

Kaspersky NGFW

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

kaspersky





Содержание

- 01 Сетевой ландшафт
- 02 Kaspersky NGFW
- 03 Ключевые технологии и возможности
- 04 Оборудование и лицензирование
- 05 Интеграционные сценарии
- 06 Преимущества Kaspersky NGFW
- 07 План развития продукта

Сетевой ландшафт

и технология NGFW

01



Сетевой ландшафт

4

343 млн

отражено атак
с различных ресурсов

50 млн

обнаружено уникальных
вредоносных ссылок

15 млн

заблокировано
нежелательных объектов



Рост количества
и сложности сетевых угроз,
уязвимости в приложениях
и сервисах



Бесконтрольное использование
сотрудниками приложений и
веб-ресурсов



Низкая прозрачность сетевой
архитектуры и потребность
в оптимизации процессов
внутри нее



Большое количество средств
защиты разных классов
и вендоров, интегрированных в
сложную сетевую инфраструктуру



Необходимость выполнять
требования регуляторов
и соответствовать стратегии
импортонезависимости



Потребность в замене решений
ушедших зарубежных вендоров
в условиях отсутствия
качественных российских аналогов

Kaspersky NGFW

02



Бескомпромиссная защита от сетевых угроз и контроль активности приложений

6



**Kaspersky
NGFW**

Межсетевой экран нового поколения на основе глобальной экспертизы и передовых технологий. Под капотом решения собственная архитектура и движки безопасности.

95%

Показатель обнаружения и предотвращения сетевых угроз с помощью IDPS*

6 000+

Распознаваемых приложений с помощью DPI

До 100 000

Поддерживаемых правил движком Stateful Firewall

до 200 Гбит/с

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

9 000+

Поддерживаемых сигнатур гибким IDPS

* Данные IXIA BreakingPoint, Strike Level 3 и 5, 2521 попытка атак

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

Бескомпромиссная защита от сетевых угроз и контроль активности приложений

7



Технологии

Контроль сетевых соединений

Высокотехнологичный
Stateful Firewall

User-aware политики

Производительный DPI
на 6 000+ приложений

Защита от сетевых угроз

Гибкий IDPS с большим количеством сигнатур

Продвинутая SSL/TLS-инспекция

Высокоскоростной потоковый антивирус

AI-powered антивирус

Контроль веб-трафика и обогащение аналитикой

DNS Security

Высокоточный
веб-категоризатор

Проверка репутации
URL-адресов

Threat
Intelligence



Архитектура

Поддержка многопоточной обработки трафика с минимизацией количества копирований

Эффективное
использование
ресурсов

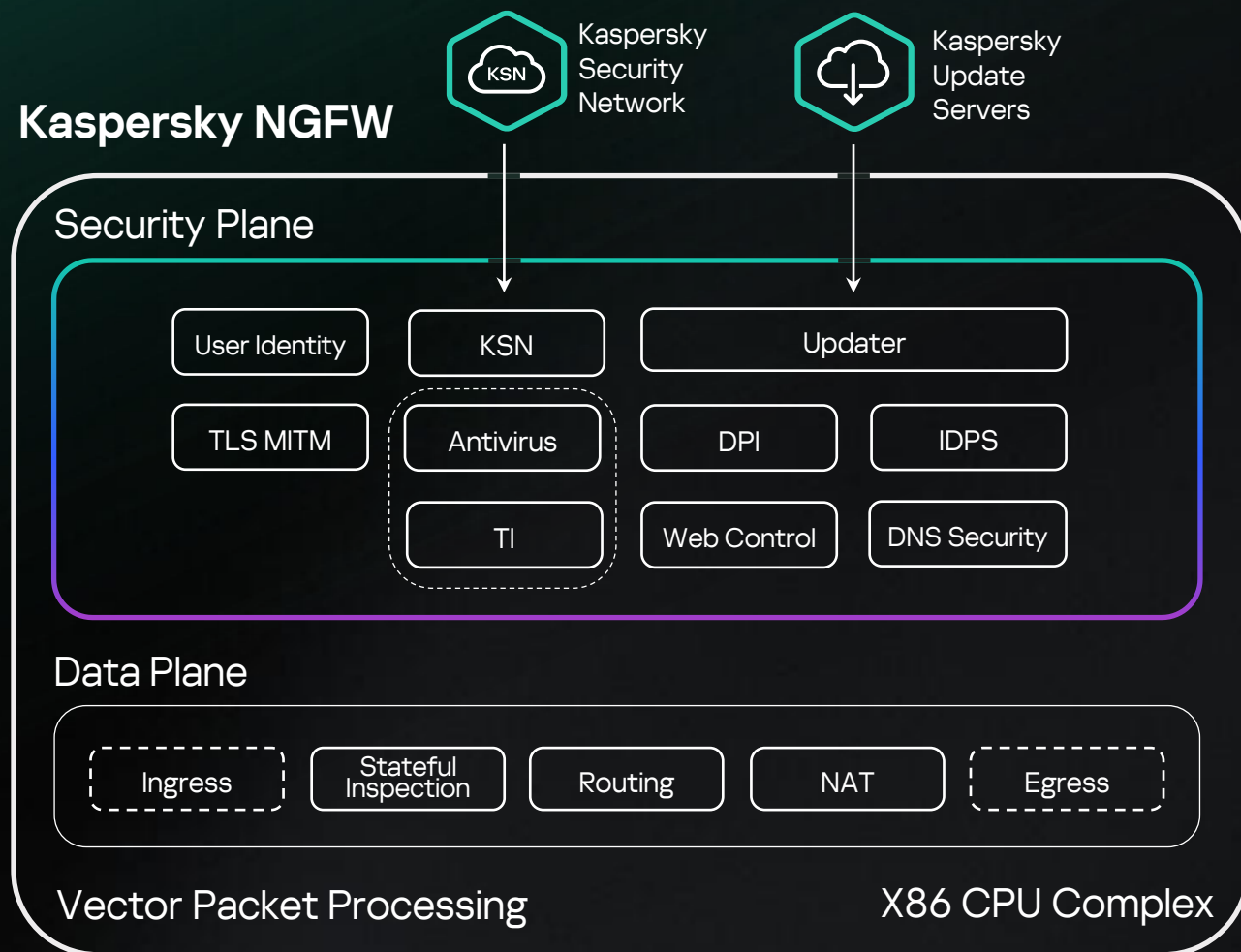
Оптимизация
производительности
продукта

Высокие показатели
производительности
на x86 процессорах

Возможность
кластеризации на
базе собственного
протокола

Архитектура

8



Security Plane

- Функции защиты от угроз и фильтрация трафика
- KSN — обновление локальных антивирусных и репутационных баз; облачные запросы хешей, IP и URL с неизвестной репутацией
- Updater — обновление сигнатур, URL-категорий, репутации IP и URL

Data Plane

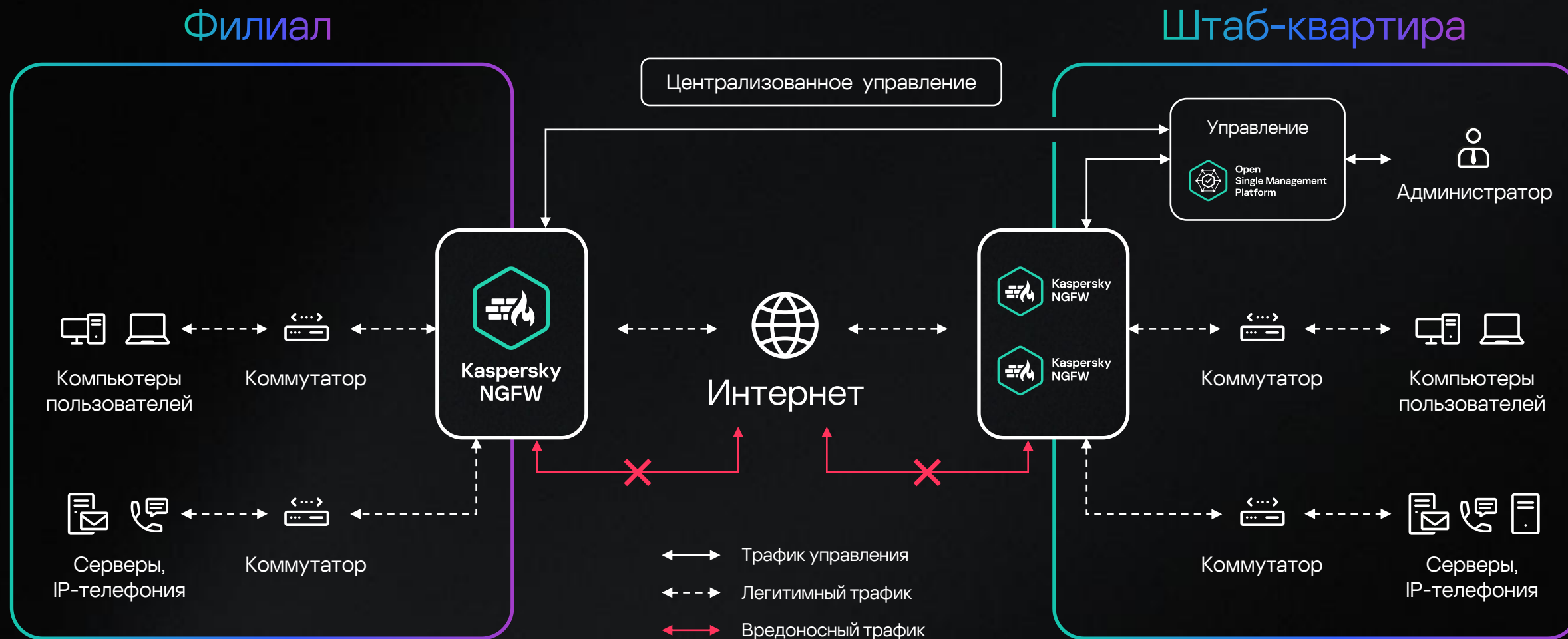
- Ingress — входящий сетевой интерфейс
- Stateful Inspection — анализ и отслеживание состояния соединений TCP/IP
- Routing, NAT — маршрутизация и трансляция сетевых адресов
- Egress — исходящий сетевой интерфейс

VPP

Высокопроизводительная обработка сетевых пакетов

Схема работы с централизованным управлением

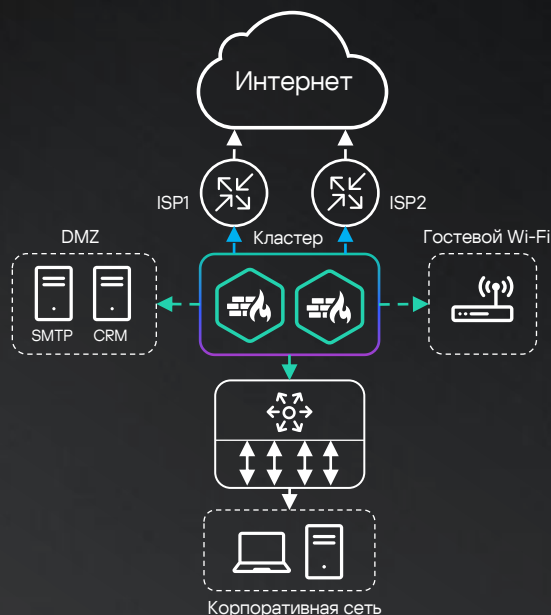
9



Основные сценарии использования

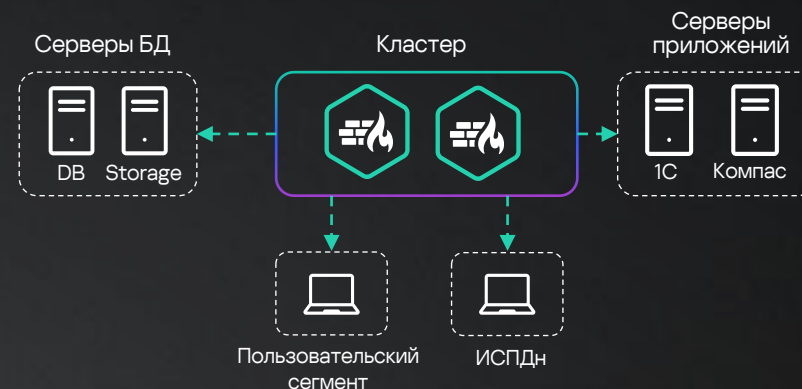
Защита периметра корпоративной сети — проверка входящего и исходящего трафика

- Контроль доступа к интернет и облачным приложениям
- Анализ и защита сетевого трафика на наличие угроз
- Организация корпоративного VPN для удаленных филиалов
- Публикация корпоративных сервисов
- Мониторинг и аналитика



Сегментация корпоративной сети — разделение ресурсов внутри организации

- Сегментация корпоративной сети
- Гранулярный контроль пользователей и приложений
- Ограничение распространения угроз
- Мониторинг и аналитика сетевого взаимодействия, выявление аномалий



Ключевые технологии

И ВОЗМОЖНОСТИ

03



Ключевые технологии



Высокотехнологичный Stateful Firewall

- Отслеживает состояния активных соединений и возможные угрозы в них
- Принимает решения на основе контекста трафика
- Возможность блокировки установленных сессий



Продвинутая SSL/TLS-инспекция

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

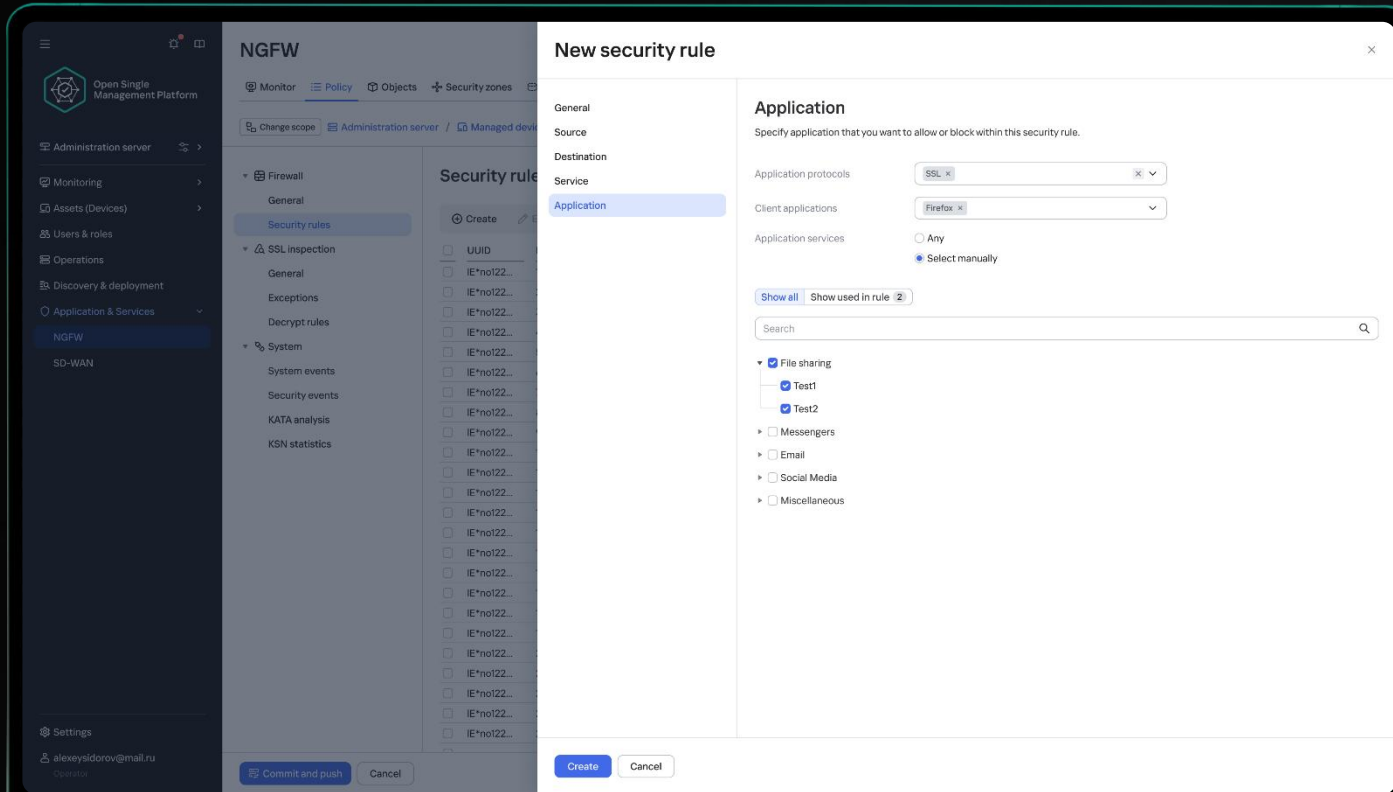


Threat Intelligence

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

Производительный DPI

13



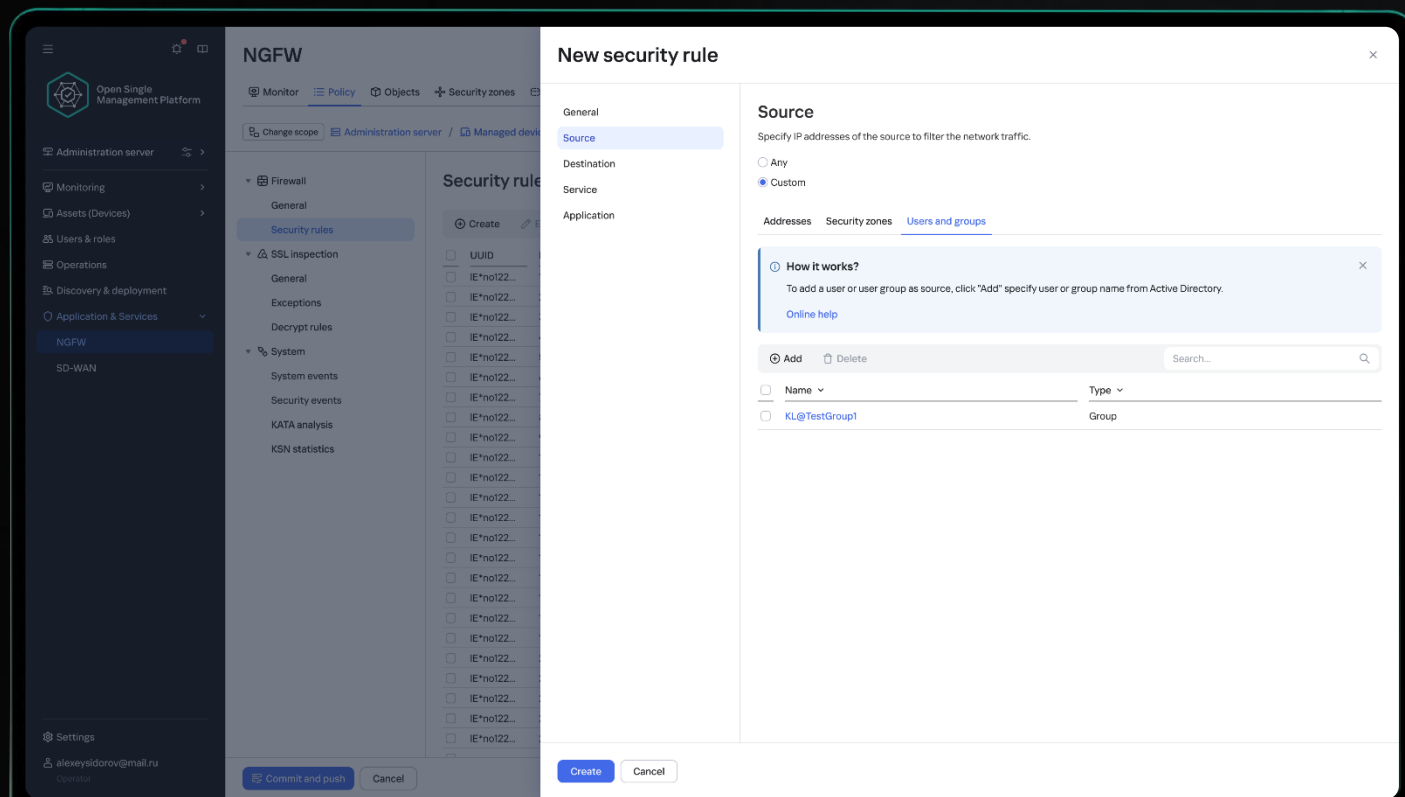
Определяет в трафике более 6 000 приложений и сервисов

Собственный центр экспертизы по распознаванию приложений

Распознавание приложений осуществляется с помощью сигнатурного метода и через Server Name Indication (SNI)

User-aware политики

14

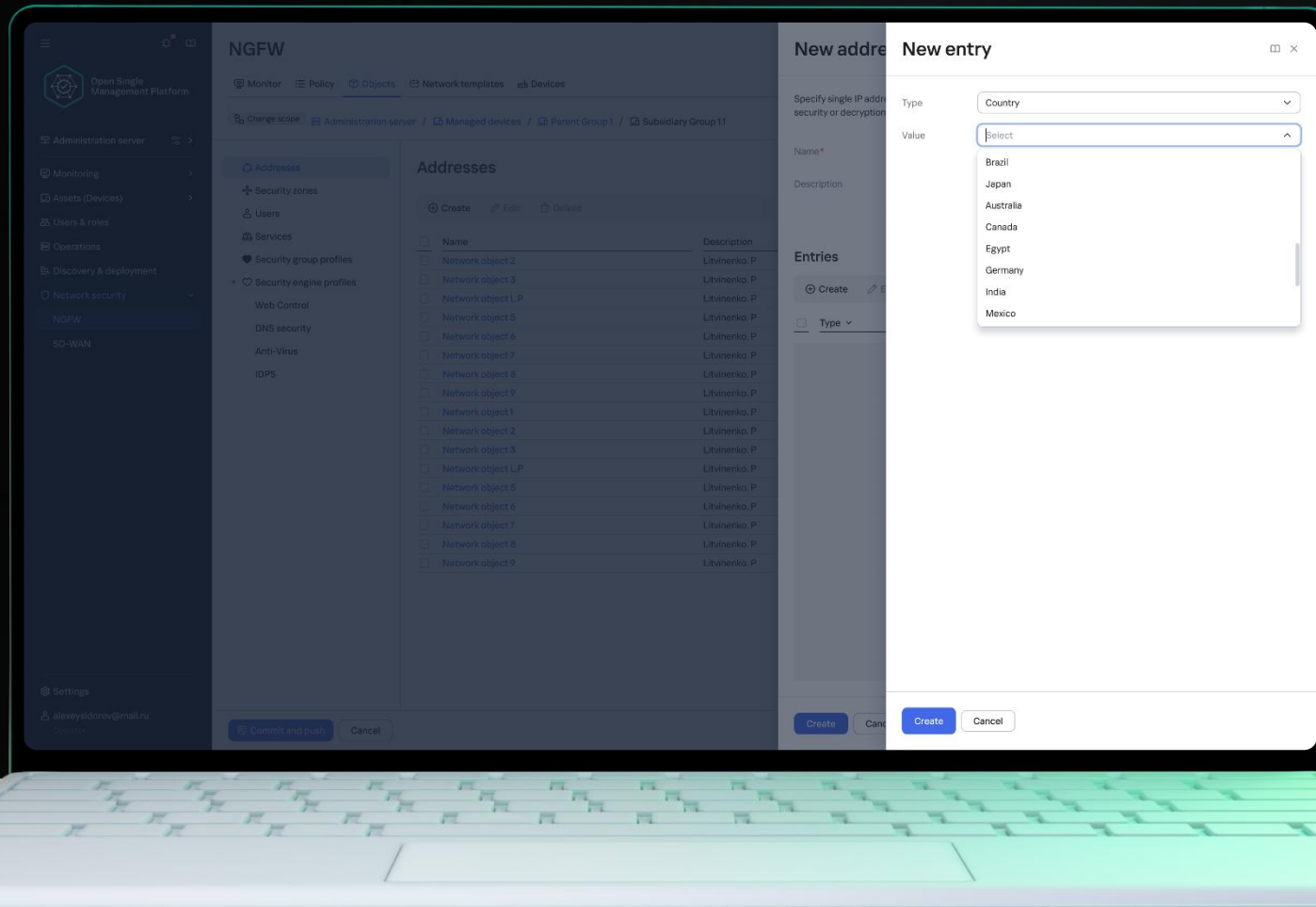


Позволяют контролировать доступы для отдельных пользователей или целых групп

Обеспечивают более полный контроль сети и упрощают работу специалистов ИТ/ИБ

Политики GeoIP

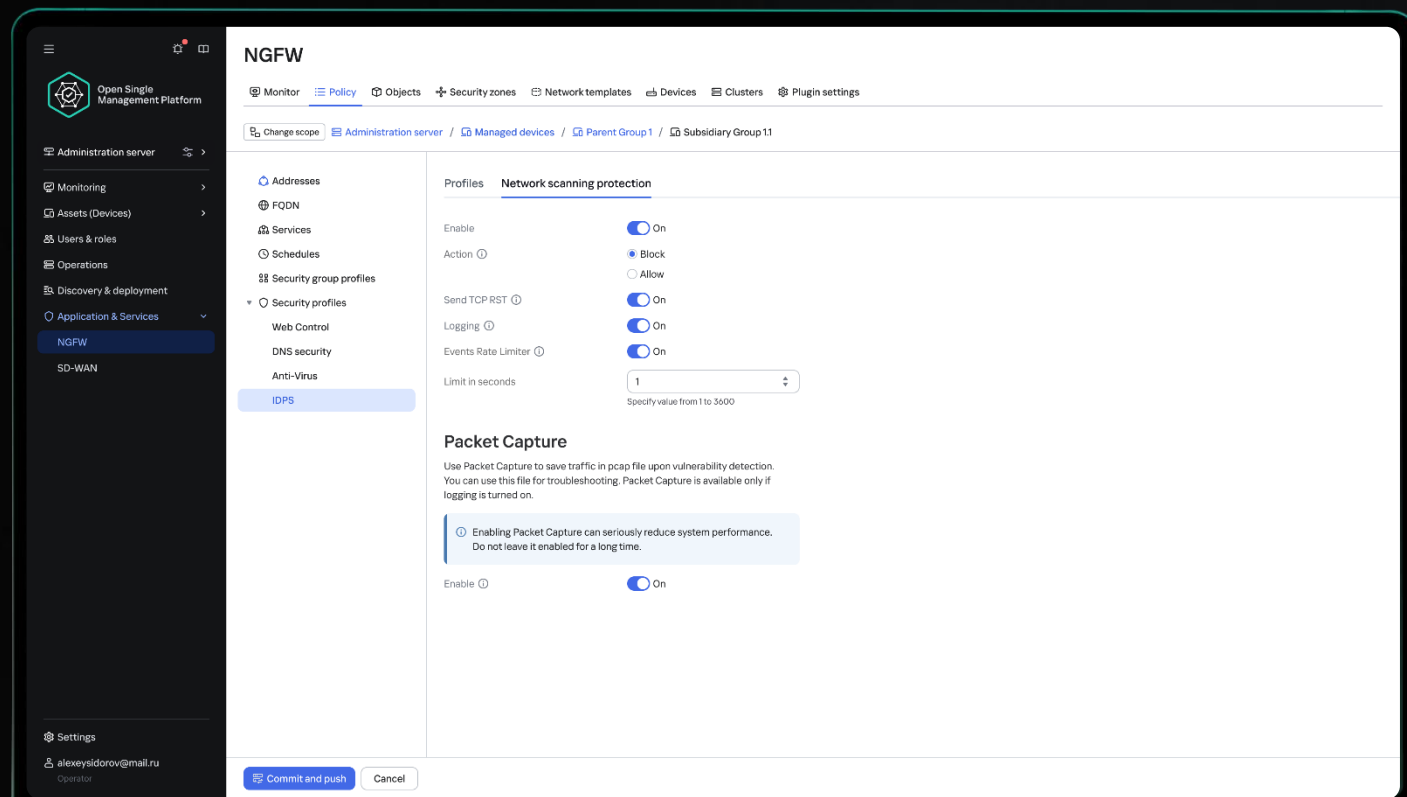
15



Позволяют контролировать трафик для конкретных регионов

Гибкий IDPS

16



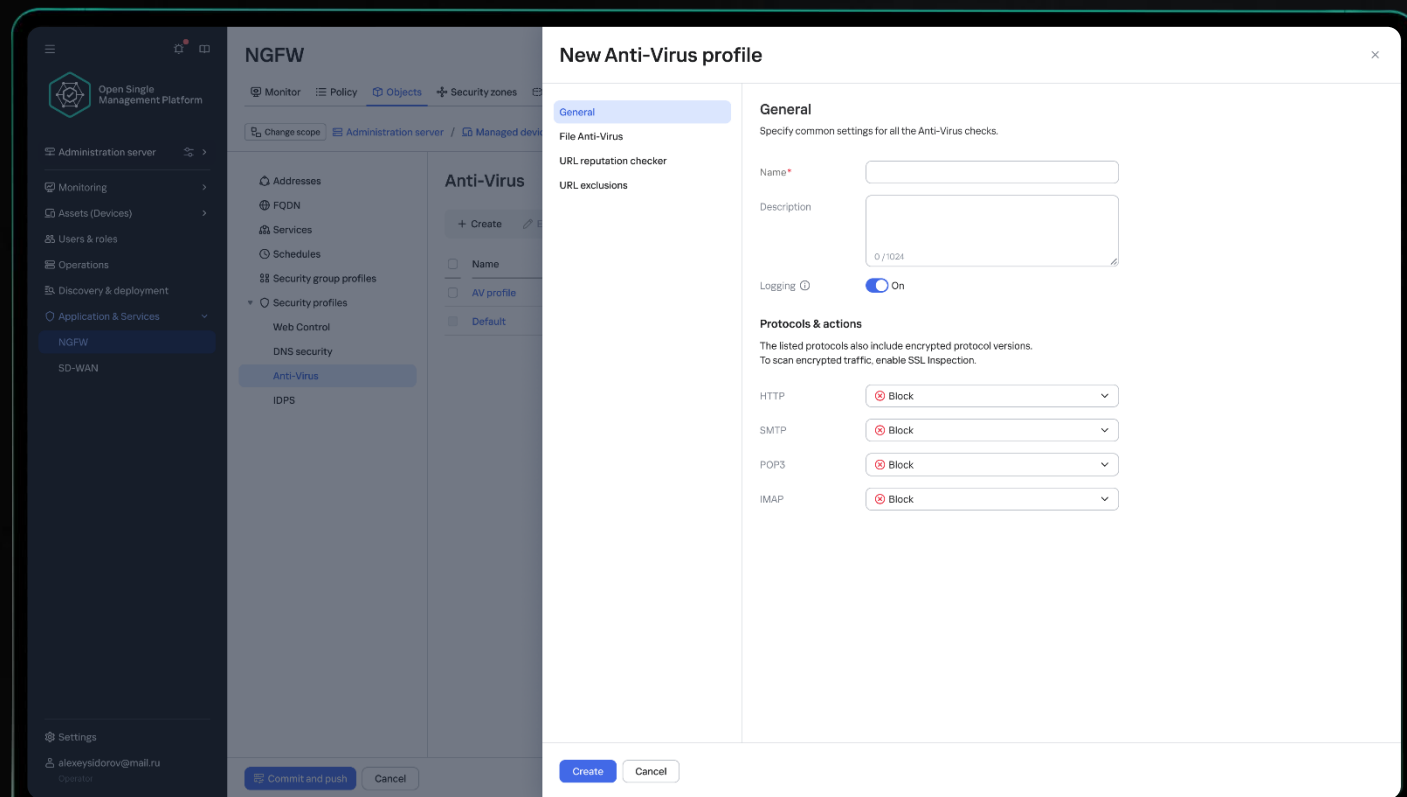
Выявляет и предотвращает атаки
в режиме реального времени

Поддержка более 9 000 сигнатур

Показатель обнаружения
и предотвращения сетевых угроз
(Detection Rate) превышает 95%*

* Данные IXIA BreakingPoint, Strike Level 3 и 5, 2521 попытка атак

Высокоскоростной потоковый антивирус¹⁷



Выявляет вредоносные активности
на самых ранних этапах

Высокое соотношение
качества детектирования
и производительности

Интеграция с Kaspersky Security
Network

Разработан самым надежным
поставщиком защитных решений

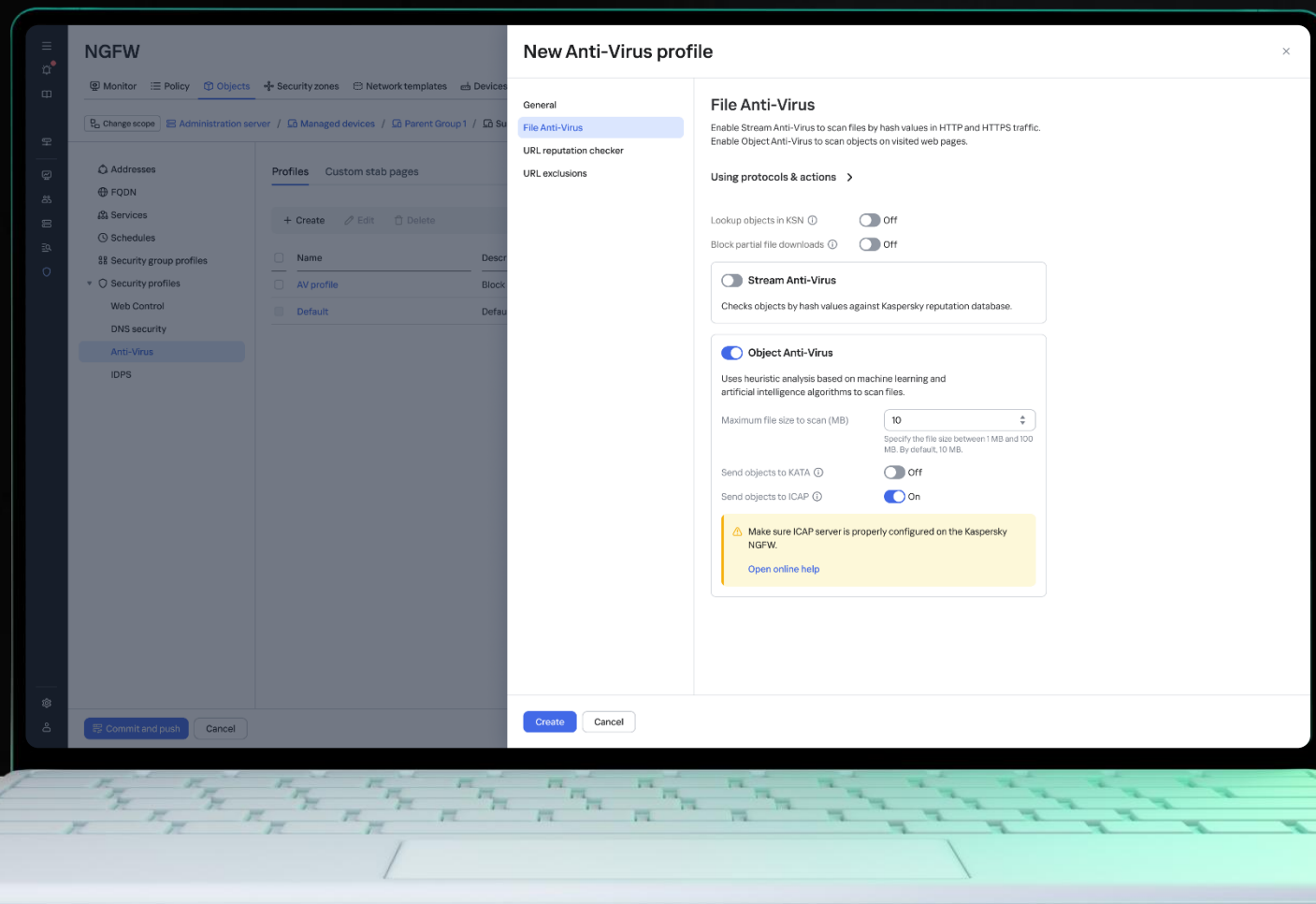


Показатель ТОП-3

[Подробнее](#)

AI-powered антивирус

18



Проводит эвристический анализ файлов с применением механизмов Machine Learning (ML) и Artificial Intelligence (AI)

Разработан на базе оптимизированных технологий Kaspersky Endpoint Security

Глобальные данные об угрозах из облака Kaspersky Security Network

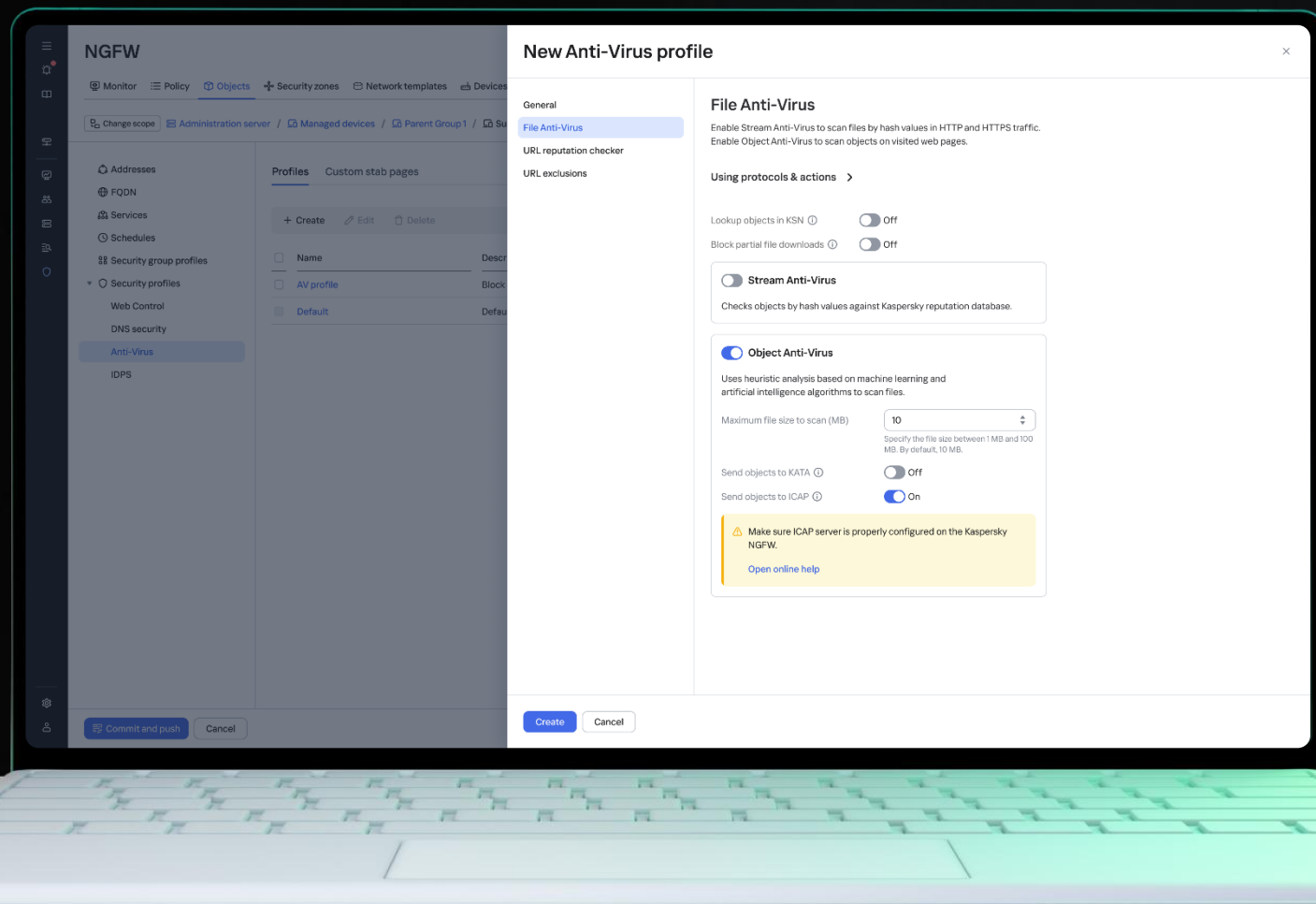


Показатель ТОП-3

[Подробнее](#)

AI-powered антивирус

19

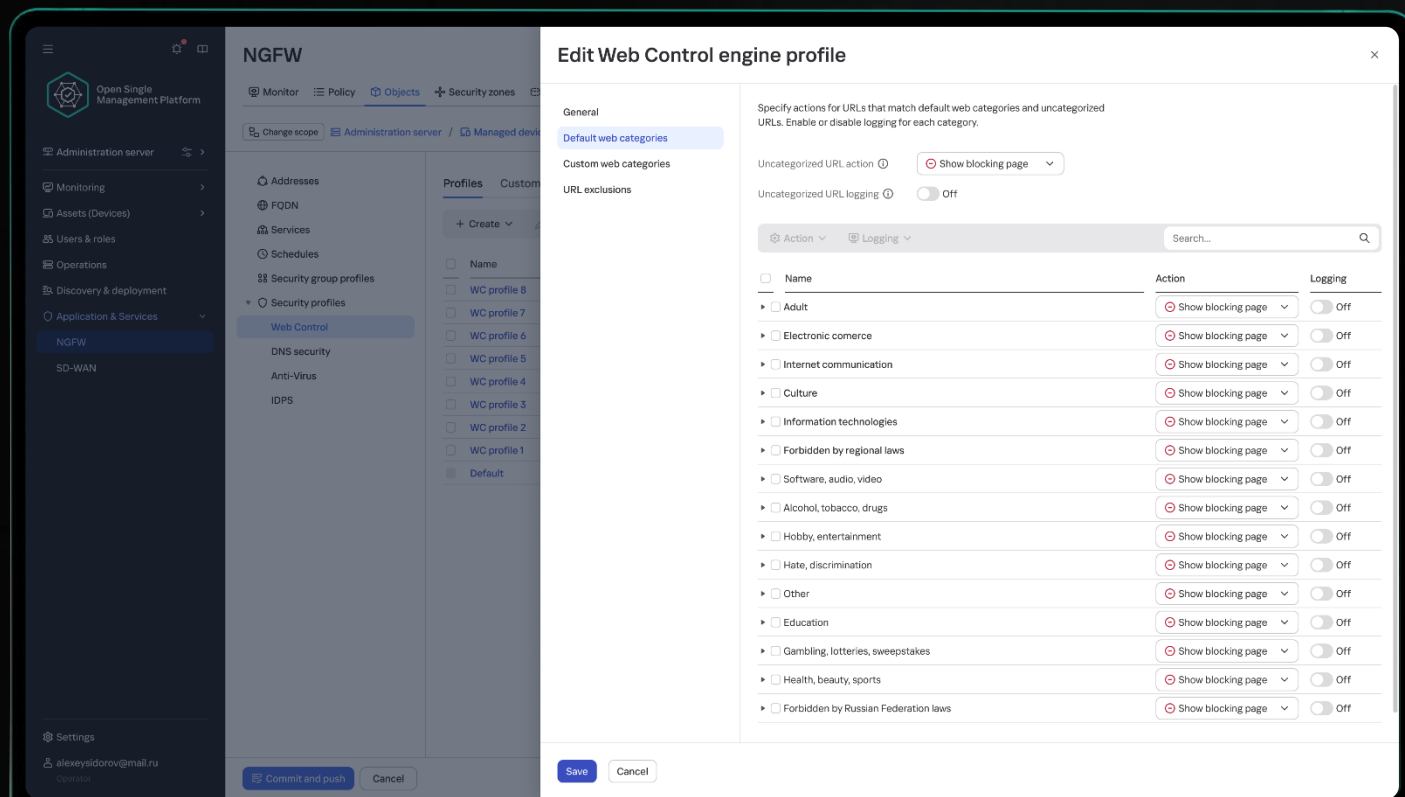


Антивирусная проверка архивов
с любыми расширениями и
уровнями вложенности

ICAP-клиент для отправки файлов
на проверку в сторонние
«песочницы» и DLP-системы

Высокоточный веб-категоризатор

20



Точное определение категории URL

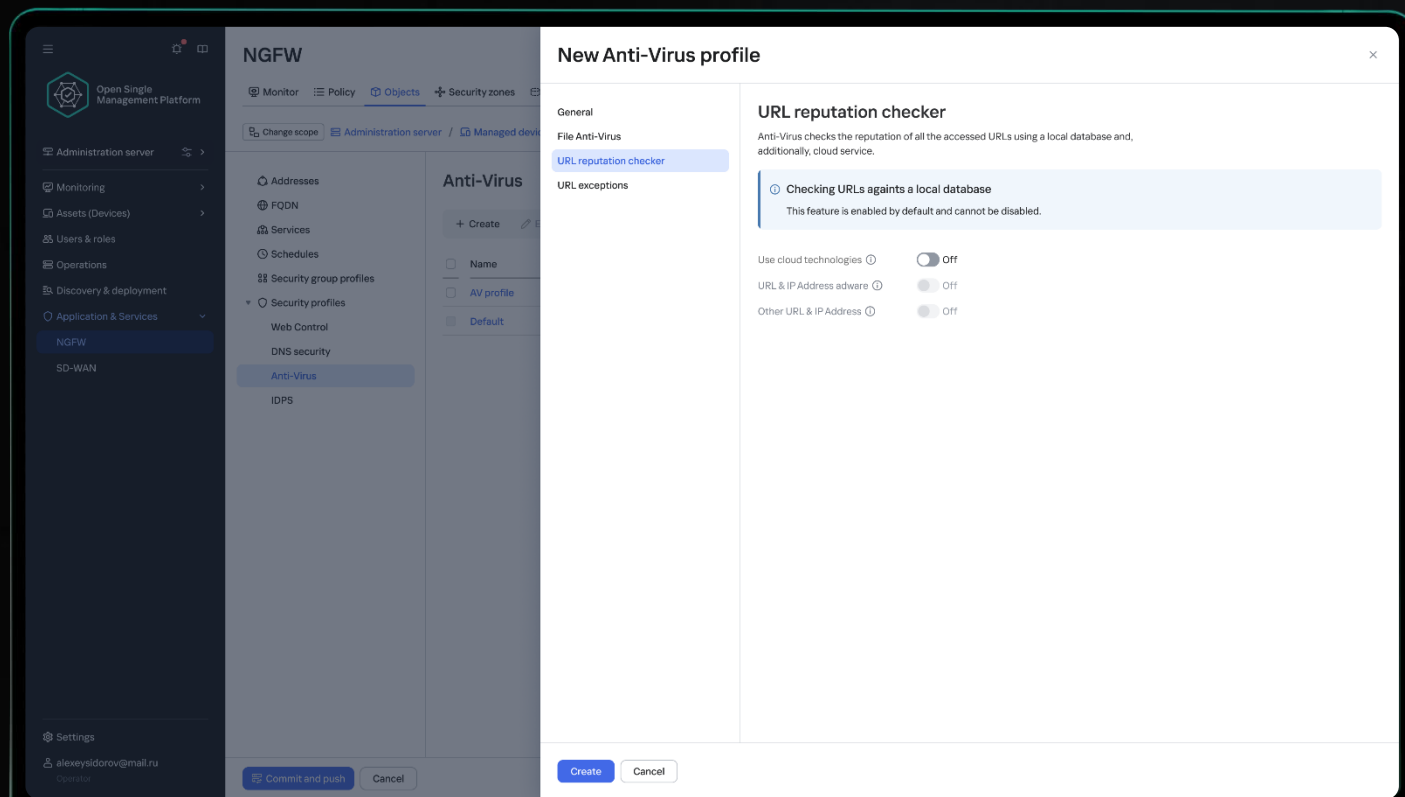
Возможность создания собственных категорий с гибкими сценариями реагирования, в т.ч. блокированием доступа к веб-ресурсам

Локальные базы и непрерывно обновляющиеся данные Kaspersky Security Network

Возможность исключения из проверки конкретных URL-адресов

Проверка репутации URL-адресов

21

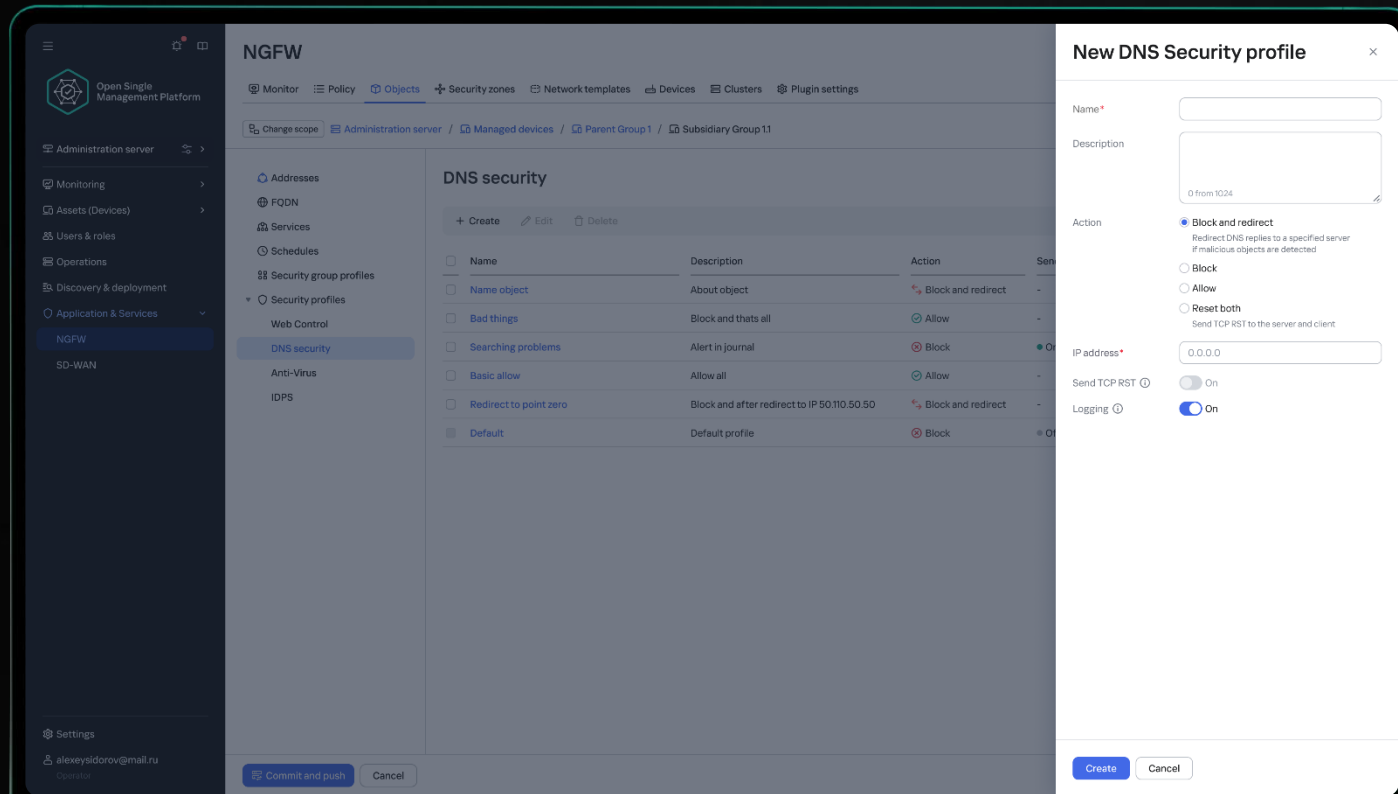


Ограничение доступа к опасным
и потенциально опасным
веб-ресурсам и IP-адресам

Блокировка рекламных
и потенциально опасных ресурсов,
а также C&C-серверов

DNS Security

22

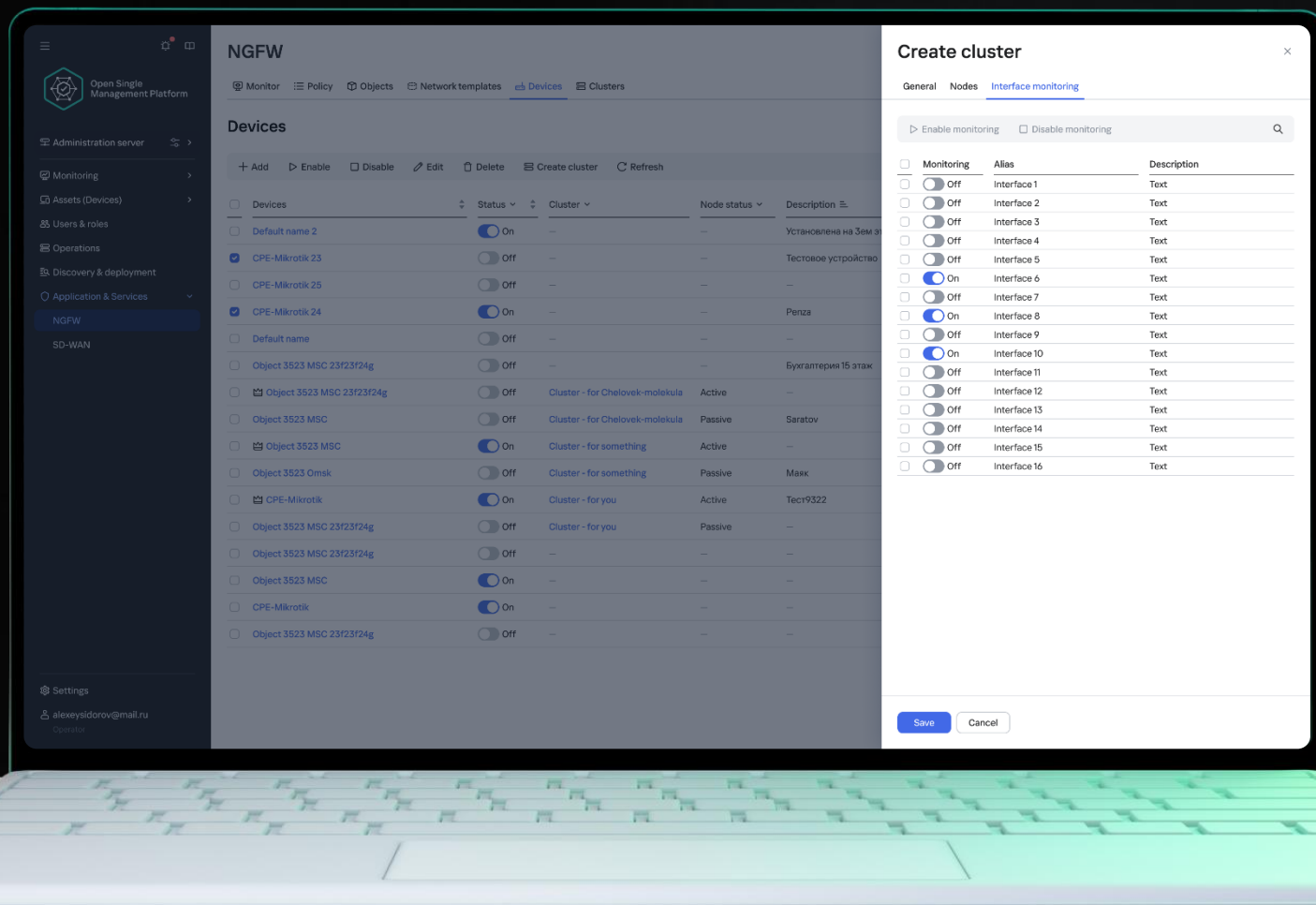


Проверяет принадлежность
доменных имен к потенциально
опасным

Позволяет оптимизировать
производительность за счет
фильтрации на уровне доменов

Кластер active-passive

23



Стабильный кластер с синхронизацией сессий на основе собственного протокола — Kaspersky High-Availability Cluster Protocol

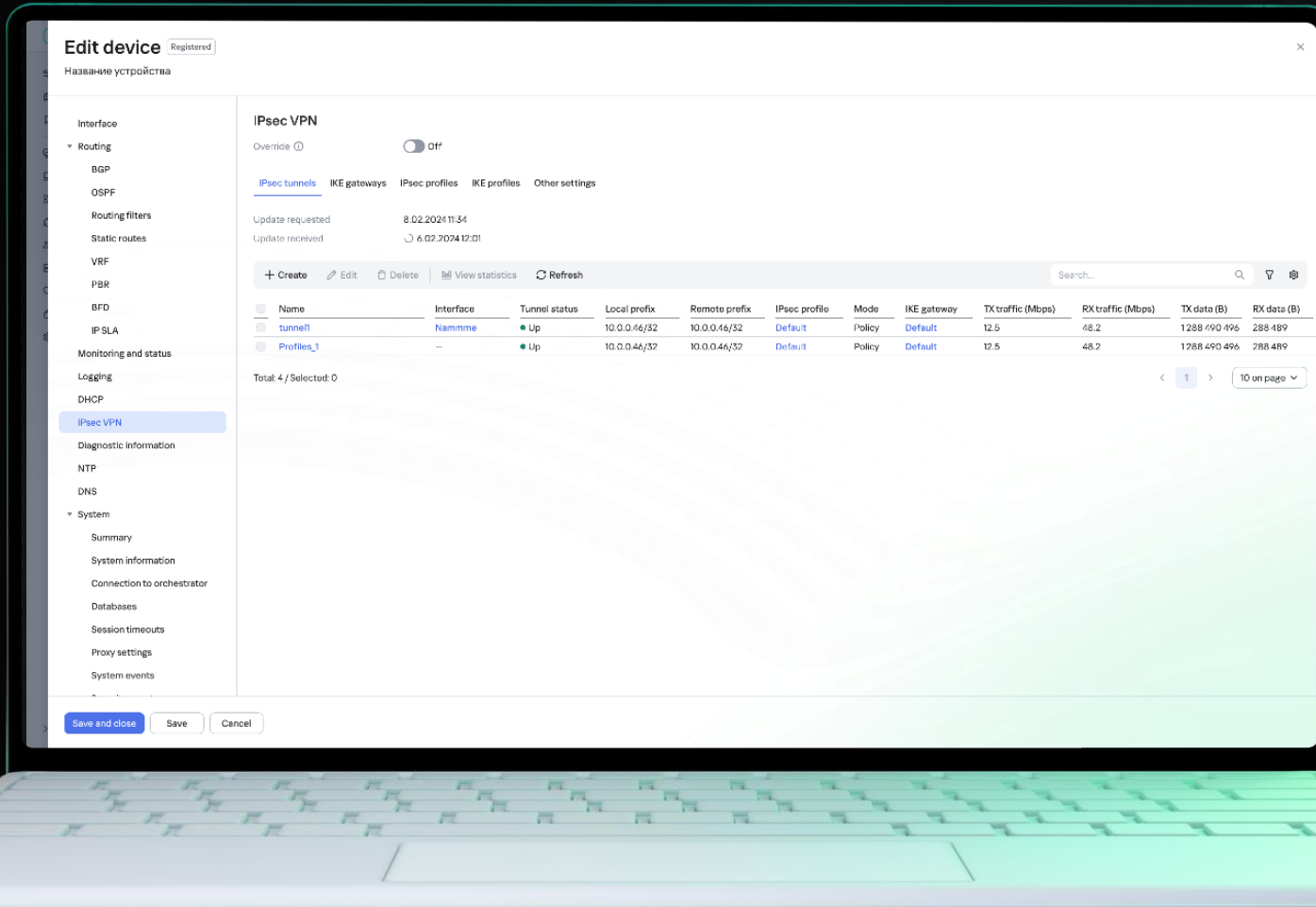
Моментальное переключение между нодами кластера

Мониторинг интерфейсов

Синхронизация маршрутной информации между нодами (RIB)

Site-to-Site VPN

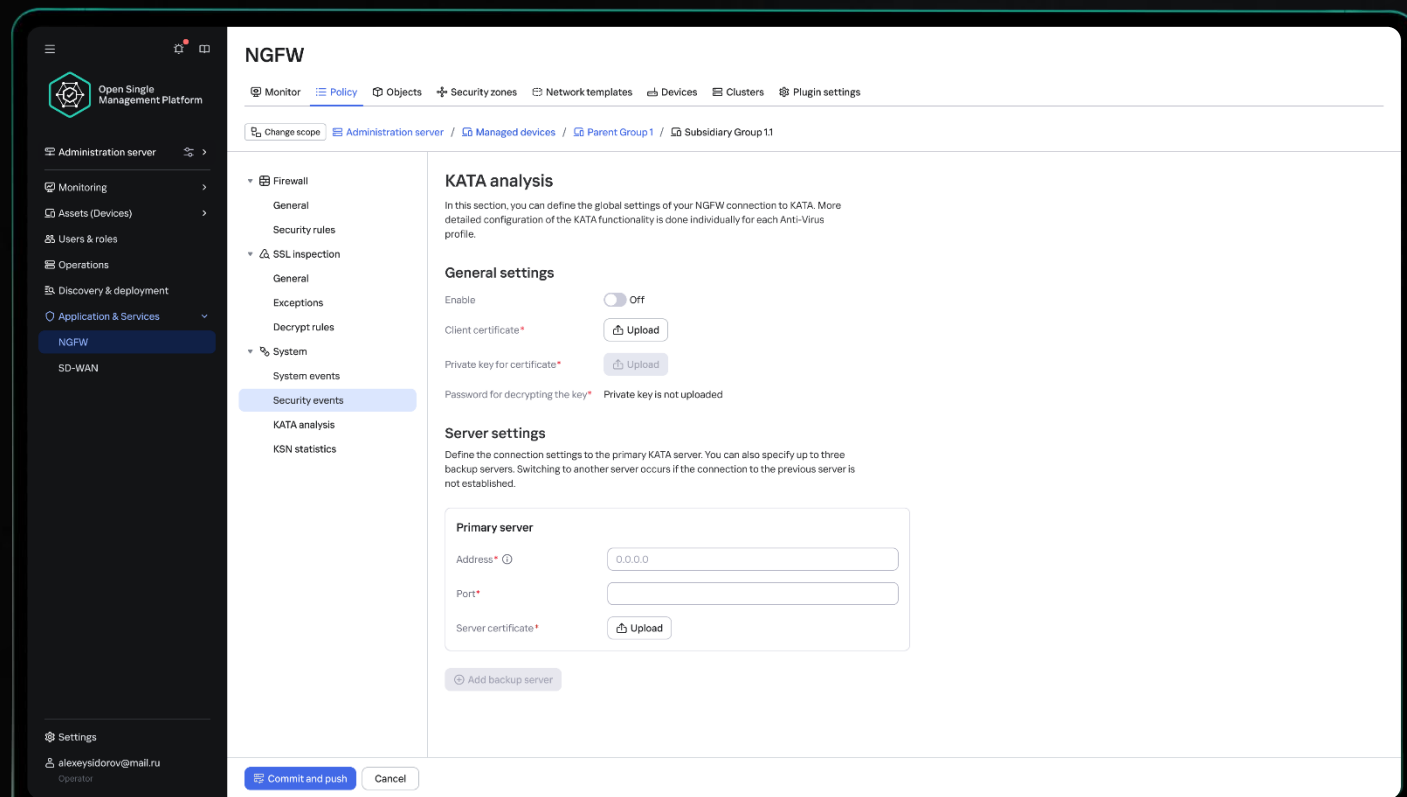
24



Организация защищенного сетевого соединения (туннеля) между географически удаленными офисами или филиалами

Объединение локальных сетей удаленных офисов или филиалов в единое приватное сетевое пространство через интернет

Интеграция с Kaspersky Anti Targeted Attack



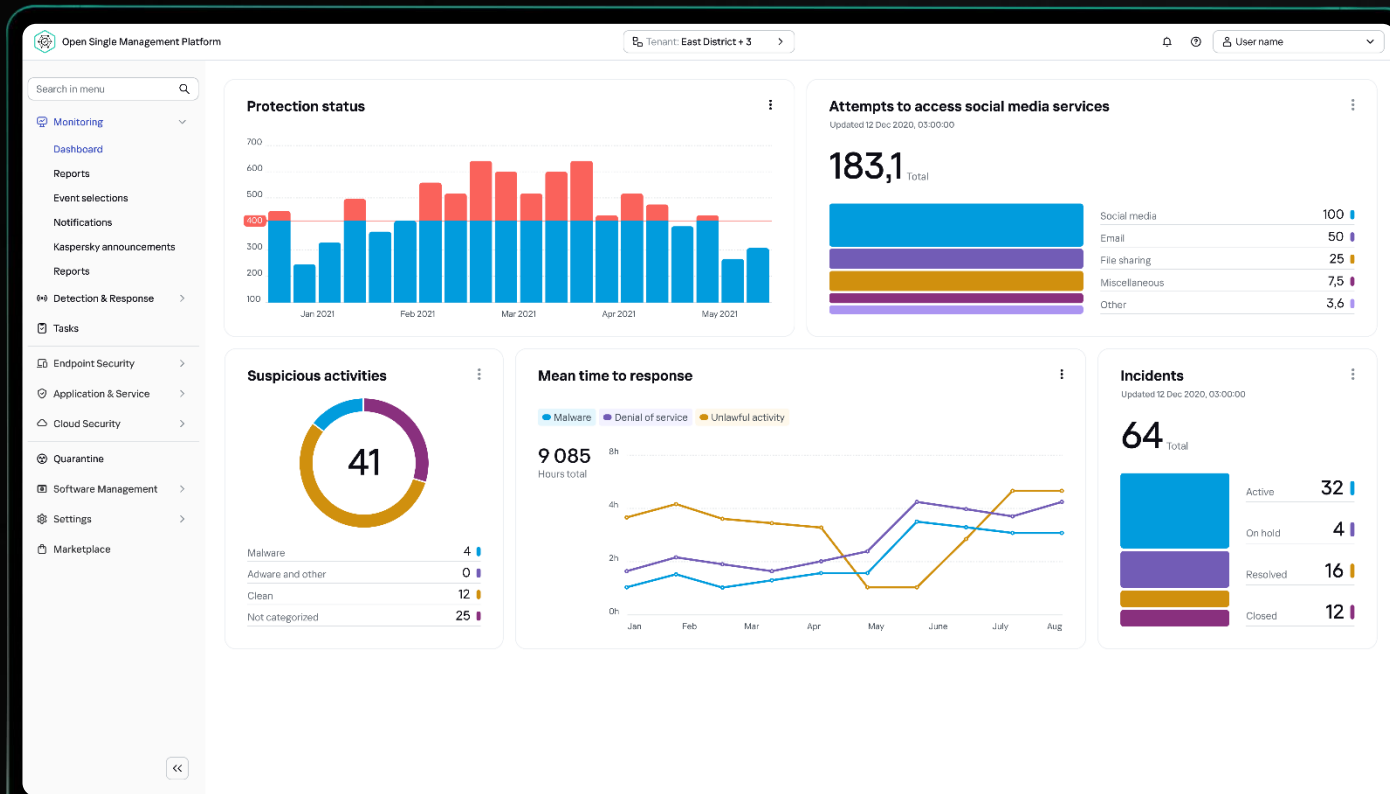
Предотвращение сложных атак и угроз нулевого дня с помощью проверки подозрительных файлов в специальной среде — Sandbox

Интеграция по API для достижения максимальной скорости получения вердикта

Кеширование вердиктов для оптимизации скорости обработки запросов на проверку файлов

Open Single Management Platform

26



Централизованная консоль мониторинга и управления всеми развернутыми 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

Полный список возможностей

27



Функции управления и мониторинга

- Централизованная система управления (Kaspersky Security Center (KSC) + Kaspersky Unified Monitoring and Analysis Platform (KUMA))
- Комплексное управления продуктами экосистемы Kaspersky для XDR-сценария 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
- Мониторинг состояния решения в режиме реального времени
- Экспорт событий в SIEM-системы через Syslog
- Аналитические панели мониторинга и отчеты по результатам работы решения в OSMP или KUMA
- Ролевая модель доступа (RBAC)
- Поддержка виртуальных контекстов (VSS)
- Возможность предварительного просмотра внесенных в политику изменений перед ее применением
- Централизованное управление сетевой конфигурацией при помощи шаблонов
- Поддержка обновления ПО NGFW
- Zabbix-шаблон для мониторинга NGFW
- Командная строка (CLI)
- SNMPv2, SNMPv2c, SNMPv3
- SNMP trap
- Подключение через SSH
- Интеграция по LDAP (MS AD)
- Многофакторная аутентификация TOTP (RFC 6238)
- Языки интерфейса — русский, английский

Полный список возможностей

28

Сетевые функции

- Статическая маршрутизация IPv4
- BGPv4
- OSPFv2
- BFD
- Поддержка агрегированных интерфейсов (LACP)
- Поддержка L2 (bridge) интерфейсов
- Поддержка L3-интерфейсов
- Поддержка VLAN (802.1q) и суб-интерфейсов
- Поддержка VRF
- Поддержка DNS-клиента
- Поддержка DHCP-клиента
- Поддержка NTP-клиента
- Policy-Based Routing (PBR)
- Поддержка Multi-WAN на базе IP SLA
- DHCP Relay

Полный список возможностей

29



Site-to-Site VPN

- Policy-Based IPsec
- Route/GRE-Based IPsec
- IKEv2
- Алгоритмы шифрования
 - AES-CBC-128
 - AES-CBC-192
 - AES-CBC-256
 - AES-GCM-128
 - AES-GCM-192
 - AES-GCM-256
- NAT Traversal



Трансляция сетевых адресов

- Source NAT
- Destination NAT
- Статический NAT
- Динамический NAT
- PAT
- NAT oversubscription

Полный список возможностей

30



Отказоустойчивость

- Поддержка отказоустойчивого кластера active-passive на базе собственного протокола KHCP (Kaspersky High-availability Cluster Protocol)
- Синхронизация сессий
- Синхронизация маршрутной информации (RIB)
- Синхронизация ARP-таблиц
- Мониторинг интерфейсов в кластере
- Поддержка виртуальных MAC и IP-адресов
- GARP
- Режимы автоматического и ручного переключения на резервный узел кластера
- Режим автоматического переключения на резервный канал связи в случае нарушения параметров IP SLA (задержка, потери, доступность)
- Поддержка отказоустойчивости системы управления
- Возможность использования нескольких Sync-интерфейсов для кластера
- Возможность агрегирования management-интерфейсов
- Выделенный control plane



Межсетевой экран

- Поддержка Stateful Packet Inspection
- Поддержка использования зон
- Поддержка фильтрации трафика по:
 - IP-адресам (host, подсеть, диапазон)
 - FQDN
 - Сервисам (L3/L4 протокол + порт)
 - Пользователям и группам пользователей
 - GeoIP
 - Зонам
 - Приложениям и категориям приложений
- Распознавание при помощи DPI более 6 000 приложений
- Интеграция с внешними каталогами пользователей (MS AD)
- Поддержка групп объектов и вложенных групп
- Логирование начала и конца сессии
- Время жизни и/или расписание работы для правил
- Использование групповых профилей модулей безопасности в правилах

Полный список возможностей

31

Функции безопасности

- Поточковый антивирус
- AI-powered антивирус
- Антивирусная проверка по протоколам: HTTP(S), SMTP(S), POP3(S) и IMAP(S)
- Антивирусная проверка архивов с любыми расширениями
- Возможность блокировки Partial Content
- Интеграция с песочницей KATA по API
- ICAP клиент
- Проверка репутации URL-адресов (malware, phishing, c&c, adware и т.п.)
- Система обнаружения и предотвращения вторжений (IDPS) с поддержкой более 9 000 собственных сигнатур
- Возможность исключения сигнатур IDPS
- Захват трафика при сработках сигнатур IDPS
- IDPS проверка по неклассифицированным сессиям
- Инспектирование SSL/TLS-трафика с поддержкой TLS 1.1, 1.2 и 1.3
- Возможность исключений в SSL/TLS-инспекции по веб-категориям и конкретным доменам
- Отправка расшифрованного трафика на анализ всеми модулями безопасности
- Возможность указания минимальной версии TLS
- Валидация сертификата сервера
- Категоризация и контроль веб-трафика по SNI или URL
- Более 90 предустановленных веб-категорий
- Поддержка пользовательских веб-категорий
- Поддержка исключений для веб-фильтрации
- Поддержка работы правил фильтрации по расписанию
- Отображение страниц блокировок и предупреждения при попытке доступа на веб-ресурс
- Поддержка проверки DNS-трафика (DNS Security) по репутационным базам
- Поддержка DNS-redirect
- Защита от IP Spoofing
- Защита от сетевого сканирования
- Возможность настройки периода и источника обновления локальных баз NGFW
- Нативная интеграция с Threat Intelligence для обогащения баз модулей антивируса и веб-фильтрации
- Менеджер сессий для просмотра и контроля установленных сессий
- Возможность настройки таймаутов сессий для устройств и VSS

Полный список возможностей

32



Поддержка
гипервизоров

KVM

VMware ESXi



Интеграция с продуктами
от Лаборатории Касперского



Kaspersky
Symphony
XDR

посредством
плейбуков



Kaspersky
Unified Monitoring
and Analysis Platform



Kaspersky
Anti Targeted
Attack

по API для проверки файлов
с помощью Sandbox

Оборудование и лицензирование

04



Модельный ряд KX-Series

34

KX-Series (Kaspersky Extension)

Семейство сетевых аппаратных платформ, разработанных специально для решения Kaspersky NGFW.

Предназначены для максимального раскрытия потенциала решения в сетевых инфраструктурах любой сложности.

до 200 Гбит/с

производительность в режиме
L4 FW + Application Control

x86

высокая производительность
без использования внешних
ускорителей

1 Rack Unit

удобное исполнение и экономия
места в серверной стойке



высокоскоростные порты
SFP+ и QSFP28

Модельный ряд KX-Series

35

KX-Series (Kaspersky Extension)

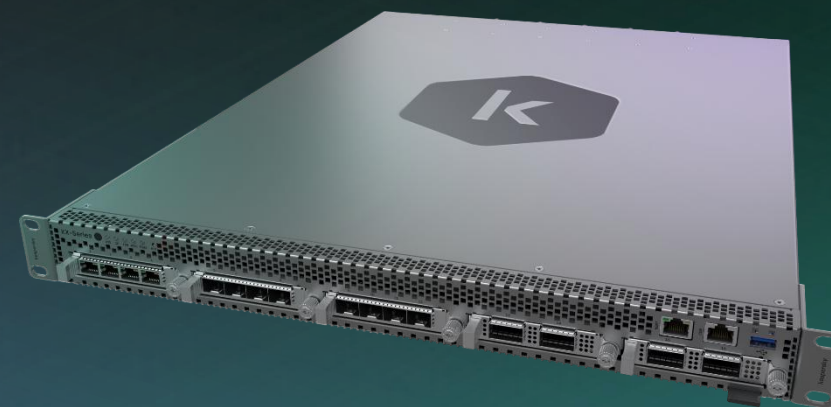
Семейство сетевых аппаратных платформ, разработанных специально для решения Kaspersky NGFW.

Предназначены для максимального раскрытия потенциала решения в сетевых инфраструктурах любой сложности.

Внешний вид моделей
KX-100



Внешний вид моделей
KX-400
KX-1000
KX-3500



Аппаратные платформы



Подробнее о методике
тестирования
производительности



Подробнее
о моделях



Параметры оборудования

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 15 Гбит/с

до 40 Гбит/с

до 140 Гбит/с

Процессор

Intel Atom

Intel Atom

Intel Xeon Gen 4

Intel Xeon Gen 5

Intel Xeon Gen 5

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

Крепление

Настольное
размещение
или в серверной
стойке 19"

Размещение в
серверной
стойке 19"

Размещение в
серверной
стойке 19"

Размещение в
серверной
стойке 19"

Размещение в
серверной
стойке 19"

* Тестирование проводилось с 20 000 правил Firewall и включенным логированием

Виртуальные платформы



Подробнее о методике
тестирования
производительности



Подробнее
о модели



vKX



Виртуальные исполнения, предназначенные для развертывания Kaspersky NGFW на собственных ресурсах заказчика без необходимости использования аппаратных платформ.

В данный момент доступно виртуальное исполнение Kaspersky NGFW vKX-8.

Параметры оборудования

vKX-8

Производительность в режиме
L4 FW + Application Control*

до 5 Гбит/с

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

до 4 Гбит/с

Гипервизоры

KVM или VMware ESXi

Интерфейсы

10 шт.

Формат поставки

- QCOW2 + XML файл
- OVA

* Тестирование проводилось с 20 000 правил Firewall и включенным логированием

Базовые параметры

- Запросы обрабатываются экспертами «Лаборатории Касперского»
- Приоритетная телефонная линия в режиме 24/7 для критических ситуаций
- Удаленное подключение при необходимости

Указанные параметры обслуживания включены в оба представленных варианта технической поддержки.



Лицензии Kaspersky NGFW включают в себя техническую поддержку в соответствии с выбранным уровнем обслуживания.

Premium

Прием запросов по инцидентам

Уровень критичности 1 в режиме 24×7, остальные с 10:00 по 18:30 (по Москве)

Время реакции на инциденты:

- Уровень критичности 1 – 2 часа*
- Уровень критичности 2 – 6 рабочих часов
- Уровень критичности 3 – 8 рабочих часов
- Уровень критичности 4 – 10 рабочих часов

Контактные лица

4 – возможное количество контактных лиц со стороны клиента

Premium Plus

Прием запросов по инцидентам

Уровни критичности 1 и 2 в режиме 24×7, остальные с 10:00 по 18:30 (по Москве)

Время реакции на инциденты:

- Уровень критичности 1 – 30 минут*
- Уровень критичности 2 – 4 часа*
- Уровень критичности 3 – 6 рабочих часов
- Уровень критичности 4 – 8 рабочих часов

Контактные лица

8 – возможное количество контактных лиц со стороны клиента



Персональный
технический менеджер

Отчеты по открытым
инцидентам

* В нерабочее время необходимо дополнительное обращение по телефону

Гарантия на аппаратные платформы

39

Для аппаратных платформ модельного ряда KX-Series доступна расширенная гарантия (Hardware MSA).



Гарантия на аппаратные платформы приобретается отдельно.

Расширенная гарантия Hardware MSA

Срок

Возможность ежегодного продления до трех лет через «Лабораторию Касперского»

Тип обслуживания

On-site (на месте эксплуатации оборудования)

Прием запросов и время реакции:

- Прием заявок в режиме 24/7
- Время реагирования до 24 часов

Логистика

Забор дефектного и доставка отремонтированного или подменного оборудования за счет производителя*

Поддержка:

- Первая линия поддержки в «Лаборатории Касперского»
- Последующий мониторинг закрытия инцидента после передачи оборудования производителю или его партнеру

Замена устройств:

- Авансовая замена с отгрузкой на следующий календарный день с сервисного склада в Москве
- Возможность создания подменного фонда в регионах для обеспечения быстрой отгрузки при условии предоставления «Лаборатории Касперского» информации о месте установки устройства

* За исключением дефектов, возникших по вине клиента

Возможности		Standard	Advanced	
	Управление, мониторинг и интеграция в сеть	Централизованное управление и мониторинг	•	•
		Маршрутизация	•	•
		VRF	•	•
		Поддержка виртуальных контекстов (VSS)	•	•
	Контроль сетевых соединений	Межсетевой экран с отслеживанием состояния сессий (Stateful Firewall)	•	•
		User-aware политики	•	•
		Контроль трафика приложений с помощью Deep Packet Inspection (DPI)*	•	•
	Защита от сетевых угроз	SSL/TLS-инспекция	•	•
		Система обнаружения и предотвращения вторжений (IDPS)*	•	•
		Антивирус + интеграция с Kaspersky Security Network*	•	•
	Контроль веб-ресурсов	Проверка репутации URL-адресов + интеграция с Kaspersky Security Network*		•
		Веб-фильтрация + интеграция с Kaspersky Security Network*		•
		Проверка DNS-трафика*		•

* Функции продолжают работать после окончания срока действия лицензии, но обновление собственных баз и взаимодействие с Kaspersky Security Network недоступно

Модель лицензирования



Подробнее
о лицензировании



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 EPS*)

Скидка 95%
в течение года

Пример

KX-3500

В варианте
Advanced

С включенной технической
поддержкой уровня
Premium

* Events Per Second (события в секунду)

Интеграционные сценарии

05

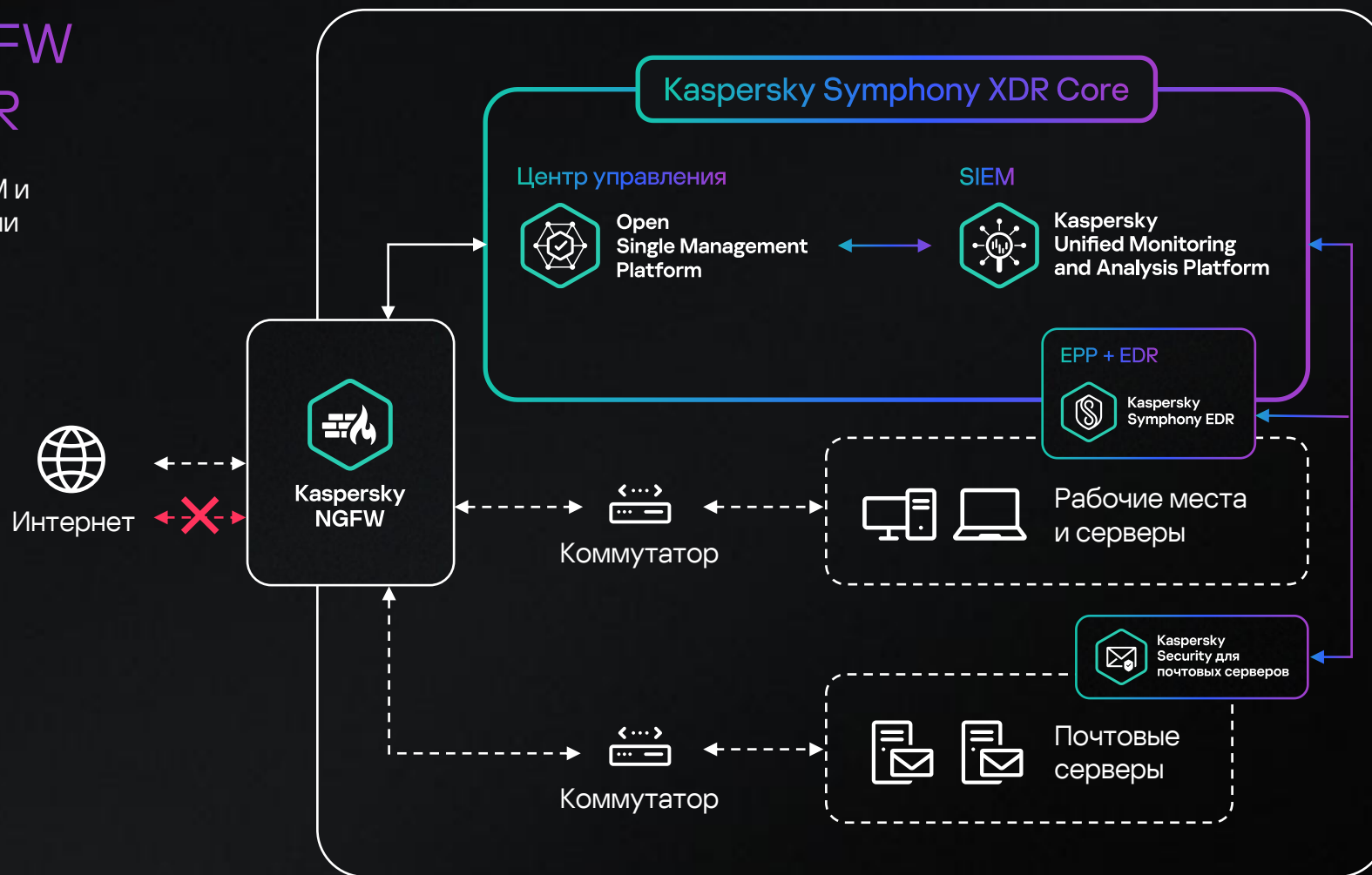
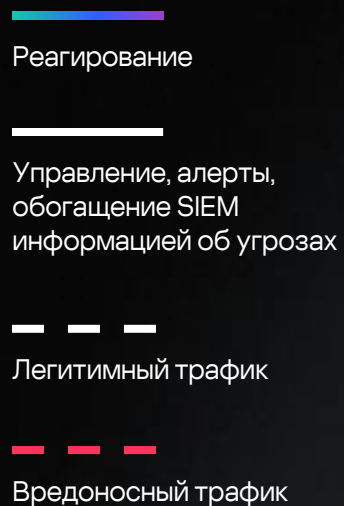


Интеграционные сценарии

43

Интеграция Kaspersky NGFW и Kaspersky Symphony XDR

- Передача информации об угрозах (алертов) в SIEM и обогащение картины кибербезопасности компании
- Реагирование с помощью продуктов экосистемы Kaspersky Symphony XDR

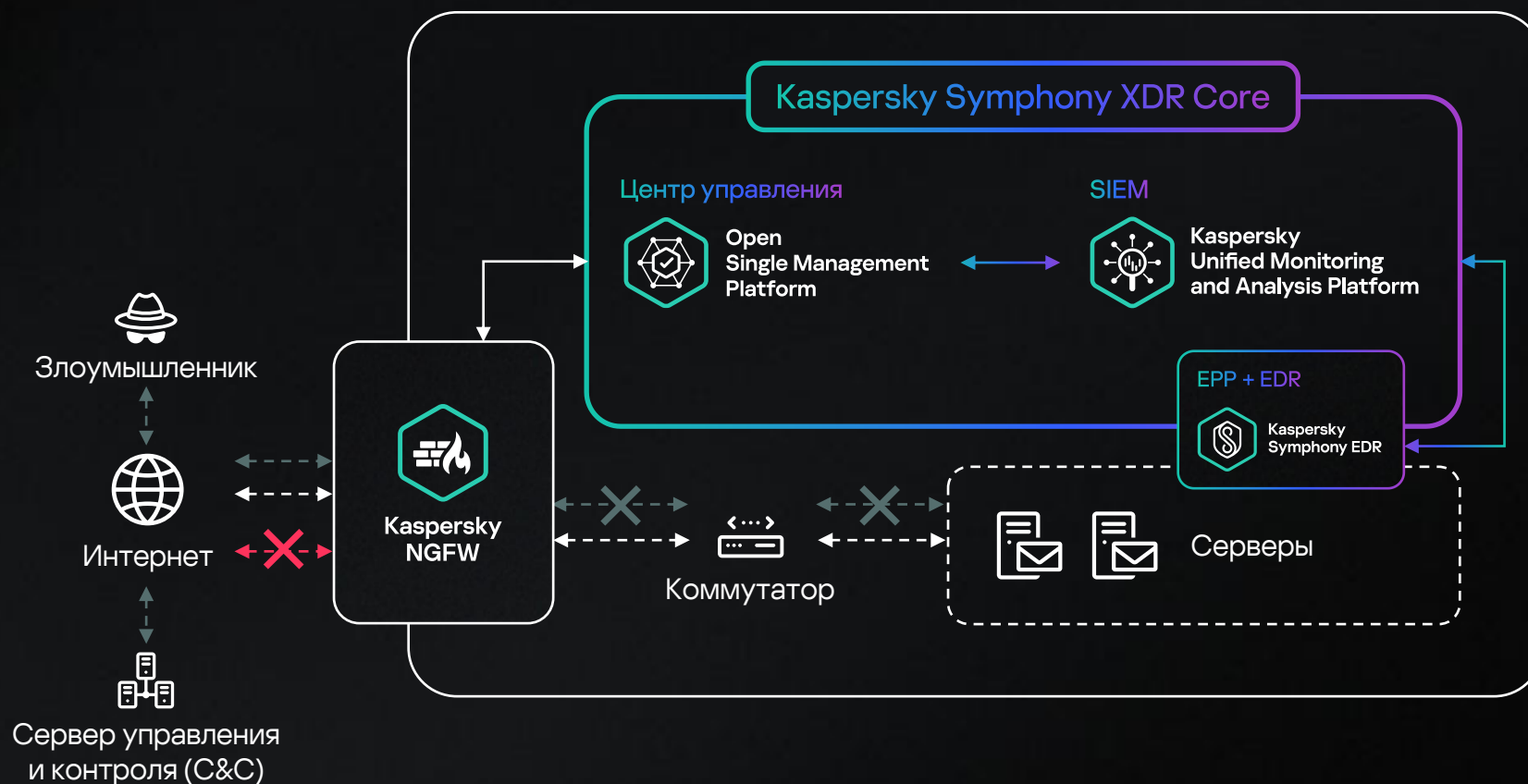


Интеграционные сценарии

44

Блокирование установленной сессии

- Злоумышленник устанавливает соединение с серверами в инфраструктуре компании, используя учетные данные администратора
- При попытке подключения с внутреннего сервера компании к С&С-серверу установленные сессии блокируются с помощью Kaspersky NGFW
- Осуществляется реагирование на конечных точках с помощью Kaspersky Symphony EDR (блокирование скомпрометированной учетной записи администратора)



Реагирование

Управление, алерты, обогащение SIEM информацией об угрозах

Легитимный трафик

Вредоносный трафик

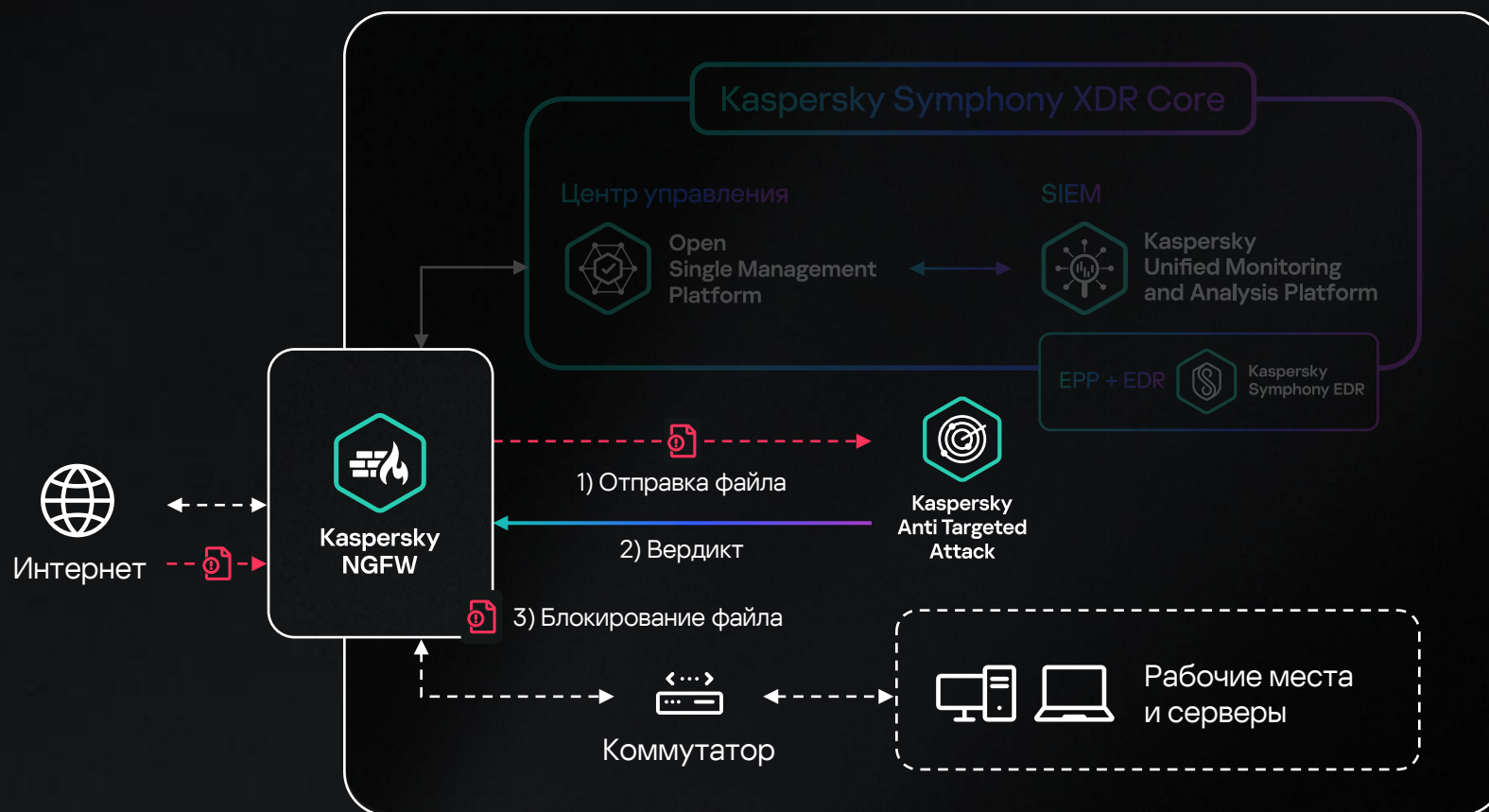
Нелегитимный трафик

Интеграционные сценарии

45

Интеграция Kaspersky NGFW и Kaspersky Anti Targeted Attack

1. Файл отправляется с Kaspersky NGFW на Kaspersky Anti Targeted Attack для дополнительной проверки на наличие угроз с помощью песочницы (Sandbox)
2. По результатам анализа Kaspersky Anti Targeted Attack отправляет вердикт на Kaspersky NGFW
3. Если в файле найдены угрозы или он не соответствует заданным политикам, Kaspersky NGFW блокирует файл и возможность его дальнейшего распространения в инфраструктуре компании



Интеграционные сценарии

46

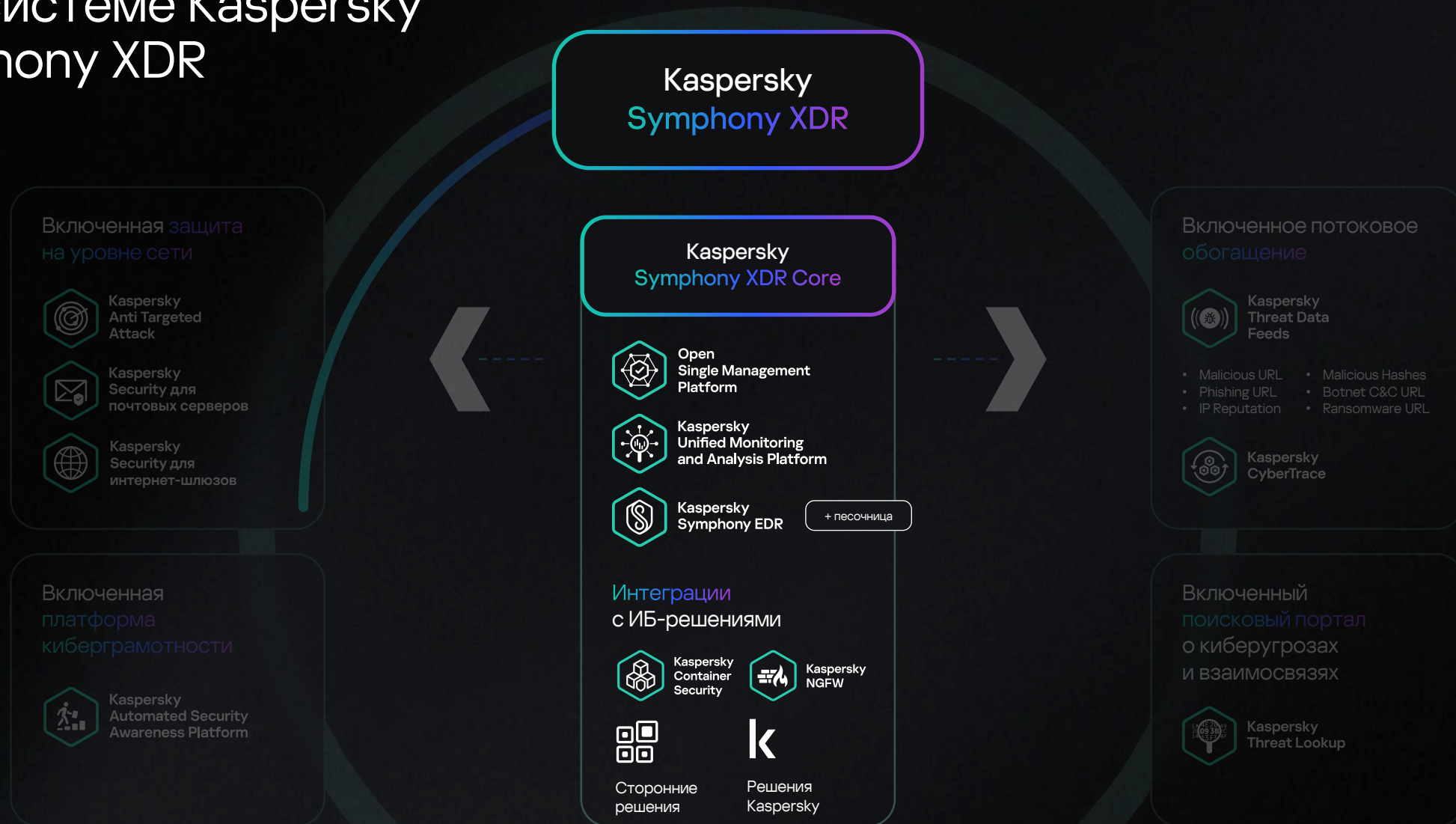
Движок безопасности (возможность)	Защита периметра или сегментация сети  Kaspersky NGFW	Защита от продвинутых угроз и сетевая аналитика  Kaspersky Anti Targeted Attack	Защита корпоративной почты  Kaspersky Security для почтовых серверов	Защита и реагирование на конечных точках  Kaspersky Security для бизнеса  Kaspersky Symphony EDR
Антивирусная проверка	 Возможность выбора между потоковым и оптимизированным под защиту периметра объектным антивирусом	 Встроенный объектный антивирус	 Антивирусная проверка почтовых вложений	 Полноценный объектный антивирус с возможностью гранулярной настройки проверок
Контроль веб-ресурсов	 Возможность фильтрации по URL и категориям, в т.ч. проверка репутации URL	 Анализ сетевого трафика и алертов, но не классический контроль веб-ресурсов	 Возможность фильтрации почтовых вложений по содержимому и проверки URL в сообщениях	 Возможность фильтрации по URL, категориям и содержимому вложений
Анти-фишинг и анти-спам	 Есть анти-фишинг (контроль фишинговых ссылок)	 Обнаружение фишинга как часть анализа атак/алертов, но не классические анти-фишинг и анти-спам	 Встроенные полноценные движки анти-фишинг и анти-спам с анализом заголовков и черными/белыми списками	 Встроенная проверка сообщений и вложений на наличие фишинга и спама
SSL/TLS-инспекция	 Возможность расшифровки любых версий SSL и TLS с последующим анализом всеми движками безопасности	 Расшифровка возможна только сторонними средствами (SSLSplitter) с последующим анализом	 Поддержка TLS для почты, возможность расшифровки зависит от сценария	 Ряд движков может расшифровывать и проверять сетевой трафик
Сетевой экран (Firewall)	 Встроенный полноценный межсетевой экран (Stateful Firewall) с возможностью гранулярной настройки			 Встроенный сетевой экран (Firewall) для контроля соединений и приложений на хосте

Интеграционные сценарии

47

Движок безопасности (возможность)	Защита периметра или сегментация сети  Kaspersky NGFW	Защита от продвинутых угроз и сетевая аналитика  Kaspersky Anti Targeted Attack	Защита корпоративной почты  Kaspersky Security для почтовых серверов	Защита и реагирование на конечных точках  Kaspersky Security для бизнеса  Kaspersky Symphony EDR
Контроль приложений	 Полноценный контроль трафика приложений и сетевых сервисов	 Определение трафика приложений для выявления аномалий в нем		 Полноценное управление приложениями, правами доступа и группами
IDPS (IDS/IPS)	 Встроенная система обнаружения и предотвращения вторжений (IDPS)	 Встроенная система обнаружения вторжений с фокусом на выявлении аномалий в сетевом трафике		 Отслеживание во входящем трафике аномальных активностей
Sandbox	 Только возможность интеграции с Kaspersky Anti Targeted Attack	 Полноценный модуль «песочницы» для гранулярного анализа подозрительных файлов	 Только возможность интеграции с Kaspersky Anti Targeted Attack	 Только возможность интеграции с Kaspersky Anti Targeted Attack
Kaspersky Security Network (KSN)	 Взаимодействие с KSN для получения информации об актуальных угрозах	 Взаимодействие с KSN для получения информации об актуальных угрозах	 Взаимодействие с KSN для получения информации об актуальных угрозах	 Взаимодействие с KSN для получения информации об актуальных угрозах

Kaspersky NGFW в экосистеме Kaspersky Symphony XDR



Kaspersky NGFW в экосистеме Kaspersky Symphony XDR

49



Преимущества Kaspersky NGFW

06



Преимущества Kaspersky NGFW для российских компаний

51



Собственная архитектура и движки безопасности, основанные на лидерских технологиях



Полный контроль и эффективное управление сетевым трафиком и активностью приложений



Экосистемный подход к защите корпоративной инфраструктуры и централизованное управление

Преимущества Kaspersky NGFW для российских компаний

52



Полностью российский продукт, соответствующий стратегии движения к импортонезависимости (сертификация ФСТЭК России)



Прозрачное лицензирование без дополнительных модулей и расширений



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

Уникальный опыт экспертов в основе решения

53



[Подробнее](#)



Глобальный центр исследований и анализа угроз

Исследование сложных угроз и расследование финансово мотивированных киберпреступлений



Центр исследования технологий искусственного интеллекта

Обнаружение угроз с помощью ИИ / усиление ИБ решений алгоритмами ИИ



Центр исследования угроз

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



Центр исследования безопасности промышленных систем*

Анализ угроз в промышленных инфраструктурах



Исследование угроз

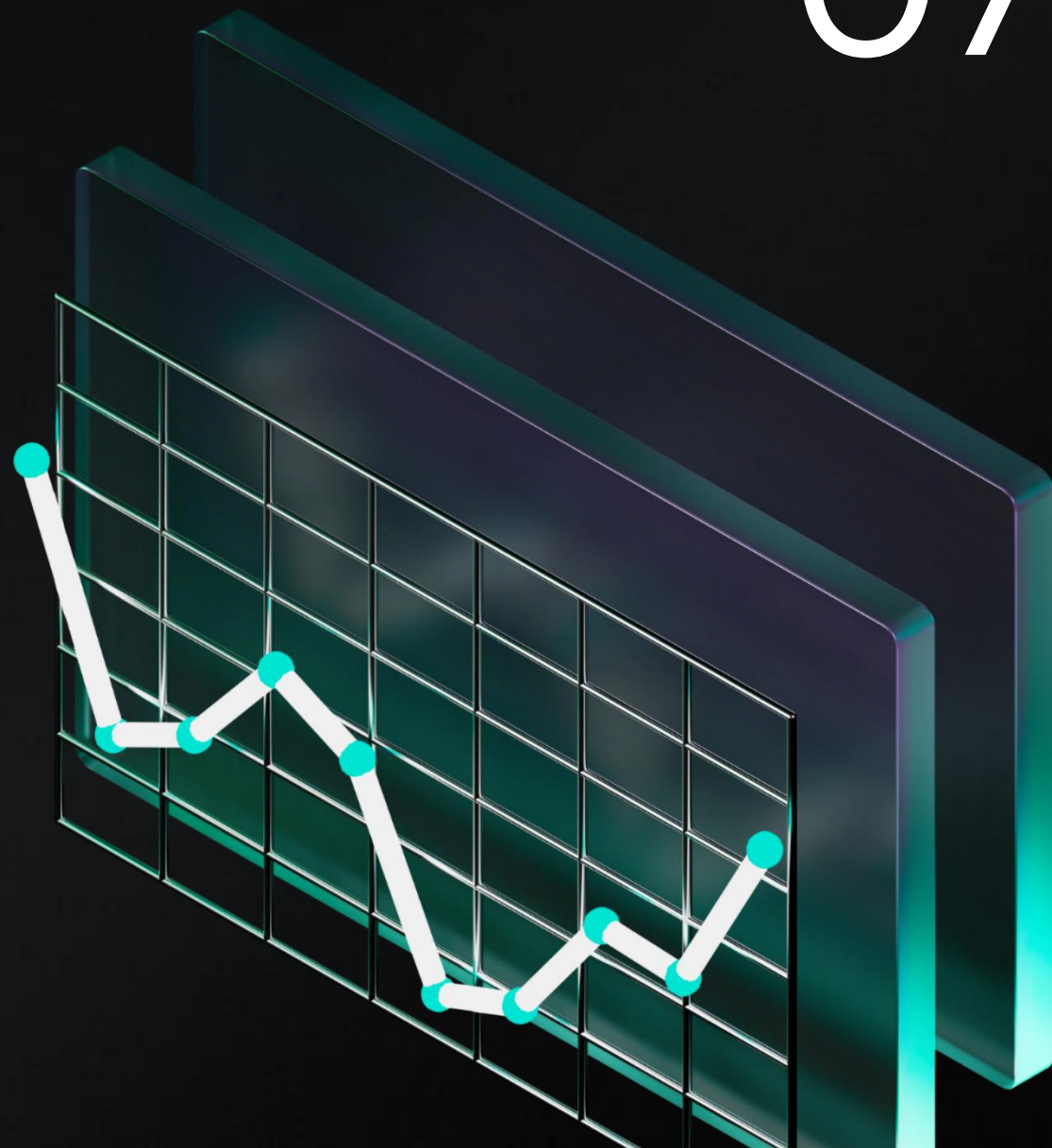


Расследование инцидентов

* В рамках разработки решения для промышленных инфраструктур, с 2027 года

План развития продукта

07



План развития на 2026 год

55

2.0*

Q4 2026

Сеть и интеграции

- Контроль пропускной полосы
- Политики DoS Protection
- RA VPN gateway
- Новые аппаратные платформы
- Поддержка ALD Pro для user aware политик

Диагностика

- Hit counters в правилах (веб-интерфейс)
- Эмуляция прохождения пакета по модулям NGFW
- Отображение связи объектов и правил политик

Развитие сценариев безопасности

- ALG для VoIP и FTP
- Поддержка промышленных протоколов
- Double NAT + Hairpin NAT
- Кастомизация страниц-заглушек (антивирус / веб-фильтрация)

Внешние интеграции

- Подключение внешних динамических списков
- Нативная интеграция с Kaspersky CyberTrace

* Возможны изменения

Планы развития на 2027+

56

*2027+

Инфраструктура и надежность

- Active-Active кластер + Геораспределенный кластер
- IPv6
- QoS
- DHCP Server
- Выделение ресурсов для виртуальных систем
- Новые аппаратные платформы

Сетевая гибкость

- Объединение NGFW и SD-WAN
- ZTNA
- Netflow
- Зеркалирование расшифрованного трафика
- OSPF и IPsec в нескольких VRF
- Поддержка дополнительных BGP атрибутов

Развитие безопасности

- Поведенческий анализ в IDPS
- Интерактивная интеграция: KATA Sandbox + EPP + XDR
- Создание собственных сигнатур для IDPS и DPI
- Развитие AV (Websocket+SMB)
- SSH Inspection
- Расширение функций веб-фильтрации
- Парсинг syslog для user aware политик

Эксплуатация и UX

- AI-ассистент
- Иерархические политики
- Блокировка политик на время редактирования
- Развитие commit-based системы в веб
- Инверсивные объекты
- Локальный веб-интерфейс + RBAC
- RADIUS, TACACS+
- Мониторинг и централизованное обновление через OSMP/KSC

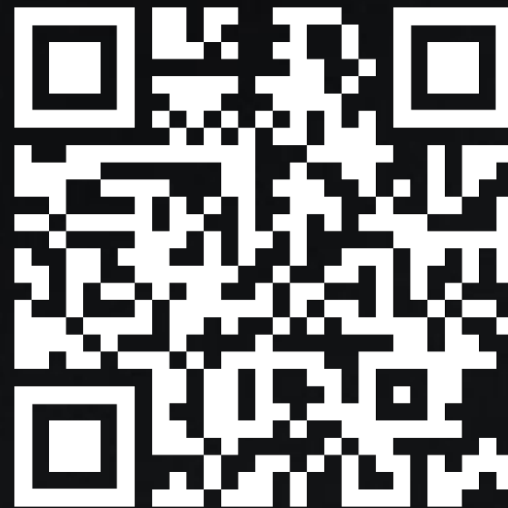
* Возможны изменения



Узнать о продукте
на сайте

«Лаборатории Касперского»
или запросить демо

Подробнее



Задать вопросы
о продукте

в нашем официальном
Telegram-канале

Подробнее



Станьте одним
из первых, кто
сможет забыть
о сетевых
угрозах

Спасибо!

Центральный офис «Лаборатории
Касперского»: Россия, Москва, 125212
Ленинградское шоссе, д.39А стр.3

+7 (495) 797-8700
kaspersky.com