Интеграционные возможности

Kaspersky NGFW

kaspersky активируй будущее

Интеграционные возможности и сценарии взаимодействия

Kaspersky NGFW — межсетевой экран нового поколения для защиты российских компаний от современных сетевых угроз. Продукт анализирует сетевые активности по целому ряду параметров и выявляет угрозы даже в зашифрованном трафике. Решение является основой для защиты корпоративных сетей.

В рамках экосистемного подхода Kaspersky NGFW поддерживает интеграцию с решениями класса XDR, Sandbox и SIEM «Лаборатории Касперского», а также SIEM-системами сторонних производителей:

Kaspersky Symphony XDR

для автоматизации управления безопасностью и реализации сценариев реагирования

Kaspersky Anti Targeted Attack

для предотвращения сложных атак и угроз нулевого дня

Kaspersky Unified Monitoring and Analysis Platform

для сбора и корреляции событий безопасности

Помимо интеграций с перечисленными решениями возможны сценарии взаимодействия с другими продуктами «Лаборатории Касперского»:

Kaspersky Security для бизнеса

Kaspersky Symphony EDR

для защиты конечных точек

Kaspersky Security для почтовых серверов

для защиты корпоративной почты

Kaspersky Automated Security Awareness Platform

для развития навыков кибербезопасности сотрудников

Дополнительно Kaspersky NGFW поддерживает взаимодействие с Kaspersky Security Network для обогащения решения уникальной информацией об актуальных угрозах.

Управление и мониторинг осуществляется через единую для всех продуктов «Лаборатории Касперского» консоль – Open Single Management Platform.

Сценарий взаимодействия с Kaspersky Symphony XDR и включенными продуктами платформы

Возможности:

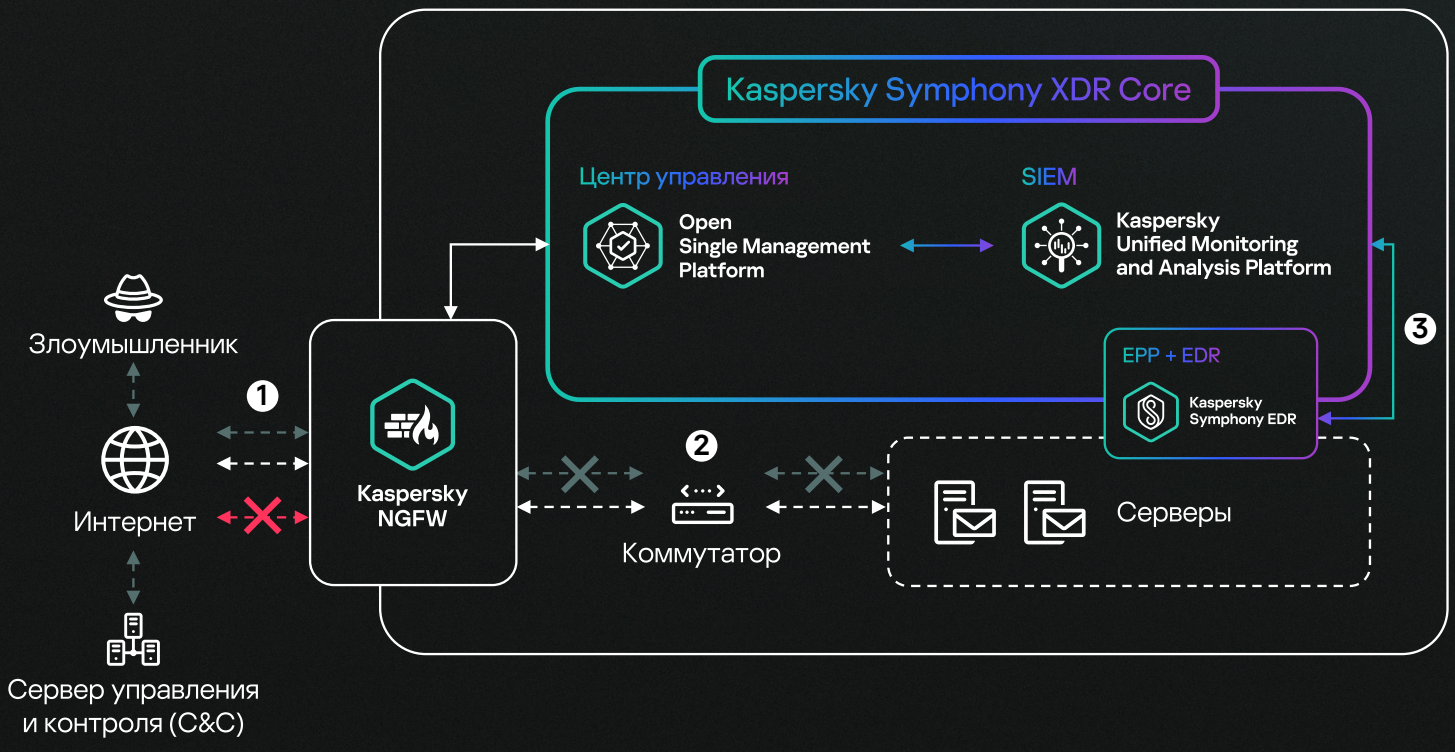
Передача информации об угрозах (алертов) в SIEM и обогащение картины кибербезопасности компании

Реагирование с помощью продуктов экосистемы Kaspersky Symphony XDR

Пример:

Блокирование установленной сессии и IP-адреса скомпрометированного хоста

1. Злоумышленник устанавливает соединение с серверами в инфраструктуре компании, используя учетные данные администратора
2. При попытке подключения с внутреннего сервера компании к C&C-серверу установленные сессии блокируются, а зараженный хост изолируется с помощью Kaspersky NGFW
3. 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

Сценарий взаимодействия с Kaspersky Anti Targeted Attack

Возможности:

Проверка подозрительных файлов в специальной среде — Sandbox

Интеграция по API для достижения максимальной скорости получения вердикта

Кеширование вердиктов на Kaspersky NGFW для оптимизации скорости обработки запросов на проверку файлов

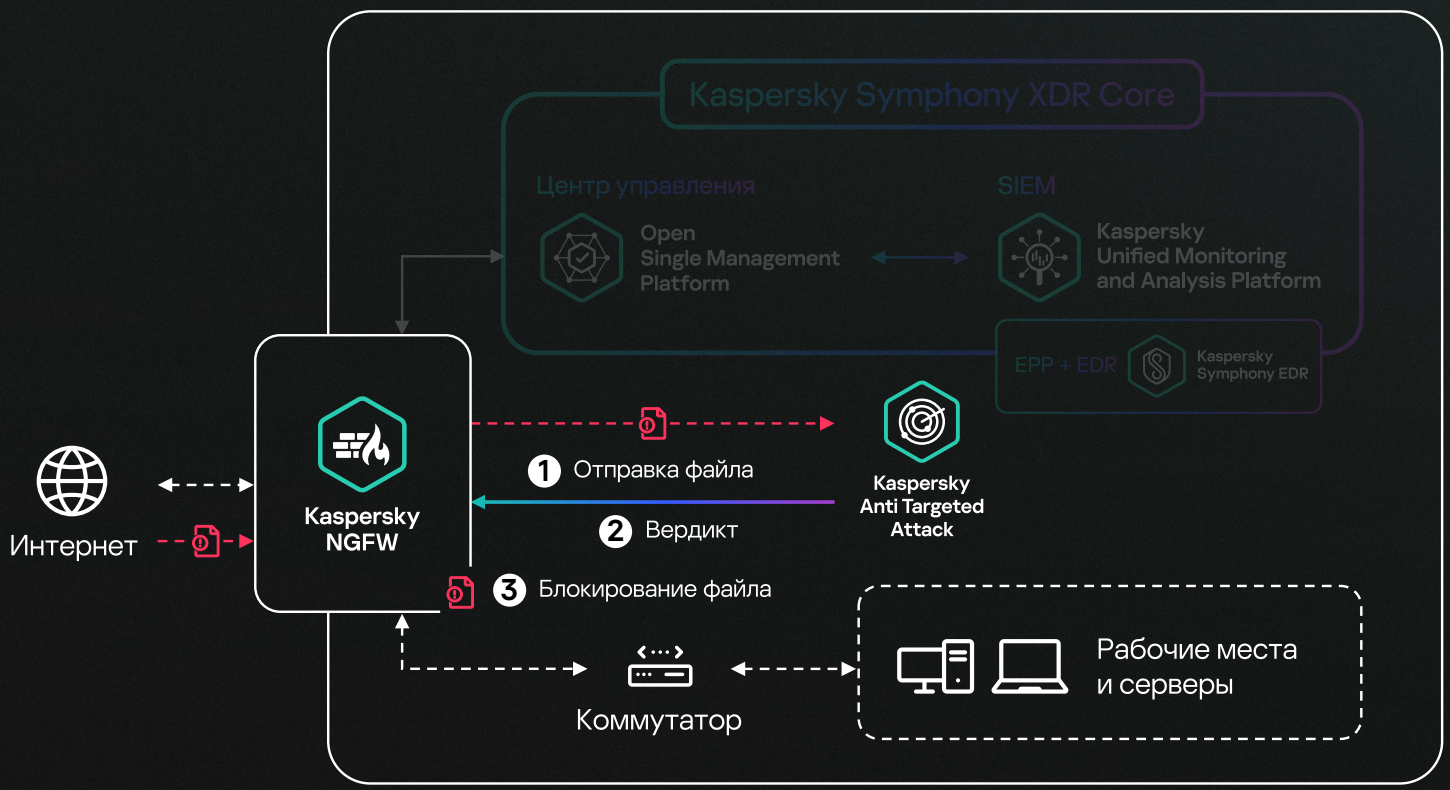
Пример:

Проверка подозрительного файла

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



Реагирование

Управление, алерты, обогащение SIEM информацией об угрозах

Легитимный трафик

Вредоносный файл

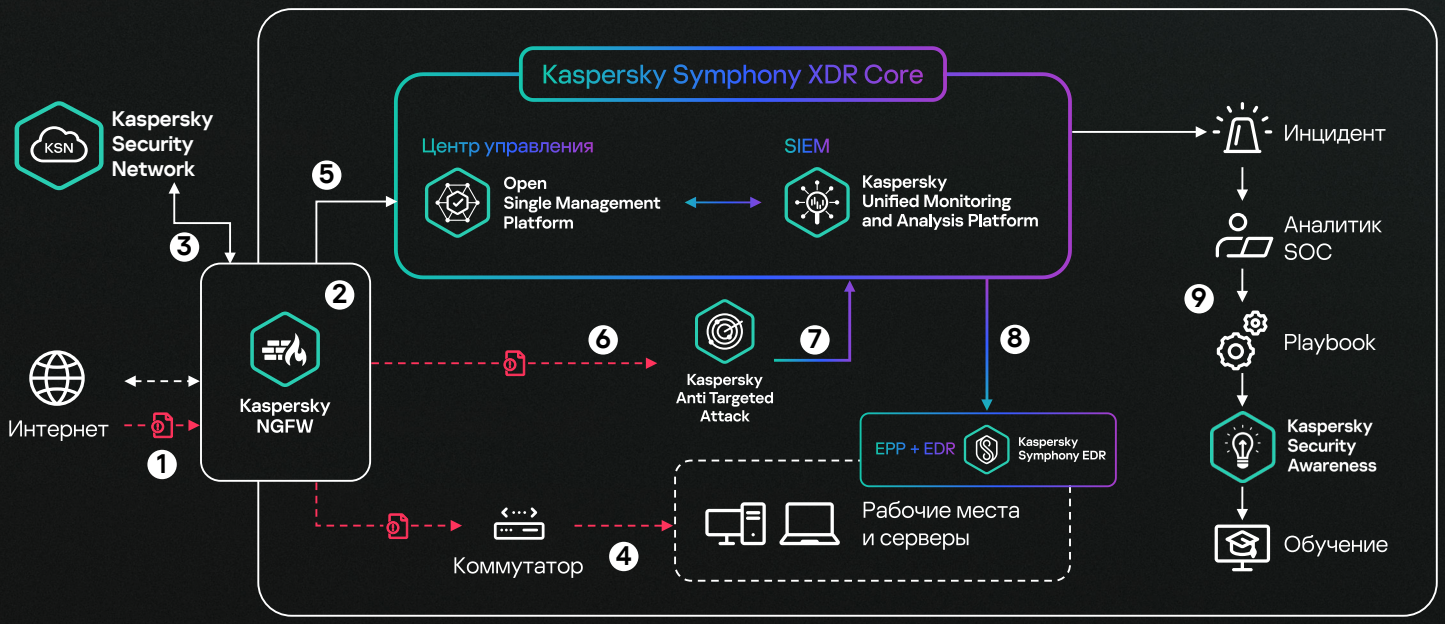
Пример комплексного сценария взаимодействия Kaspersky NGFW с продуктами «Лаборатории Касперского»

Таргетированный фишинг: обнаружение и реагирование

1. Пользователь становится жертвой таргетированного фишинга
2. Kaspersky NGFW проверяет загружаемый файл потоковым и объектным антивирусом
3. Kaspersky NGFW уточняет репутацию файла через Kaspersky Security Network

> Несмотря на используемые движки, ввиду целевой атаки файл имеет неизвестную репутацию и не поддается детектированию

4. Пользователь загружает файл
5. Kaspersky NGFW отправляет журнал загрузки файла с неизвестной репутацией в Kaspersky Symphony XDR
6. Kaspersky NGFW направляет файл на анализ в Kaspersky Anti Targeted Attack
7. Модуль Sandbox в Kaspersky Anti Targeted Attack отправляет журнал в Kaspersky Symphony XDR
8. Kaspersky Symphony XDR запускает команду реагирования для помещения хоста в сетевой карантин
9. Проводится анализ первопричин и запуск скрипта для назначения релевантного обучения пользователю с помощью Kaspersky Automated Security Awareness Platform



Реагирование

Управление, алерты, обогащение SIEM информацией об угрозах

Легитимный трафик

Фишинг

Взаимодействие движков безопасности Kaspersky NGFW и похожих технологий смежных продуктов экосистемы

Под капотом Kaspersky NGFW находится целый ряд технологий и движков безопасности. В рамках построения комплексной системы защиты инфраструктуры важно понимать, чем отличаются возможности этих технологий от похожих механизмов в других классах решений и как они взаимодействуют между собой.

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

	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

Ключевые выводы на основе сравнения

Kaspersky NGFW — база для защиты корпоративной сети так же, как решения класса EPP/EDR для конечных точек

Полноценная защита почтового трафика возможна только при совместной работе специализированного решения и Kaspersky NGFW

Для выявления сложных угроз и целевых атак важен гранулярный анализ сетевого трафика с помощью модулей Sandbox и NDR

Антивирусные движки, IDS/IPS, технологии контроля веб-трафика, анти-фишинг — в зависимости от класса решения эти механизмы защиты нацелены на решение разных задач

Интеграция Kaspersky NGFW с решениями смежных классов позволяет сформировать единый центр корпоративной защиты, где каждое средство безопасности усиливает другое. Организация получает не просто набор разрозненных инструментов, а согласованную систему, способную эффективно противостоять современным угрозам.

Kaspersky NGFW

Узнать больше

www.kaspersky.ru

#kaspersky
#активируйбудущее