



Kaspersky NGFW

Глобальная экспертиза и передовые технологии для защиты от сетевых угроз и контроля активности приложений

95%

Показатель обнаружения и предотвращения сетевых угроз с помощью IDPS (Detection Rate)*

до 200 Гбит/с

Производительность Kaspersky NGFW в режиме L4 FW + Application control**

5 000+

Распознаваемых приложений с помощью собственного DPI

7 000+

Поддерживаемых сигнатур IDPS

20 000+

Поддерживаемых правил Firewall

Межсетевой экран нового поколения на основе глобальной экспертизы и передовых технологий. Продукт защищает корпоративную сеть компаний от широкого спектра киберугроз, контролирует активность приложений и сервисов, позволяет эффективно управлять трафиком и оптимизирует производительность инфраструктуры.



Архитектура

Под капотом Kaspersky NGFW собственные технологии безопасности и архитектура, которая поддерживает многопоточную обработку трафика с минимизацией количества копирований



Эффективное использование ресурсов



Оптимизация производительности продукта



Высокие показатели производительности на x86 процессорах



Возможность кластеризации на базе собственного протокола Kaspersky High-availability Cluster Protocol

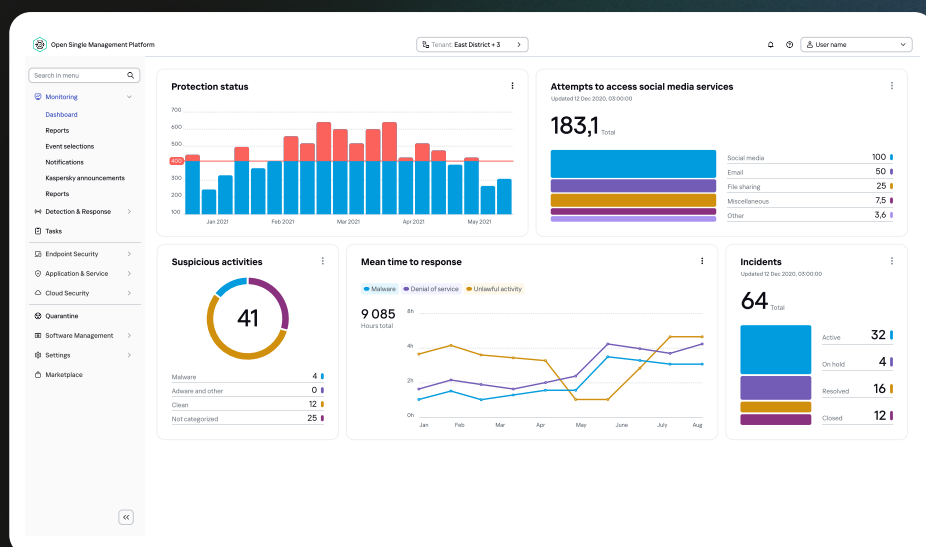


Open
Single Management
Platform

Open Single Management Platform — консоль мониторинга и управления всеми развёрнутыми NGFW и другими продуктами Kaspersky упрощает рутинные операции и администрирование

- Возможность реагирования на киберугрозы с помощью Kaspersky Symphony XDR
- Полная картина кибербезопасности компании в рамках единого окна

Экосистемный подход и централизованное управление



* Тестирование проводилось с помощью IXIA BreakingPoint, Strike Level 3 и 5, 2521 попытка атак

** Тестирование проводилось с 20 000 правил Firewall и включенным логированием

Ключевые технологии

Контроль сетевых соединений

Высокотехнологичный Stateful Firewall

- Отслеживает состояния активных соединений и возможные угрозы в них
- Принимает решения на основе контекста трафика
- Возможность блокировки установленных сессий
- Контроль трафика конкретных стран и регионов с помощью GeoIP-политик

User-aware политики

- Позволяют контролировать доступы, как разрешать, так и запрещать, для отдельных пользователей или целых групп
- Обеспечивают более полный контроль сети и упрощают работу специалистов ИТ / ИБ с инфраструктурой

Производительный DPI

- Определяет в трафике более 5 000 приложений и сервисов
- Собственный центр экспертизы по распознаванию приложений

Защита от сетевых угроз

Гибкий IDPS

- Выявляет и предотвращает атаки в режиме реального времени
- Поддержка более 7 000 сигнатур
- Показатель обнаружения и предотвращения сетевых угроз (Detection Rate) превышает 95%*

Продвинутая SSL/TLS-инспекция

- Расшифровывает трафик любых протоколов
- Поддержка исключений из расшифровки на основе веб-категорий
- Подключает к анализу все движки безопасности

Высокоскоростной потоковый антивирус

- Выявляет вредоносные активности на самых ранних этапах
- Высокое соотношение качества детектирования и производительности

↑
↓
Возможность выбора наиболее подходящего варианта

AI-powered антивирус

- Разработан на базе технологий Kaspersky Endpoint Security, специально оптимизированных для Kaspersky NGFW
- Эвристический анализ файлов на базе механизмов Machine Learning (ML) и Artificial Intelligence (AI)
- Проверка архивов с любыми расширениями и возможность отправки файлов на дополнительную проверку в сторонние системы через ICAP-клиент

Контроль веб-трафика

Высокоточный веб-категоризатор

- Точное определение категории URL
- Собственные категории с гибкими сценариями реагирования
- Возможность исключения конкретных URL-адресов

Проверка репутации URL-адресов

- Ограничение доступа к опасным и потенциально опасным веб-ресурсам и IP-адресам
- Блокировка рекламных ресурсов

DNS Security

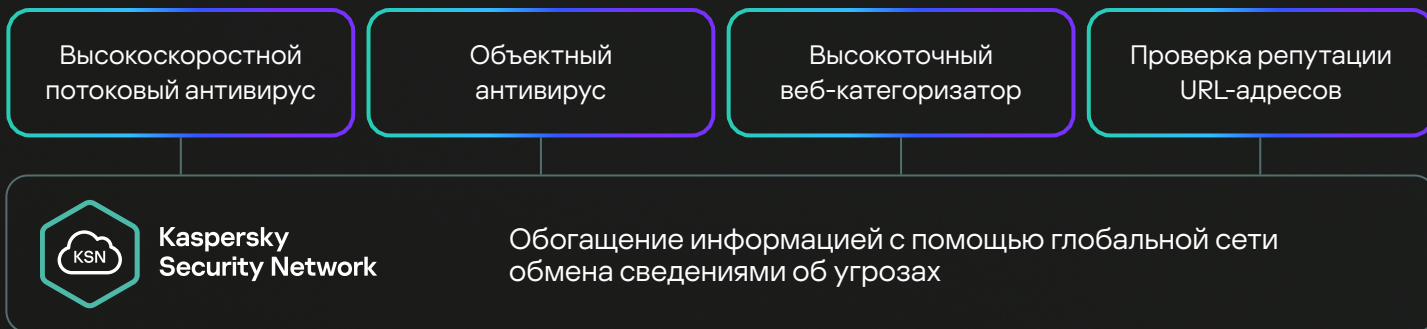
- Проверяет принадлежность доменных имен к потенциально опасным
- Позволяет оптимизировать производительность за счет фильтрации на уровне доменов

* Тестирование проводилось с помощью IXIA BreakingPoint, Strike Level 3 и 5, 2521 попытка атак

Актуальные данные об угрозах и обогащение аналитикой

Threat Intelligence

- Встроенное автоматическое обогащение актуальной информацией об угрозах
- Уникальные тактические данные на основе опыта экспертов «Лаборатории Касперского»



652 млн

отражено атак с различных ресурсов*

109 млн

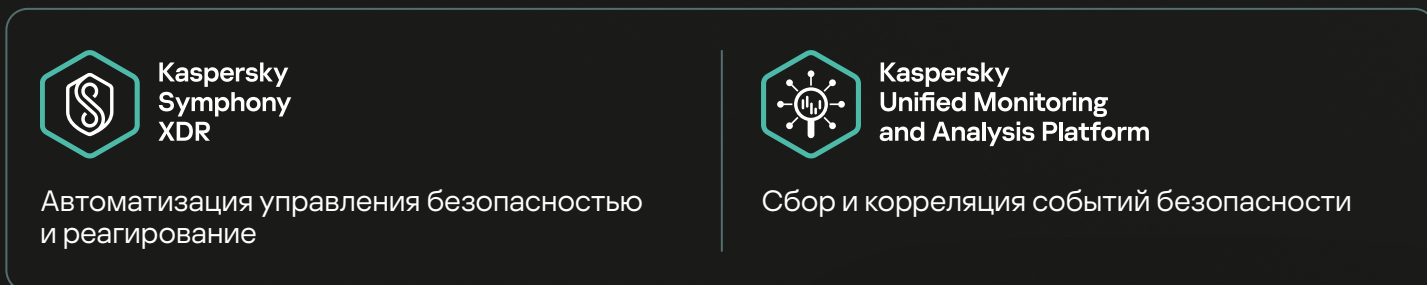
обнаружено уникальных вредоносных ссылок*

23 млн

заблокировано нежелательных объектов*

Интеграционные сценарии

Kaspersky NGFW поддерживает интеграцию с другими решениями «Лаборатории Касперского» в рамках экосистемного подхода.



Предотвращение сложных атак и угроз нулевого дня с помощью проверки подозрительных файлов в специальной среде — Sandbox

- Интеграция по API для достижения максимальной скорости получения вердикта
- Кеширование вердиктов для оптимизации скорости обработки запросов на повторную проверку файлов

* Развитие информационных угроз в третьем квартале 2024 года. «Лаборатория Касперского»

Policy test

KATA analysis

In this section, you can define the global settings of your NGFW connection to KATA. More detailed configuration of the KATA functionality is done individually for each Anti-Virus profile.

General settings

Enable ☒ On

Client certificate*

Private key for certificate*

Password for decrypting the key* Private key is not uploaded

Server settings

Define the connection settings to the primary KATA server. You can also specify up to three backup servers. Switching to another server occurs if the connection to the previous server is not established.

Primary server

Address*

Port*

Server certificate*

Add backup server

Save and close Save Cancel

Возможности продукта



Функции управления и мониторинга

Централизованное управление Kaspersky NGFW и мониторинг состояния решения через централизованную консоль управления Open Single Management Platform (OSMP)	●
Ролевая модель доступа (RBAC) для разграничения возможных действий пользователя при работе с политиками и настройками в OSMP	●
Отправка системных событий и событий безопасности, сформированных Kaspersky NGFW, в консоль OSMP и сторонние SIEM-системы	●
Аналитические панели мониторинга и отчеты по результатам работы решения в OSMP	●
Импорт и экспорт политик безопасности решения в OSMP	●
Централизованное управление сетевой конфигурацией при помощи шаблонов	●
Создание и настройка зон в OSMP	●
Поддержка обновления ПО NGFW	●
Возможность настройки периода и источника обновления локальных баз NGFW	●
Zabbix-шаблон для мониторинга NGFW	●



Сетевые функции

Поддержка настройки статической маршрутизации IPv4 через CLI Kaspersky NGFW	●
Поддержка отказоустойчивого кластера active-passive с синхронизацией сессий на базе собственного протокола KHCP (Kaspersky High-availability Cluster Protocol)	●
Поддержка синхронизации маршрутной информации между нодами кластера (RIB)	●
Поддержка агрегированных интерфейсов	●
Поддержка L2-интерфейсов	●
Поддержка VLAN и саб-интерфейсов	●
Поддержка VRF	●
Поддержка DNS-клиента	●
Поддержка DHCP-клиента	●
Поддержка NTP-клиента	●
Поддержка SNMP	●
Поддержка виртуального исполнения Kaspersky NGFW на базе гипервизоров KVM и VMware ESXi	●
BFD	●
BGP	●
OSPF	●
Мониторинг интерфейсов в кластере	●
DHCP Relay	●
Возможность настройки таймаутов сессий	●

Функции безопасности

Возможность создания групповых политик безопасности	●
Автоматическое обновление локальных баз движков безопасности Kaspersky NGFW: антивируса, веб-контроля, защиты DNS-трафика и IDPS	●
Межсетевой экран с отслеживанием состояния сессий (Stateful Firewall)	●
Поддержка GeoIP-политик	●
Система обнаружения и предотвращения вторжений (IDPS) с поддержкой более 7 000 сигнатур	●
Глубокая проверка пакетов (DPI) с поддержкой контроля трафика более 5 000 приложений	●
Инспектирование SSL/TLS-трафика с поддержкой TLS 1.1, 1.2 и 1.3	●
Возможность создания исключений по веб-категориям и конкретным доменам в движке SSL/TLS-инспекции	●
Потоковый антивирус	●
Проверка репутации URL-адресов (malware, phishing, c&c, adware и т.п.)	●
Категоризация и контроль веб-трафика	●
Возможность создания пользовательских веб-категорий	●
Механизм добавления исключений в правила проверки веб-трафика	●
Менеджер для просмотра установленных через Kaspersky NGFW сессий с возможностью их сброса	●
Поддержка проверки DNS-трафика (DNS Security) по репутационным базам	●
Получение актуальных тактических данных об угрозах (Threat Intelligence) для проверки репутации URL-адресов и обогащения баз антивируса и веб-категоризатора	●
Нативная интеграция с Kaspersky Symphony XDR посредством плейбуков	●
Поддержка политик с использованием зон	●
Поддержка NAT	●
Поддержка работы правил фильтрации по расписанию	●
Интеграция по API с Kaspersky Anti Targeted Attack для проверки файлов с помощью Sandbox	●
AI-powered антивирус	●
Антивирусная проверка архивов с любыми расширениями	●
Поддержка ICAP-клиента для отправки файлов на проверку в сторонние системы	●
User-aware политики	●
Возможность использования FQDN в качестве destination в правилах межсетевого экрана	●
Поддержка действия Reset-both в правилах межсетевого экрана	●
Антивирусная проверка по почтовым протоколам	●
Использование зон в качестве квалификаторов в правилах SSL/TLS-инспекции	●

Аппаратные и виртуальные платформы

Линейка KX (Kaspersky Extension) — семейство сетевых аппаратных платформ, разработанных специально для решения Kaspersky NGFW. Эти устройства обеспечивают высокую производительность, надежную защиту от киберугроз и масштабируемость для различных сценариев использования.

Внешний вид модели

KX-100



Внешний вид моделей

KX-400
KX-1000
KX-3500



	KX-100-KA1	KX-100-KB1	KX-400	KX-1000	KX-3500
Производительность в режиме L4 FW + Application Control*	До 10 Гбит/с	До 10 Гбит/с	До 40 Гбит/с	До 100 Гбит/с	До 200 Гбит/с
Производительность в режиме NGFW (L4 FW + Application Control + IDPS)*	До 3 Гбит/с	До 3 Гбит/с	До 10 Гбит/с	До 20 Гбит/с	До 50 Гбит/с
Интерфейсы	• 6 × 10/100/1000 Ethernet RJ45 • 2 × SFP+	• 14 × 10/100/1000 Ethernet RJ45 • 2 × SFP+	• 4 × 10/100/1000 Ethernet RJ45 • 8 × 25G SFP28 • 4 × 100G QSFP28	• 4 × 10/100/1000 Ethernet RJ45 • 8 × 25G SFP28 • 4 × 100G QSFP28	• 4 × 10/100/1000 Ethernet RJ45 • 8 × 25G SFP28 • 4 × 100G QSFP28

В рамках линейки KX-Series доступны также виртуальные исполнения — vKX. Они предназначены для развертывания Kaspersky NGFW на собственных ресурсах заказчика без необходимости использования аппаратных платформ. В данный момент доступно виртуальное исполнение Kaspersky NGFW vKX-8.

vKX-8

Производительность в режиме L4 FW + Application Control*

До 5 Гбит/с

Производительность в режиме NGFW (L4 FW + Application Control + IDPS)*

До 2.5 Гбит/с

Гипервизоры

KVM и VMware ESXi

Для аппаратных платформ также доступна Расширенная гарантия Hardware MSA

Подробнее

Более подробно изучить линейку KX-Series можно в нашем каталоге оборудования

Подробнее

Узнать подробнее о методике тестирования производительности

Подробнее

* Тестирование проводилось с 20 000 правил Firewall и включенным логированием

Лицензирование

Решение Kaspersky NGFW представлено в двух вариантах: Standard и Advanced.



Kaspersky
NGFW

Standard

Предоставляет все необходимые инструменты управления и мониторинга, контроля сетевых соединений и защиты от сетевых угроз.



Kaspersky
NGFW

Advanced

Предлагает расширенные возможности для контроля веб-ресурсов и построения комплексной защиты корпоративной сети.

Каждый вариант решения включает в себя техническую поддержку в соответствии с выбранным уровнем обслуживания: Premium или Premium Plus.

Лицензия

1

Выбранная аппаратная платформа

2

Необходимый вариант решения:

Standard или
Advanced

3

Подходящий уровень технической поддержки:

Premium или
Premium Plus



Kaspersky NGFW Log Analyzer — модуль аналитики на базе OSMP с подходящим количеством событий в секунду (EPS, Events Per Second)

Бесплатно до конца
2025 года

Пример

1

KX-3500

2

В варианте
Advanced

3

С включенной технической поддержкой уровня
Premium

Подробнее
о лицензировании

Подробнее

Почему Kaspersky NGFW



Полностью российский продукт, соответствующий стратегии движения к импортонезависимости



Полный контроль и эффективное управление сетевым трафиком и активностью приложений



Экосистемный подход к защите корпоративной инфраструктуры и централизованное управление



Собственная архитектура и механизмы безопасности, основанные на лидерских технологиях



Прозрачное лицензирование без дополнительных модулей и расширений



Глобальная экспертиза в борьбе с киберугрозами, разработке продуктов и поддержке клиентов

[Подробнее](#)

Уникальный опыт экспертов в основе решения



Глобальный центр исследований и анализа угроз

Исследование сложных угроз и расследование финансово мотивированных киберпреступлений



Центр исследования угроз

Исследование угроз, создание детектирующей логики, контентная фильтрация, безопасная разработка



Центр исследования технологий искусственного интеллекта

Обнаружение угроз с помощью ИИ / усиление ИБ решений алгоритмами ИИ



Центр исследования безопасности промышленных систем*

Анализ угроз в промышленных инфраструктурах

● Исследование угроз ● Расследование инцидентов

* В рамках разработки решения для промышленных инфраструктур, с 2026 года



Kaspersky NGFW

Узнать больше

www.kaspersky.ru

© 2025, АО «Лаборатория Касперского».
Зарегистрированные товарные знаки и знаки
обслуживания являются собственностью
их правообладателей.

#kaspersky
#активируйбудущее