙ

Цифровые инновации быстро расширяют периметр



Сегодняшний периметр уже не так легко определить. Центр обработки данных был когда-то основной точкой входа и выхода вашей сети, но теперь быстрый рост новых подключенных устройств, сетей 5G и гипермасштабируемых облачных развертываний расширили периметр инфраструктуры.

Лидер сетевой безопасности



Первое поколение сетевой безопасности (межсетевые экраны с контролем состояния соединений) было ориентировано только на защиту соединения. Второе поколение сетевой безопасности (межсетевые экраны следующего поколения (NGFW) и унифицированное управление угрозами (UTM)), представленное компанией Fortinet, распространило контроль на приложения и контент. С появлением облачных технологий, Интернета вещей и мобильных устройств возникла необходимость в третьем поколении сетевой безопасности, которая обеспечивает сквозную сегментацию и защищает данные, пользователей и инфраструктуру везде.

Архитектура безопасности

Безопасность сети третьего поколения

Fortinet снова лидирует на рынке с Security Fabric, системой на основе открытого архитектурного подхода к безопасности, которая динамически адаптируется и защищает развивающуюся ИТ-инфраструктуру.

Глобальная

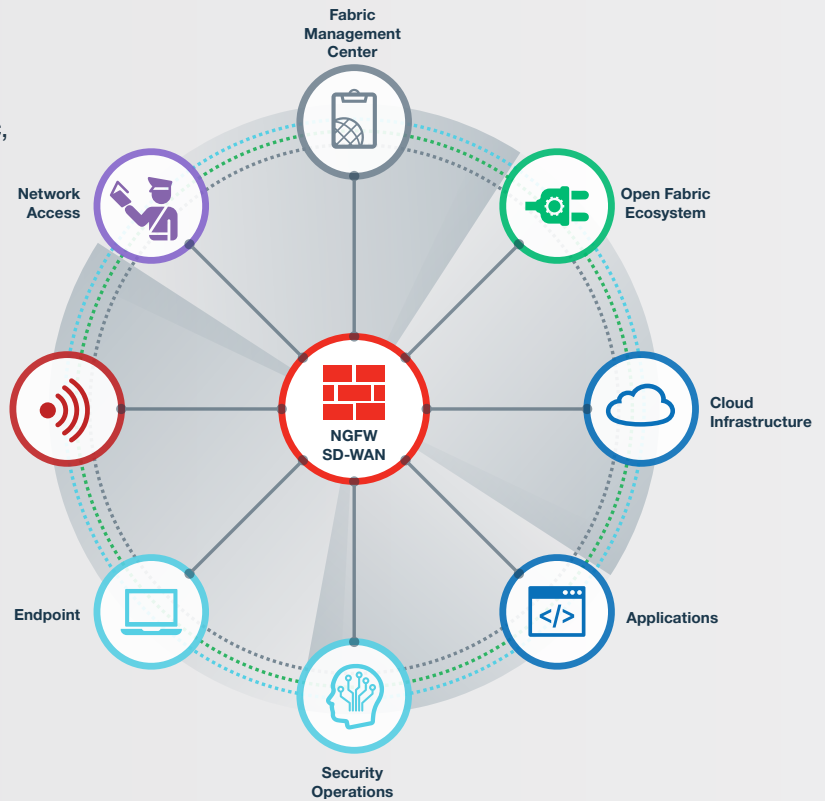
видимость всей поверхности цифровых атак для лучшего управления рисками.

Интегрированная

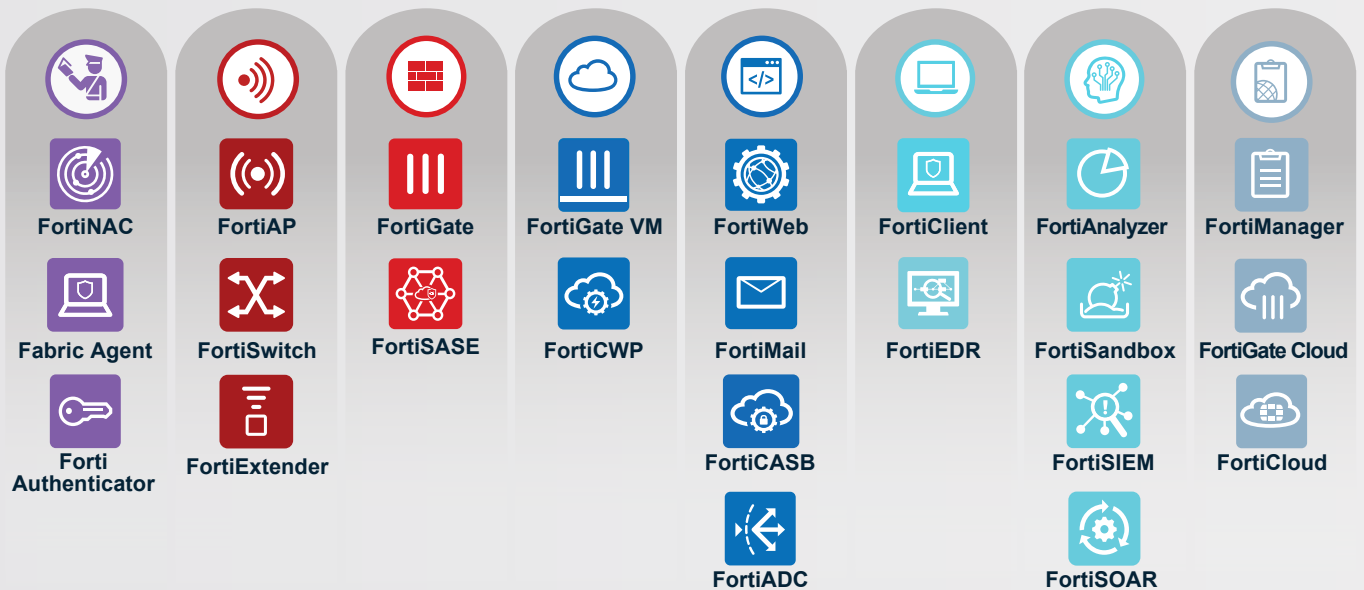
уменьшение поддержки нескольких разрозненных продуктов.

Автоматизированная

рабочие процессы для увеличения скорости операций и реагирования.



Полная защита всей поверхности цифровых атак



FortiGuard Services





Сетевая безопасность

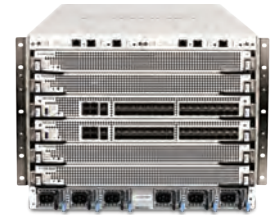
Высокопроизводительные межсетевые экраны FortiGate разработаны на базе специализированной ОС со встроенными процессорами системы безопасности и интегрированной аналитикой угроз от лаборатории FortiGuard, что обеспечивает консолидированную высокотехнологичную защиту сети от известных и неизвестных угроз.

Системы серий 5000 и 7000 на базе шасси

Форм-фактор	Расширяемое модульное шасси
Интерфейсы	10, 40, и 100 GE
Пропускная способность FW(TP)	Более 1 Тбит/с (до 189 Гбит/с)
Особенности	Операторский класс, NEBS, полное резервирование



FortiGate 5144C



FortiGate 7060E

Высокопроизводительные системы серий 1000 – 4000 и 6000

Форм-фактор	Системы 2RU – 5RU
Интерфейсы	10, 25, 40, и 100 GE
Пропускная способность FW(TP)	52 Гбит/с – 1 Тбит/с (4 Гбит/с – 100 Гбит/с)
Особенности	Сверхмалая задержка передачи данных, сверхвысокая скорость проверки SSL



FortiGate 2200E



FortiGate 6500F

Системы средней производительности серий 100-900

Форм-фактор	Системы 1RU – 2RU
Интерфейсы	1 и 10 GE
Пропускная способность FW(TP)	7 Гбит/с – 36 Гбит/с (1 Гбит/с – 7 Гбит/с)
Особенности	Высокая скорость проверки SSL



FortiGate 400E



FortiGate 600E

Системы начального уровня серий 30 – 90

Форм-фактор	Настольное устройство
Интерфейсы	1 GE повышенной плотности
Пропускная способность FW(TP)	1 – 4 Гбит/с (150 Мбит/с – 700 Мбит/с)
Особенности	Wi-Fi, PoE, специализированные защищенные варианты исполнения для сложных условий эксплуатации



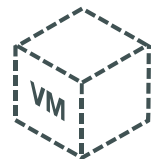
FortiGate 40F



FortiGate 60F

Межсетевые экраны виртуальной/частной облачной среды

	Частное облако	Публичное облако
Модели внедрения и интеграция	Все основные гипервизоры VMware, Cisco, OpenStack, Nuage, Nutanix, Azure Stack	AWS, Azure, Google, Oracle, IBM, Alibaba
Пропускная способность	Зависимость от аппаратного обеспечения	Зависимость от облачной среды
Лицензирование	Бессрочно, подписка, контроль потребления	BYOL или по требованию



Virtual Machine

Характеристики нового продукта — FortiGate 4400F

Первый в отрасли межсетевой экран для гипермасштабируемых центров обработки данных, 5G и гибридных ИТ-архитектур.

Feature / Performance	FortiGate 4400F*
Межсетевой экран	1,2 Тбит/с
Параллельные сеансы	600 миллионов**
Сеансов в секунду	10 миллионов**
IPsec VPN	420 Гбит/с
SSL проверка	65 Гбит/с
Интерфейсы	1G, 10G, 25G, 40G, 100G

* Результаты предварительного внутреннего тестирования Fortinet. Окончательные цифры могут меняться.

** При покупке дополнительной лицензии

*** Слоновый поток — одна сессия, в рамках которой потребляется большое количество полосы пропускания.



- Предоставляет масштабируемый доступ для удаленных работников
- Справляется со всплесками событийно-управляемых соединений
- Супермасштабируемая сегментация с аппаратно-ускоренным VXLAN
- Обеспечивает безопасную передачу больших массивов данных слоновыми потоками 100 Гбит/с***
- Предотвращение объемных атак с помощью аппаратного ускорения



Преимущество FortiOS

FortiOS представляет собой фундамент экосистемы Fortinet Security Fabric, в рамках которого консолидированы различные технологии и модели внедрения в рамках упрощенной единой стратегии и структуры управления. FortiOS предлагает клиентам непревзойденный уровень защиты, большую прозрачность и управляемость, простоту и повышенную операционную эффективность для защиты всей поверхности атаки.



NGFW



DCFW



CCFW



IPS



ISFW



SD-WAN



SWG



VPN/Scalable Remote Access



Преимущество процессора системы безопасности

Процессоры системы безопасности от компании Fortinet значительно повышают производительность, масштабируемость и пропускную способность решений Fortinet, позволяя существенно экономить пространство и потребление электроэнергии в сравнении с решениями на базе обычных ЦПУ. Было проведено сравнение производительности специализированного брандмауэра следующего поколения (NGFW) на базе ASIC компании Fortinet с продуктами других производителей NGFW и SD-WAN, которые используют стандартные процессоры для сетей и обеспечения безопасности. Как видно в приведённой таблице, FortiGate 4400F на базе процессора Fortinet NP7 показывает превосходные результаты.

Спецификация	FortiGate 4401F*	Средний показатель в отрасли***	Рейтинг безопасности	Palo Alto Networks PA-7050 ²	Check Point CP28000	Cisco FPR-4145	Juniper SRX5400 ³
Множественный экран	1.2 Тбит/с	165 Гбит/с	7x	N/A	145 Гбит/с	80 Гбит/с	270 Гбит/с
IPsec VPN	420 Гбит/с	39 Гбит/с	11x	28 Гбит/с	49 Гбит/с	18 Гбит/с	60 Гбит/с
Проверка SSL	65 Гбит/с	10 Гбит/с	6.5x	N/A	N/A	10 Гбит/с	N/A
Параллельные сеансы	600 млн***	46 млн	13x	32 млн	32 млн	30 млн	91 млн
Сеансов в секунду	10 млн*	822 тыс	12x	623 тыс	615 тыс	350 тыс	1.7 млн

Источник: Результаты тестов Fortinet. Информация из справочных материалов других вендоров. N/A означает, что поставщик не раскрывает технические характеристики производительности.

*Целевые показатели производительности. Конечные показатели производительности могут быть изменены

** Среднее значение по отрасли рассчитывается с использованием аналогичных решений в ценовых категориях от Palo Alto Networks, Check Point и Cisco.

*** При покупке дополнительной лицензии

Параллельная обработка на базе процессора Fortinet



Гибкая политика



Ускоряет сетевой трафик



Ускоряет проверку контента

Ускоряет проверку контента



Оптимизирован для SD-WAN и форм-факторов начального уровня



Преимущество аналитики по угрозам безопасности от лаборатории FortiGuard

Наша команда по исследованию угроз в лаборатории FortiGuard занимается аналитикой, которая передается на все решения Fortinet. В лаборатории FortiGuard применяются новейшие технологии машинного обучения и искусственного интеллекта для предоставления наивысшего уровня защиты на постоянной основе*, включая информацию о том, как противостоять сегодняшним угрозам для защиты наших заказчиков по всему миру. FortiGuard Labs сотрудничает с правоохранительными органами, правительственными организациями, с другими производителями решений ИБ, является членом альянсов, занимая тем самым лидерскую позицию в борьбе с новыми угрозами информационной безопасности, а также эффективно реагируя на возникающие угрозы безопасности по всему миру.

Сервисы по подписке

Сервис	Контроль приложений**	IPS	Расширенная защита от вредоносных программ**	Анти-спам	Веб-фильтрация	Повышенная безопасность	IoT Security	Служба рейтингов безопасности	Сервис FortiConverter	Управление IP-адресами	Облако FortiManager	Облако FortiAnalyzer	Функция облачного мониторинга SD-WAN	Функция VPN-контроля SD-WAN	Управление SD-WAN
Сервис 360	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Сервис Enterprise	x	x	x	x	x	x	x	x	x						
Сервис Унифицированное Управление Угрозами (UTM)	x	x	x	x	x										
Сервис защита от угроз	x	x	x												
Сервис a la carte		x	x		x	x	x	x		x	x	x	x	x	x

Услуги подписки FortiGuard

Другие услуги

*Из множества независимых сторонних тестов. Смотрите страницы 10-11. ** Контроль приложений входит в стандартную комплектацию каждого контракта на поддержку FortiCare.

*** Включает в себя AV, Antitbotnet, Mobile Security, Cloud Sandbox, Content Disarm и Reconstruction, и Virus Outbreak Protection.

Более 400 открытых экосистем



Коннекторы Connectors (12)

Разработанные Fortinet системы глубокой интеграции, позволяющие автоматизировать операции и безопасность

Alibaba Cloud AWS Aruba Cisco Google Cloud Azure ORACLE servicenow Symantec vmware



Fabric APIs (161)

Интеграции, разработанные партнерами с использованием Fabric API. Обеспечивают видимость и комплексные решения

ARISTA DELL IBM intel Lenovo Lightspeed Systems SIEMENS splunk> TERIDIUN TIGERA tufin



Fabric DevOps (9)

Системная инженерия, автоматизирующая запуск, настройку и управление сетью и системой безопасности

Alibaba Cloud AWS Google Cloud Terraform Azure openstack ORACLE Red Hat Ansible Automation Platform vmware



Расширенная экосистема безопасности (200+)

Сотрудничество с организациями, оповещающими об угрозах. Интеграция со сторонними продуктами

CYBER THREAT ALLIANCE MITRE STIX INTERPOL OT CSA Firewalls Switching Wireless Endpoint Security

Социальная ответственность компании Fortinet

Окружающая среда



Наш приоритет – экологическая устойчивость; подразумевает создание энергоэффективных продуктов и экологичных рабочих мест. И мы, и наши партнеры придерживаемся самых высоких стандартов в отношении экологически чистых продуктов, упаковки и переработки.

Бизнес и инновации



Миссия Fortinet - изобретать и разрабатывать лучшие технологии для защиты людей и организаций, обеспечивать цифровую конфиденциальность и защищать клиентов от нарушений безопасности. Мы - лидер в области общедоступной кибербезопасности и потому образовываем людей, чтобы улучшить их карьерные возможности, и защищаем наших клиентов, устраняя пробелы в их кибербезопасности.

Этичный менеджмент



Fortinet стремится вести бизнес этично и в соответствии со всеми законами. Наше корпоративное управление прозрачно; рекомендации для руководителей гарантируют подотчетность и выполнение наших обязательств перед акционерами и другими заинтересованными сторонами по обеспечению долгосрочной привлекательности компании.

Люди и сообщества



Fortinet создает разнообразную, инклюзивную, справедливую и безопасную рабочую среду - настоящую меритократию, где сотрудники могут полностью раскрыть свой потенциал. Мы также поддерживаем людей в разных концах света через наш благотворительный фонд, систему сводных благотворительных взносов сотрудник/компания, предоставляем сотрудникам оплачиваемые выходные и осуществляем просветительскую деятельность.

Подробнее на нашем сайте: www.fortinet.com

Наши меры по борьбе с COVID-19:

Fortinet защищает здоровье и благополучие сотрудников, помогает нуждающимся и пытается вместе с клиентами и партнерами облегчить работу в это непростое время. Предприняты следующие шаги:

Сотрудники: надлежащие меры по социальному дистанцированию, политика удаленной работы, профилактические санитарно-гигиенические меры, и многое другое

Обучение кибербезопасности: бесплатное онлайн-обучение безопасности для наших партнеров, клиентов и сообществ - чтобы защитить конечных пользователей, повысить навыки безопасности и компетенции.

Клиенты и партнеры: инновационные, масштабируемые заложенные возможности для быстрой защиты непрерывности бизнеса и безопасной удаленной работы.

Благотворительные обязательства: увеличение отчислений на благотворительность до 2 млн долларов; средства направляются в НКО, борющиеся с COVID-19.



Служба поддержки клиентов FortiCare предлагает глобальную техническую поддержку по всем продуктам Fortinet. Персонал поддержки FortiCare в Америке, Европе, России, странах Ближнего Востока и Азии обслуживает организации любого масштаба.



Professional Services



Premium RMA

ПОЛЕЗНЫЕ СВЕДЕНИЯ О СЕРВИСАХ И ПОДДЕРЖКЕ

360 Protection — это новый пакет поддержки и обслуживания, который обеспечивает расширенную поддержку, управление сетью в реальном времени и полный набор услуг безопасности и эксплуатации.



FortiCare

- 24x7 FortiCare
- Расширенная поддержка



FortiGuard

- Предприятие Bundle level



Функционал

- Облачная аналитика/управление
- SD-WAN related services
- FortiConverter

Обучение и сертификаты

Программа подготовки экспертов в области сетевой безопасности Fortinet (NSE) представляет собой 8-уровневую систему обучения и оценки, разработанную для клиентов, партнеров и сотрудников; до настоящего времени по программе выдано свыше **470 000** сертификатов.

Авторизованные учебные центры Fortinet (ATC) проводят обучение на местном языке на уровне экспертов в более чем **100** странах мира. Курсы предлагаются в классах и в виртуальных форматах, все курсы открыты для публичного зачисления.

Академия сетевой безопасности Fortinet предлагает зарекомендовавшую себя в отрасли программу обучения Fortinet с возможностью сертификации для специалистов по всему миру.

Начиная с 2016 года, эта инновационная, быстро развивающаяся программа уже реализована в **318** академиях в **82** странах мира.

- Подготовка к карьере в области сетевой безопасности
- Теоретические лекции и практические занятия в лаборатории
- Сертификация Fortinet



470,000+
СЕРТИФИКАТОВ



318
АКАДЕМИЙ



82
СТРАН

Углублённое бесплатное обучение кибербезопасности

Компания Fortinet делает доступными для всех свои курсы повышения квалификации специалистов по сетевой безопасности (Network Security Expert training courses). Чтобы удовлетворить быстро меняющиеся потребности организаций, обеспечивающих безопасность удаленных рабочих мест, до конца 2020 года курсы будут бесплатными*..



МЛАДШИЙ СПЕЦИАЛИСТ ПО БЕЗОПАСНОСТИ

В ОТКРЫТОМ ДОСТУПЕ

Развитие фундаментального понимания постоянно развивающегося ландшафта угроз и общих концепций сетевой безопасности.



АНАЛИТИК

В ОТКРЫТОМ ДОСТУПЕ*

Формирование глубинного понимания в области управления и анализа угроз сетевой безопасности.



МЛАДШИЙ СПЕЦИАЛИСТ ПО БЕЗОПАСНОСТИ

В ОТКРЫТОМ ДОСТУПЕ

Формирование знания по решениям Fortinet в контексте ландшафта угроз и проблем безопасности, рассматриваемых на уровне NSE 1.



СПЕЦИАЛИСТ

В ОТКРЫТОМ ДОСТУПЕ*

Формирование понимания продуктов компании Fortinet, являющихся частью экосистемы Security Fabric и дополняющих FortiGate с целью обеспечения комплексной сетевой безопасности на более глубоком уровне.



МЛАДШИЙ СПЕЦИАЛИСТ ПО БЕЗОПАСНОСТИ

Тренинг по продажам только для сотрудников и партнеров Fortinet



АРХИТЕКТОР

В ОТКРЫТОМ ДОСТУПЕ*

Формирование навыков внедрения, диагностики и централизованного управления инфраструктурой безопасности, состоящей из разных устройств FortiGate.



ПРОФЕССИОНАЛ

В ОТКРЫТОМ ДОСТУПЕ*

Формирование навыков управления, мониторинга и эксплуатации устройств FortiGate в поддержку корпоративных стратегий сетевой безопасности.



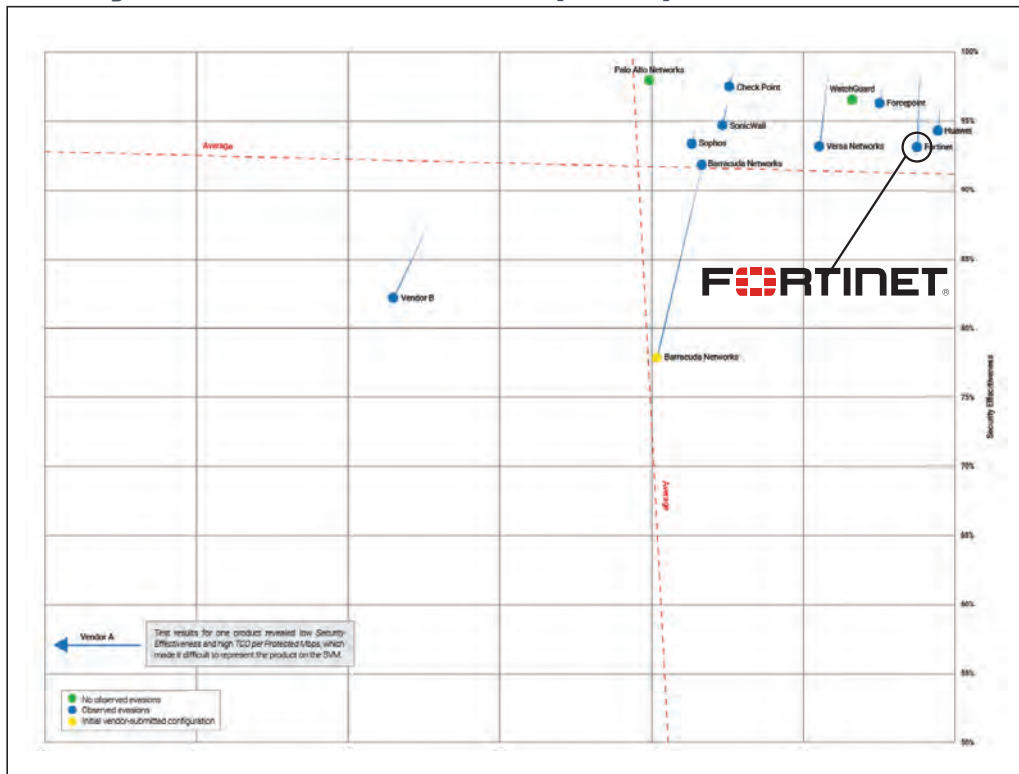
ЭКСПЕРТ

Демонстрация умения разрабатывать, конфигурировать, внедрять и диагностировать комплексное решение в области сетевой безопасности в реальных условиях эксплуатации.

* Только курсы для самостоятельного изучения NSE 4-7 будут бесплатными до 31 декабря 2020 года. Курсы под руководством эксперта, практические занятия и сертификация не включены. Подробнее об обеих программах можно узнать на сайте www.fortinet.com/support-and-training.html.

Рекомендовано в 9 из 9 тестов NSS LABS

Тестирование межсетевых экранов следующего поколения (2019) FortiGate 500E

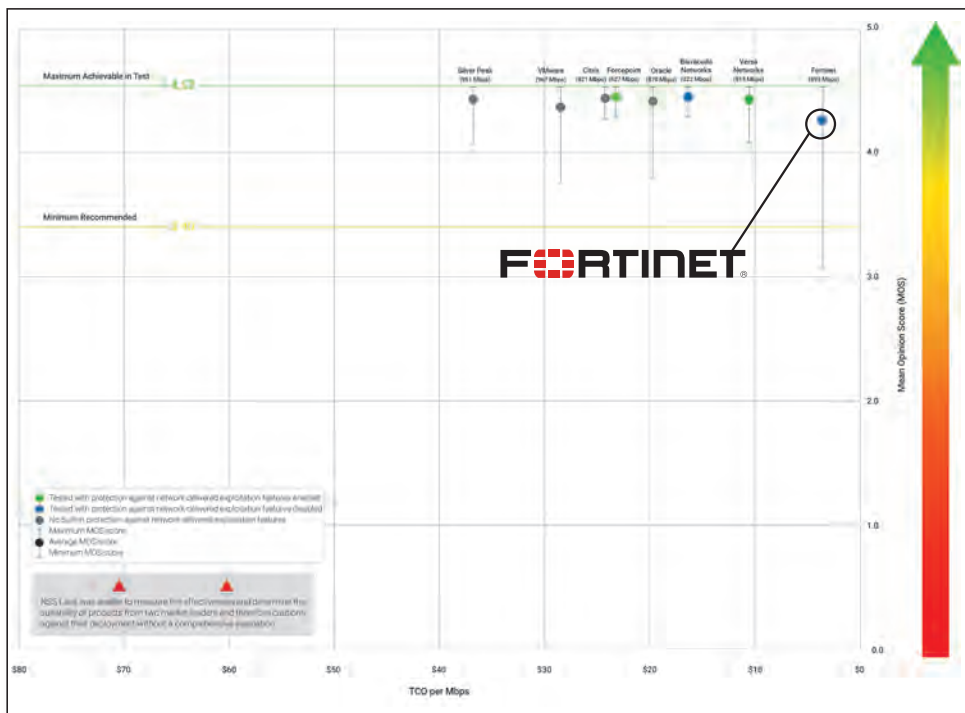


■ “Рекомендовано” 6-й год подряд

- 99% эффективность защиты
- 100% блокировка обходов
- Лучшая производительность SSL с наименьшим ухудшением качества
- Низкая общая стоимость использования (2 доллара за защищенный Мбит/с)



Тестирование решений класса SD-WAN (2019) FortiGate 61E



■ Единственный “рекомендуемый” поставщик с рейтингом безопасности

- Самая низкая стоимость использования, в 8 раз ниже, чем у конкурентных предложений
- Развертывание менее чем за 6 минут с помощью Zero-Touch Provisioning
- Надежное качество для видео и VOIP
- Лучший пользовательский опыт в развертывании соединения высокой доступности
- Встроенная безопасность NGFW



Не имеющая аналогов независимая сертификация

■ РЕКОМЕНДОВАННО/ СЕРТИФИЦИРОВАННО ■ ОСТОРОЖНО ○ НЕРАСКРЫТО

CERTIFICATION	FORTINET	Check Point	Cisco	Palo Alto	Juniper SRX	FireEye
1 NSS Next-Gen Firewall	■	■	○	■	○	X
2 NSS DC Security Gateway	■	X	■	■	■	X
3 NSS Next-Gen IPS	■	X	○	■	○	X
4 NSS DC IPS	■ ■	X	■	X	X	X
5 NSS Breach Detection	■	X	■	X	X	■
6 NSS Breach Prevention	■	■	■	■	■	X
7 NSS WAF	■	X	X	X	X	X
8 NSS Advanced Endpoint*	■	■	X	■	X	X
9 NSS SD-WAN	■	X	X	X	X	X
ICSA ATD—Sandbox	■	X	X	X	■	X
ICSA ATD—Email	■	X	X	X	X	X
ICSA Network Firewall	■	■	X	X	■	X
ICSA Network IPS	■	X	X	X	X	X
ICSA Anti-malware Network	■	X	X	X	X	X
ICSA WAF	■	X	X	X	X	X
Virus Bulletin 100	■	X	X	X	X	■
Virus Bulletin Spam	■	X	X	X	X	X
Virus Bulletin Web	■	X	X	X	X	X
Common Criteria	■	■	■	■	■	■
FIPS	■	■	■	■	■	■
UNH USGv6/IPv6	■	■	■	■	■	X

* Vendor products now receive a letter rating.

По состоянию на 27 апреля, 2020

Green here denotes a favorable "A" rating or better.

Единственное комплексное решение по защите от сложных угроз безопасности (ATP), рекомендованное NSS Labs.

Fortinet принимала участие в следующих открытых для отрасли испытаниях в реальных условиях эксплуатации, проводимых известной лабораторией NSS Labs. В рамках этих испытаний Fortinet показала себя единственным поставщиком решения ATP, рекомендованного лабораториями NSS для центров обработки данных, предприятий и рабочих мест.

- NGFW & NGIPS
- Шлюз безопасности центра обработки данных (DC Security Gateway & DCIPS)
- Брандмауэр веб-приложений
- Защита рабочих мест (Endpoint Protection)
- Обнаружение и предотвращение несанкционированного доступа



Признание клиентов



Рейтинг поставщиков 'Gartner Peer Insights Customers' Choice' («Gartner Peer Insights: Выбор клиентов») составляется на основе отзывов от профессионалов и конечных пользователей из различных отраслей и регионов мира. Рейтинг учитывает как количество отзывов о поставщике, так и общую оценку, которую поставщик получает от пользователей.

Fortinet гордится тем, что получила признание 'Gartner Peer Insights Customers' Choice' в нескольких важных направлениях:



Сетевые брандмауэры (2 раза)



Инфраструктура WAN Edge



Инфраструктура доступа к проводным и беспроводным локальным сетям (3 раза)

www.gartner.com/reviews

GARTNER PEER INSIGHTS CUSTOMERS' CHOICE – зарегистрированный товарный знак и знак обслуживания компании Gartner, Inc. и/или ее дочерних компаний; используется здесь с разрешения. Все права защищены. Gartner Peer Insights Customers' Choice присваивается на основе мнений отдельных пользователей, обзоров, оценок и данных, обработанных в соответствии с описанной методологией. Эти мнения не отражают позицию компании Gartner или ее аффилированных лиц.

ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ РЕШЕНИЙ КЛИЕНТАМИ



Акционерное общество «Ленинградская областная электросетевая компания»

Крупнейшая электросетевая компания на территории Ленинградской области и одно из крупнейших предприятий коммунальной энергетики в Российской Федерации.

Ключевые требования: Нужен был комплексный продукт, который включал бы в себя межсетевой экран в отказоустойчивой конфигурации (для централизованного выхода в интернет); решение для защиты электронной почты с антиспам-фильтром, встроенным антивирусом и «песочницей»; возможность защиты рабочих станций; централизованное управление системами безопасности, мониторинг всей поверхности атаки и возможность формирования отчетов.

Решение: Сегодня для обеспечения защиты от угроз, предотвращения вторжений, фильтрации веб-сайтов (как зашифрованного, так и незашифрованного трафика) и контроля приложений АО «ЛОЭСК» использует межсетевой экран следующего поколения FortiGate (кластер) – он обеспечивает полное отслеживание приложений, пользователей и сетей. Сейчас решения Fortinet защищают более чем 900 пользователей внутри компании. Используются следующие решения компании: FortiGate, FortiWeb, FortiMail, FortiSandbox, FortiClient, FortiAnalyzer, FortiManager.

«Внедрение Fortinet Security Fabric позволило нам пересмотреть укоренившиеся подходы к решению вопросов безопасности, ускорить и оптимизировать ряд ключевых процессов. Таким образом удалось значительно усилить защиту внешнего периметра информационной сети компании.»

— Глеб Иванов, начальник сектора системного администрирования, АО «ЛОЭСК»



Winston-Salem Forsyth County Schools

Сфера образования – 77-й по размеру кластер школ в США

Сфера применения: защита подключений и сети для поддержки интернет-обучения для более чем 53,000 учеников

Ключевые требования: защита от угроз на скоростях более 10+ GE, расшифрование SSL, внутренняя сегментация, аутентификация, безопасность электронной почты, отказоустойчивость на уровне аппаратного шасси

Решение: FortiGate 7040, FortiAuthenticator, FortiAnalyzer, FortiMail, сервисы FortiGuard

Клиент получил следующие преимущества:

- В одной платформе объединены межсетевое экранирование и маршрутизация для ядра и границы сети
- Удовлетворены повышенные требования к производительности для достижения скорости работы 10GB
- Простое и понятное управление, легкое развертывание, более высокая операционная эффективность.

«Для нас очень соблазнительным предложением, предопределившим выбор в пользу Fortinet, были возможности межсетевого экрана нового поколения компании Fortinet 7000-й серии, позволяющего обеспечить внутреннюю сегментацию сети, поддержку 100GE интерфейсов, скоростную инспекцию SSL и защиту от угроз по привлекательному соотношению цена/производительность. Развернув FortiGate 7040 мы консолидировали все наши сервисы безопасности в единой платформе, которую можно расширять для удовлетворения будущих требований в производительности и безопасности.»

— Кори Маклеод, ведущий инженер локальных и глобальных сетей



CENTERCREDIT

АО «Банк ЦентрКредит»

Один из первых коммерческих банков Казахстана.

Ключевые требования: С каждым годом требования стандарта PCI DSS (Payment Card Industry Data Security Standard) усложняются. Согласно им доступ к данным должен быть ограничен межсетевым экраном с наличием IPS. Для решения этой задачи было необходимо комплексное решение, включающее в себя ряд систем по обеспечению безопасности – IPS, IDS, антивирус, VPN IPsec, вскрытие SSL.

Решение: АО «Банк ЦентрКредит» использует следующие решения компании, обеспечивающие безопасность около 5000 пользователей, в том числе удаленных, а также несколько DATA-центров: NGFW FortiGate, FortiAnalyzer и FortiManager.

Клиент получил следующие преимущества:

- Решена проблема защиты сервисов, входящих в скоуп PCI DSS и SWIFT.
- Используются службы и SSL-инспекция безопасности такие как: IDS/IPS, антивирус, VPN IPsec, SSL-инспекцию.
- Формируются отчеты с помощью FortiManager и FortiAnalyzer.

«Решения Fortinet обеспечили большой ресурсный запас на будущее и соответствуют потребностям быстро растущей компании.»

— Касим Оспандияр Даниярулы, системный инженер, АО «Банк ЦентрКредит»

Лига Ставок

БК «Лига ставок»

Российская букмекерская компания, основанная в 2008 году. Деятельность компании направлена на развитие букмекерского бизнеса в России, поддержку национального спорта и создания нового вида развлечений.

Ключевые требования: управление из единого центра и гибкость. Количество специалистов, способных развернуть решение для обеспечения кибербезопасности, достаточно ограничено; в связи с этим важно было минимизировать сложность управления всей структурой. Компания постоянно развивается, сеть клубов и количество пользователей растёт, а значит, было необходимо решение, которое способно быстро масштабироваться, соответствуя актуальным и будущим вызовам.

Решение: FortiGate, FortiManager, FortiAnalyzer, FortiClient, FortiWeb, FortiMail, FortiSandbox.

Клиент получил следующие преимущества:

- Отказоустойчивость корпоративной и клиентской части бизнеса
- Объединённую в единую сеть инфраструктуру
- Защиту компании от таких угроз, как атаки на приложения, DDoS

«Создание инфраструктуры безопасности на базе Fortinet Security Fabric позволило нам сформировать прочный фундамент развития ИТ-среды компании практически с нуля. Теперь мы способны эффективно обеспечивать безопасность и непрерывность бизнеса.»

— Алексей Кислицын, директор департамента информационной безопасности БК «Лига Ставок».

Больше опубликованных примеров внедрения решений Fortinet можно найти по адресу www.fortinet.com/customers.html

