
Решения
для бизнеса
kaspersky
АКТИВИРУЙ
БУДУЩЕЕ

Содержание

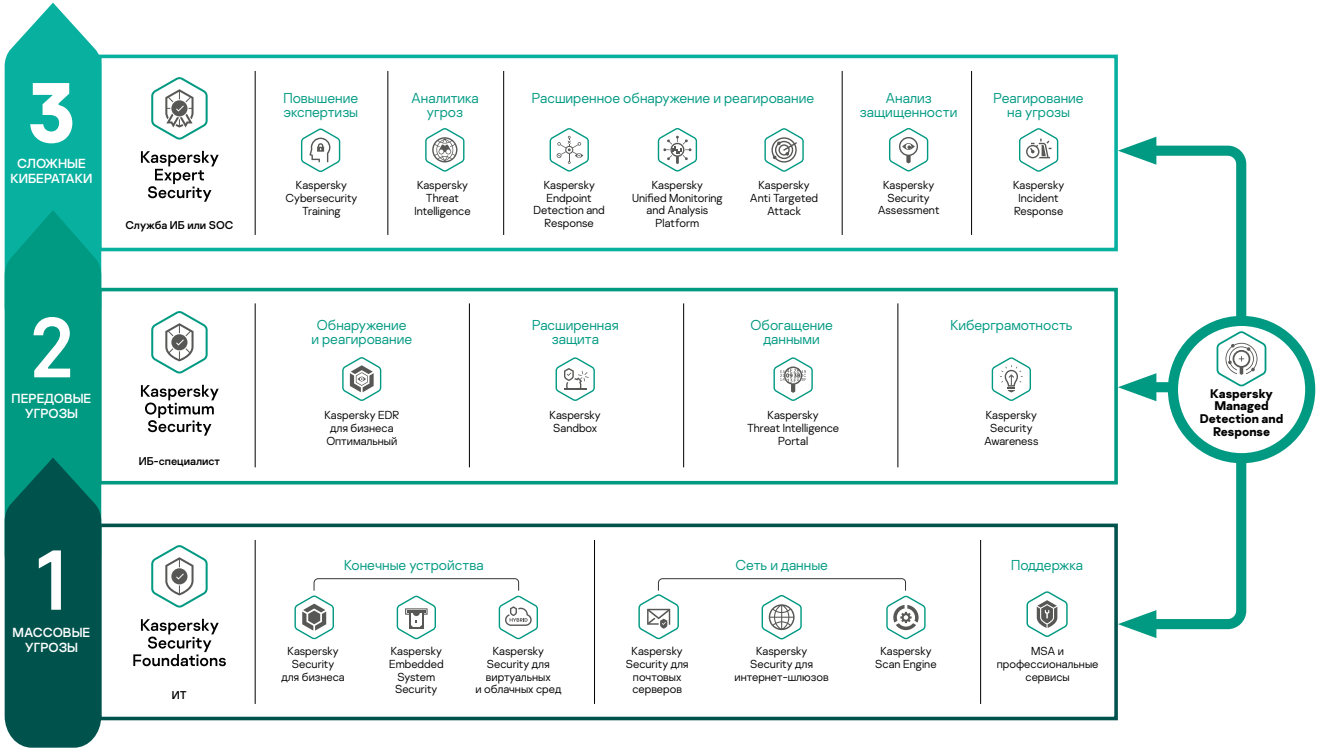
Стратегический партнер по кибербезопасности

Выбор партнера в области кибербезопасности – важный шаг для компаний, которые хотят сохранить стабильность и устойчивость в любых условиях. «Лаборатория Касперского» готова стать вашим стратегическим партнером и обеспечить защиту от угроз любой сложности, нацеленных на ваш бизнес.

- **Глобальный охват и международное признание**
- **Опыт и знания мирового уровня**
- **Доказанная эффективность технологий**
- **Высокий статус в индустрии ИБ**
- **Прозрачность и соответствие стандартам**
- **25 лет безупречной работы**

Виды угроз и уровень экспертизы

Ступенчатый подход к кибербезопасности



Комплексная безопасность бизнеса — Kaspersky Symphony

Комплексная безопасность промышленности — Kaspersky Industrial CyberSecurity

Уровень
1
Защита от массовых угроз

Kaspersky Security Foundations

Kaspersky Security для бизнеса

Линейка продуктов Kaspersky Security для бизнеса защищает вашу организацию от угроз всех типов, в том числе от шифровальщиков и бесфайловых атак. Благодаря большому числу продуктов, входящему в линейку, каждая организация может выбрать подходящий для себя уровень защиты и легко перейти на следующий уровень по мере роста и развития компании и процессов информационной безопасности.

Это сертифицированное решение, которое объединяет под одной лицензией приложения для защиты различных сред и платформ.

Это решение идеально подойдет вам, чтобы:

- организовать комплексную защиту инфраструктуру от распространенных и массовых киберугроз
- иметь в своем распоряжении гибкие инструменты контроля конечных точек

Преимущества для бизнеса

- Снижение совокупной стоимости владения за счет автоматической защиты от киберугроз
- Поддержание непрерывности бизнеса – защита всех рабочих устройств, включая мобильные, где бы они ни находились
- Обеспечение соответствия нормативным требованиям и гибкие возможности аутсорсинга для управления IT-безопасностью

Практическое применение

- Своевременная установка необходимых исправлений и управление системой защиты из облачной или локальной консоли
- Быстрый и удобный переход со сторонних решений
- Органичная интеграция технологий расширенной защиты, включая базовый EDR и песочницу, без необходимости повторной установки

Сравнение уровней Kaspersky Security для бизнеса

Возможности	Kaspersky Endpoint Security для бизнеса Стандартный	Kaspersky Endpoint Security для бизнеса Расширенный	Kaspersky EDR для бизнеса Оптимальный	Kaspersky Total Security для бизнеса	Kaspersky Total Security Plus для бизнеса
Защита от вредоносного ПО	+	+	+	+	+
Контроль устройств, программ и использования интернета	+	+	+	+	+
Единая консоль управления	+	+	+	+	+
Контроль запуска приложений на серверах		+	+	+	+
Адаптивный контроль аномалий		+	+	+	+
Инструменты системного администрирования		+	+	+	+
Встроенное шифрование		+	+	+	+
Патч-менеджмент		+	+	+	+
Инструменты EDR			+		+
Защита почтовых серверов				+	+
Защита интернет-шлюзов				+	+
Песочница					+
Расширенная техническая поддержка					+

Kaspersky Security для почтовых серверов

Kaspersky Security для почтовых серверов предотвращает угрозы, распространяемые по электронной почте, не позволяя вирусам, шифровальщикам, фишинговым письмам и спаму достигнуть рабочего места, поскольку человеческий фактор делает его наиболее уязвимым, особенно если мошенники применяют социальную инженерию. Решение показывает высокий уровень обнаружения угроз и низкое количество ложных срабатываний. Это позволяет эффективно противостоять изощренным атакам по электронной почте.

Это решение идеально подойдет вам, чтобы:

- усилить свою защиту как против массовых, так и против целевых атак, в которых электронная почта используется для доставки вредоносного ПО
- реализовать различные сценарии защиты электронной почты для различных платформ и схем развертывания

Преимущества для бизнеса

- Уменьшение ущерба от атак с использованием социальной инженерии
- Повышение производительности труда благодаря блокированию спама, отвлекающего сотрудников
- Снижение нагрузки на IT- и ИБ-специалистов и сокращение операционных затрат

Практическое применение

- Защита инфраструктуры усиливается уже на уровне почтового сервера
- Защита почтового сервера усиливается без увеличения количества ложных срабатываний
- Ваши системы обнаружения сложных угроз получают дополнительные данные и возможности

Kaspersky Security для интернет-шлюзов

Решение Kaspersky Security для интернет-шлюзов, в основе которого лежит приложение Kaspersky Web Traffic Security, обеспечивает надежную защиту на уровне шлюзов от множества веб-угроз, включая вредоносное ПО, шифровальщики, криптомайнеры, онлайн-фишинг и вредоносные веб-ресурсы. Также оно позволяет контролировать доступ к интернету, ограничивая доступ к определенным веб-ресурсам в соответствии с корпоративной политикой и запрещая передавать файлы определенных типов.

Это решение идеально подойдет вам, чтобы:

- защитить ваши рабочие места от веб-угроз
- снизить риск заражения и повысить производительность труда сотрудников
- уменьшить нагрузку на ваших IT- и ИБ-специалистов благодаря автоматическому блокированию веб-угроз

Преимущества для бизнеса

- Минимизация количества простоев и влияния внутрисетевых инцидентов безопасности на работу
- Защита вашей организации от угроз, основанных на социальной инженерии
- Повышение производительности труда сотрудников благодаря контролю доступа к веб-ресурсам

Практическое применение

- Усиление защиты ваших рабочих мест на уровне шлюзов
- Улучшение и укрепление текущей защиты веб-шлюза без увеличения количества ложных срабатываний
- Предоставление вашим системам обнаружения сложных угроз дополнительных данных и возможностей

Kaspersky Security для виртуальных и облачных сред

Kaspersky Security для виртуальных и облачных сред упростит цифровую трансформацию и обеспечит ее безопасную реализацию в ходе виртуализации вашей компании или перемещения рабочих нагрузок в облако. Запатентованная технология Легкий агент значительно сокращает использование ресурсов гипервизора. Тесная интеграция со множеством платформ виртуализации, контейнеризации и публичными облачными службами обеспечивает наглядность процессов и контроль над всей вашей инфраструктурой.

Это решение идеально подойдет вам, чтобы:

- виртуализировать ваши рабочие нагрузки на серверах и рабочих компьютерах
- переместить ваши инфраструктуры в публичные облачные службы и обеспечивать их поддержку
- интегрировать процедуры безопасности в процессы DevOps

Преимущества для бизнеса

- Минимизация финансового и репутационного ущерба
- Оптимизация расходов на IT за счет освобождения до 30% ресурсов гипервизора
- Обеспечение соответствия основным требованиям безопасности
- Обеспечение эффективного взаимодействия между отделами IT, информационной безопасности и разработки (DevOps)
- Снижение рисков и устранение слабых мест в системе безопасности

Практическое применение

- Обеспечение прозрачности процессов, контроль ЦОД и облачных развертываний
- Защита с помощью Легкого агента для сред VMware, Citrix, Microsoft, KVM, Скала-Р и других
- Защита облачных нагрузок в AWS, Microsoft Azure, Yandex.Cloud и Google Cloud
- Обеспечение безопасности DevOps

Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security – это специализированное решение для защиты встраиваемых устройств на базе Windows и рабочих станций под управлением уже не поддерживаемых операционных систем, которые вы пока не имеете возможности обновить. Контроль приложений в решении сочетается с опциональной защитой от вредоносного ПО, защитой от сетевых угроз, контролем целостности и другими технологиями обеспечения безопасности.

Это решение идеально подойдет вам, чтобы:

- защитить банкоматы, платежные терминалы, медицинское оборудование и другие встраиваемые системы
- оптимизировать безопасность систем, в которых используется устаревшее оборудование и операционные системы

Преимущества для бизнеса

- Обеспечение непрерывности бизнес-процессов в тех сферах, где последствия успешной атаки могут быть очень тяжелыми
- Плавный переход на новые операционные системы – рабочие места под управлением устаревших ОС остаются под защитой
- Обеспечение соответствия нормативным требованиям

Практическое применение

- Надежная и простая защита в условиях нерегулярного обслуживания
- Предотвращение инсайдерских атак, к которым особенно уязвимы встраиваемые системы
- Защита низкопроизводительных устройств со слабым интернет-подключением

Все решения этого уровня

Kaspersky Security Foundations

Kaspersky Security для бизнеса

Kaspersky Symphony Security

Kaspersky Security для виртуальных и облачных сред

Kaspersky Embedded System Security

Kaspersky Security для почтовых серверов

Kaspersky Security для интернет-шлюзов

Kaspersky Scan Engine

Kaspersky Professional Services

- Защита физических, виртуальных и мобильных рабочих мест
- Серверная защита в гибридных средах
- Защита виртуальных рабочих столов (VDI)
- Защита встраиваемых систем и устройств с устаревшими ОС
- Защита электронной почты
- Защита прокси-серверов, веб-приложений и почтовых шлюзов
- Помощь с внедрением, настройкой и поддержкой

Уровень
2
Передовые угрозы

Kaspersky Optimum Security

Kaspersky EDR для бизнеса Оптимальный

Kaspersky EDR для бизнеса Оптимальный позволяет небольшим командам ИБ эффективно противостоять передовым угрозам. Решение сочетает все возможности Kaspersky Endpoint Security для бизнеса Расширенный с базовыми возможностями EDR. Это простой в использовании набор инструментов, которые позволяют осуществить упрощенный анализ первопричин, сканирование индикаторов компрометации (IoC) и автоматизированное реагирование на инциденты.

Это решение идеально подойдет вам, чтобы:

- иметь наглядное представление об угрозах на всех ваших рабочих местах
- реагировать на угрозы в автоматическом и полуавтоматическом режиме
- экономить ресурсы вашей службы ИБ

Преимущества для бизнеса

- Минимизация финансовых и репутационных рисков за счет обнаружения угроз, обходящих превентивную защиту
- Оптимизация рабочей нагрузки специалистов благодаря автоматизации
- Простой в освоении и доступный по цене инструмент

Практическое применение

- Обзор всех уведомлений безопасности на всех рабочих местах
- Дальнейший анализ обнаруженной на хосте угрозы, позволяющий оценить ее масштаб и установить первопричину
- Установление факта атаки посредством поиска индикаторов компрометации (IoC), импортированных из сторонних источников
- Автоматическое реагирование на угрозы сразу после их обнаружения или в процессе расследования – в несколько кликов

Kaspersky Sandbox

Песочница Kaspersky Sandbox автоматически защищает вас от новых и неизвестных угроз, способных обходить используемые средства защиты для рабочих мест. Она дополняет решение Kaspersky Security для бизнеса и помогает организациям значительно повысить уровень защиты своих рабочих мест и серверов от ранее неизвестного вредоносного ПО, новых вирусов и шифровальщиков без необходимости нанимать новых ИБ-специалистов.

Это решение идеально подойдет вам, чтобы:

- укрепить защиту от маскирующихся угроз
- автоматизировать расширенное обнаружение угроз
- высвободить время специалистов по ИБ на другие приоритетные задачи

Преимущества для бизнеса

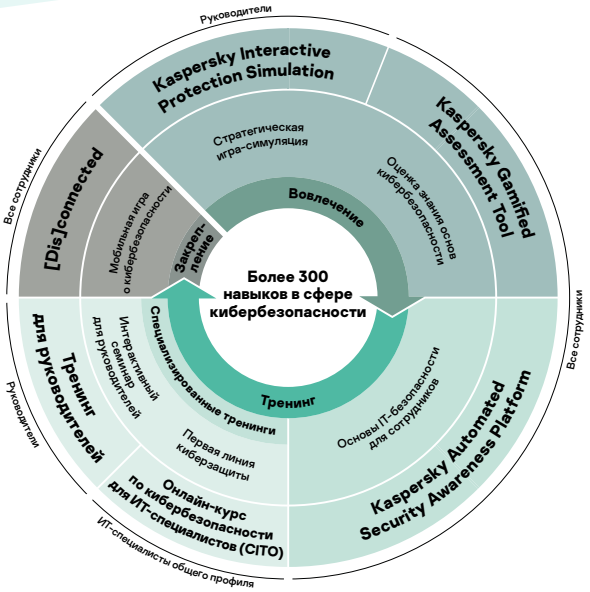
- Снижение рисков IT-безопасности и обеспечение непрерывности бизнеса
- Защита от новых и неизвестных угроз без снижения производительности рабочих мест
- Минимизация трудозатрат за счет автоматизации
- Оптимизация затрат на защиту от продвинутых угроз в удаленных офисах и филиалах

Практическое применение

- Поддержка углубленного динамического анализа и обнаружения неизвестных и маскирующихся угроз
- Автоматическое реагирование на всех защищенных рабочих местах
- Интеграция со сторонними решениями через API
- Экономия трудозатрат благодаря простоте установки и полностью автоматизированной работе

Kaspersky Security Awareness

Тренинги по безопасности Kaspersky Security Awareness помогают выработать у сотрудников навыки кибербезопасного поведения и мотивируют их применять эти навыки в повседневной работе.



Преимущества для бизнеса

- Сокращение количества инцидентов безопасности, вызванных человеческим фактором
- Обеспечение непрерывности бизнеса и минимизация ущерба от инцидентов
- Стимуляция вовлеченности и мотивации сотрудников к обучению, поддержка мер и инициатив кибербезопасности со стороны руководства
- Повышение культуры кибербезопасности

Практическое применение

- Развитие навыков на основе реальных сценариев
- Выработка правильного отношения к проблемам кибербезопасности
- Более безопасное выполнение рабочих обязанностей на всех уровнях организации

Kaspersky Automated Security Awareness Platform

Kaspersky Automated Security Awareness Platform – простой и эффективный онлайн-инструмент, помогающий постепенно формировать у сотрудников навыки в сфере кибербезопасности и мотивировать их на правильное поведение.

Онлайн-платформа является основой программы по повышению осведомленности. Она содержит тренинги для отработки более 300 навыков во всех основных областях кибербезопасности. На каждом уроке разбираются конкретные ситуации и примеры из реальной жизни, с которыми сотрудники сталкиваются в своей повседневной работе. Такой подход позволит им применять полученные навыки уже после первого урока.

Ключевые преимущества

- **Простота:** полная автоматизация, легко запустить, настроить и контролировать ход обучения
- **Эффективность:** логично построенный курс с постоянным закреплением знаний
- **Разный формат:** вы можете выбрать программу, которая лучше всего отвечает потребностям сотрудников
- **Имитация фишинговых атак:** до, во время и после прохождения курса для проверки полученных навыков
- **Гибкое лицензирование**

Все решения этого уровня

Kaspersky Optimum Security

Kaspersky EDR для бизнеса
Оптимальный

Kaspersky Managed Detection and Response
Optimum

Kaspersky Sandbox

Kaspersky Security Awareness

- Защита от передовых угроз
- Базовые инструменты EDR
- Мониторинг и поиск угроз силами экспертов «Лаборатории Касперского»
- Поведенческий анализ объектов в песочнице
- Повышение киберграмотности сотрудников

Уровень
3
Целевые атаки

Kaspersky Expert Security

Актуальные вызовы

Почему кибератаки завершаются успехом?

Недооценка угроз

Отрицание вероятности сложной атаки. Внедрение продвинутой защиты только после серьезного инцидента.

Неэффективные методы

Несистематическая обработка сложных инцидентов в сочетании с разрозненными неинтегрированными инструментами и слабой аналитикой угроз.

Отсутствие поддержки

Отсутствие стороннего партнера, способного оказать оперативную поддержку или дать экспертные рекомендации в случае инцидента.

Большой ущерб от инцидента

Kaspersky Expert Security

Kaspersky Expert Security позволяет вам взять под контроль работу с киберинцидентами и построить эффективную экосистему информационной безопасности. Мы предлагаем целостную стратегию, которая помогает оснастить, проинформировать, обучить и поддержать ваших экспертов, чтобы противостоять всему спектру современных сложных угроз, APT- и целевым атакам.

Для кого

- Для зрелых ИБ-департаментов или команд SOC
- Для организаций со сложной и распределенной инфраструктурой
- Для компаний, рискующих вследствие кибератаки понести большой ущерб

Преимущества для бизнеса

- Сокращение ущерба от сложных и целевых атак
- Сокращение операционных издержек за счет автоматизации
- Полная прозрачность корпоративной инфраструктуры
- Обеспечение помощи в соответствии нормативным требованиям

Kaspersky Expert Security

Инструменты

Обеспечим необходимыми инструментами ваших штатных ИБ-экспертов для устранения сложных инцидентов.

Информация

Проинформируем о современных угрозах и повысим квалификацию ваших ИБ-экспертов.

Поддержка

Проведем анализ защищенности, предоставим круглосуточную защиту и поможем отреагировать на инцидент.

Единая комплексная платформа XDR (Extended Detection and Response) обеспечивает полную прозрачность корпоративной инфраструктуры, осуществляет контроль популярных точек входа злоумышленников, постоянно обогащается контекстными данными о киберугрозах и автоматизирует выполнение рутинных задач по обнаружению и реагированию. Таким образом, вы будете надежно защищены от многовекторных угроз, в том числе класса APT и целевых атак.

Платформа **Kaspersky Anti Targeted Attack**, объединенная с **Kaspersky EDR**, а также решение **Kaspersky Symphony XDR** представляют собой решения класса XDR нативного и гибридного типа соответственно. С ними вы сможете контролировать и надежно защищать все точки входа потенциальных угроз: сеть, веб-трафик, электронную почту, рабочие места, серверы и виртуальные машины.

Kaspersky Anti Targeted Attack

Kaspersky Endpoint Detection and Response Expert

Kaspersky Symphony XDR

Kaspersky EDR Expert

Мощное и функциональное EDR-решение, обеспечивающее полную прозрачность, обнаружение угроз на самом высоком уровне и эффективный анализ с быстрым доступом к собранным данным. Для расследования инцидентов применяется ретроспективный анализ, проактивный поиск угроз, а также используются оперативные данные портала Kaspersky Threat Intelligence и уникальные индикаторы атаки (IoA), которые сопоставляются с данными MITRE ATT&CK. Вы сможете воссоздать всю последовательность атаки, понять принцип организации сложных атак на рабочие места и отреагировать на возникшую угрозу эффективно и быстро.

Это решение идеально подойдет вам, чтобы:

- усилить защиту ваших рабочих мест
- улучшить возможности реагирования на инциденты своими силами, сократив среднее время обнаружения и реагирования
- усилить проактивный поиск угроз

Преимущества для бизнеса

- Усиленный контроль безопасности на уровне рабочих мест
- Уменьшение киберрисков и сокращение финансовых и операционных убытков, вызванных инцидентами на рабочих местах
- Сокращение операционных издержек, связанных с IT-безопасностью
- Обеспечение соответствия нормативным требованиям

Практическое применение

- Эффективное обнаружение и быстрое реагирование на сложные атаки на уровне рабочих мест
- Ретроспективный анализ и эффективное расследование собранных данных
- Централизация управления инцидентами за счет контролируемого расследования и реагирования
- Использование возможностей автоматизированного и проактивного поиска угроз для обнаружения скрытых угроз

Платформа Kaspersky Anti Targeted Attack

Платформа Kaspersky Anti Targeted Attack – это решение класса XDR нативного типа, предназначенное для обнаружения сложных угроз, включая целевые и APT-атаки, на уровне сети и рабочих мест. Специалисты по IT-безопасности получают в едином решении все инструменты, которые позволяют выявлять угрозы на всех уровнях развития целевой атаки, проводить эффективные расследования и проактивный поиск угроз, а также оперативно и централизованно реагировать на инциденты.

Это решение идеально подойдет вам, чтобы:

- внедрить единую надежную систему защиты корпоративной инфраструктуры от сложных угроз и целевых атак
- снизить нагрузку на службу информационной безопасности
- оптимизировать затраты на процесс расследования и реагирования на комплексные инциденты
- обеспечить соответствие требованиям регуляторов

Преимущества для бизнеса

- Уменьшение киберрисков и сокращение финансовых и операционных убытков, вызванных сложными целевыми атаками
- Сокращение операционных издержек, связанных с IT-безопасностью
- Повышение продуктивности и качества работы сотрудников служб ИТ и ИБ

Практическое применение

- Защита различных потенциальных точек проникновения угроз на уровне сети и рабочих мест
- Быстрое обнаружение продвинутых угроз, обходящих традиционные защитные технологии
- Поиск скрытых угроз с использованием возможностей автоматизированного и проактивного поиска угроз

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Unified Monitoring and Analysis Platform — это решение класса SIEM, предназначенное для централизованного сбора, анализа и корреляции ИБ-событий из различных источников данных. Оно является одним из ключевых компонентов на пути к реализации единой платформы кибербезопасности. Решение обеспечивает гибкий комплексный подход к противодействию сложным угрозам и целевым атакам, помогает обеспечить соответствие требованиям внешних регулирующих органов и легко встраивается в существующую ИТ- и ИБ-инфраструктуру.

Это решение идеально подойдет, чтобы вы могли:

- построить экосистему безопасности на основе продуктов «Лаборатории Касперского»
- повысить продуктивность работы вашей службы ИБ
- соответствовать требованиям внутренних политик безопасности и внешних регулирующих органов

Преимущества для бизнеса

- Создание стратегии для борьбы со сложными и целевыми атаками
- Масштабируемая архитектура и низкие системные требования
- Высокая производительность системы поиска корреляций
- Обеспечение соответствия законодательству в сфере безопасности объектов КИИ

Практическое применение

- Инвентаризация информационных активов
- Потоковое обогащение данных
- Обогащение событий по запросу
- Интеграция «из коробки» с решениями «Лаборатории Касперского» и многими решениями других поставщиков

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Threat Intelligence

Сервисы Kaspersky Threat Intelligence предоставляют обширную, достоверную и обогащенную контекстом информацию об угрозах. Уникальные аналитические данные укрепляют вашу систему безопасности и помогают вам принимать конкретные меры. Мы предлагаем потоки данных об угрозах, отчеты по конкретным отраслям, облачную песочницу и другие сервисы с возможностью поиска по обширной базе данных.

Это решение идеально подойдет вам, чтобы:

- оптимизировать ваши возможности анализа, обнаружения и предотвращения угроз
- перейти от реактивной модели киберзащиты к проактивной
- оптимизировать принятие стратегических решений по безопасности

Преимущества для бизнеса

- Уменьшение числа рутинных операций и предотвращение выгорания ИБ-аналитиков
- Повышение операционной эффективности системы безопасности; минимизация перебоев в бизнесе и ущерба от инцидентов
- Повышение окупаемости инвестиций в IT-безопасность

Практическое применение

- Постоянное обновление защитных решений машиночитаемыми данными о киберугрозах
- Выявление критичных уведомлений и передача их в приоритетном порядке группам реагирования на инциденты
- Повышение эффективности расследований благодаря выявлению связей между обнаруженными угрозами

Kaspersky Threat Intelligence

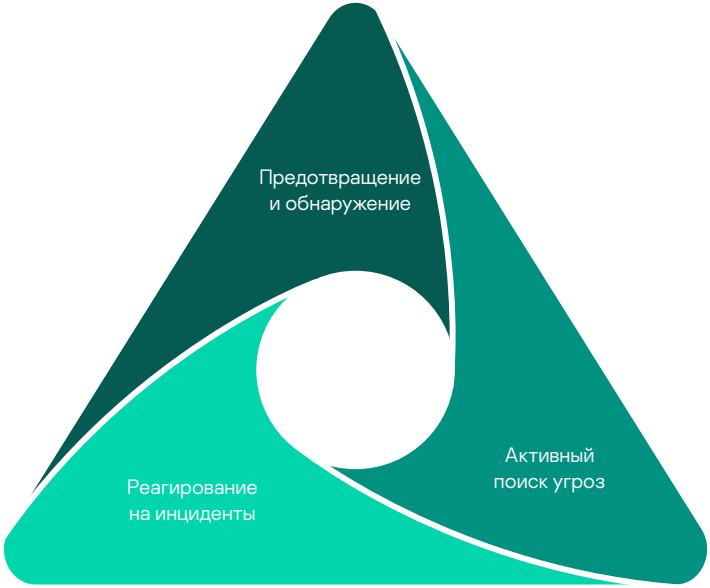
Развитие внутренней экспертизы

Ваши ИБ-специалисты могут повысить экспертизу и получить новые навыки, приняв участие в тренингах **Kaspersky Cybersecurity Training**. В ходе тренингов участники оттачивают навыки работы с цифровыми уликами, узнают, как обнаруживать и анализировать вредоносное ПО, а также как эффективно реагировать на инциденты.

- Повышение квалификации экспертов в области реагирования и цифровой криминалистики
- Профессиональное развитие и мотивация ваших экспертов
- Экономия времени и денег: вам не придется искать новых сотрудников

Kaspersky Cybersecurity Training

Поддержка ваших экспертов



Ресурсы ИБ-команд часто ограничены, и наши эксперты готовы оказать поддержку вашим специалистам, чтобы те могли сосредоточиться на других, не менее важных задачах.

С **Kaspersky Managed Detection and Response** вы можете положиться на наш опыт в области изучения угроз. Мы возьмем на себя задачи по круглосуточной управляемой защите и проактивному поиску угроз.

В случае инцидента вы можете воспользоваться сервисом **Kaspersky Incident Response**. Он охватывает полный цикл реагирования на инциденты — от сбора доказательств и раннего реагирования на инцидент до выявления дополнительных следов взлома и подготовки плана устранения последствий атаки.

Kaspersky Managed Detection and Response

Kaspersky Incident Response

Kaspersky Managed Detection and Response

Kaspersky Managed Detection and Response (MDR) предоставляет круглосуточную управляемую защиту от растущего числа киберугроз и сложных атак, которые обходят автоматические средства защиты. Сервис подходит как небольшим организациям, у которых нет ИБ-специалистов или которые испытывают нехватку знаний в вопросе реагирования на киберинциденты, так и более крупным компаниям, ИБ-эксперты которых перегружены.

Это решение идеально подойдет вам, чтобы:

- разгрузить вашу ИБ-службу, чтобы ваши специалисты могли сосредоточиться на критичных инцидентах, действительно требующих их участия
- повысить эффективность работы вашей ИБ-службы, дополнив собственные наработки многолетним экспертным опытом «Лаборатории Касперского»

Преимущества для бизнеса

- Возможность пользоваться ключевыми преимуществами SOC без затрат на его создание
- Максимальная отдача от использования решений «Лаборатории Касперского»
- Сокращение расходов на безопасность благодаря повышению уровня IT-безопасности без необходимости нанимать и обучать штатных ИБ-специалистов

Практическое применение

- Круглосуточный мониторинг
- Активный поиск угроз и расследование инцидентов
- Рекомендации по реагированию и удалённое реагирование на инциденты
- Проверка работоспособности защитных механизмов и обзор защищаемых ресурсов

Понимание уровня защищенности вашей компании

Чтобы определять текущее состояние защищенности ваших систем и эффективно реагировать на сложные инциденты, вам нужен надежный партнер с богатым опытом оказания таких услуг и обладающий глубокой экспертизой.

Воспользуйтесь сервисами **Kaspersky Security Assessment** и **Kaspersky Targeted Attack Discovery**, чтобы проверить готовность вашей системы безопасности к отражению атак и узнать, не стали ли вы уже жертвой скрытой долгосрочной атаки.

Kaspersky Security Assessment

Kaspersky Targeted Attack Discovery

Все решения этого уровня

Kaspersky Expert Security

Kaspersky Symphony XDR

Kaspersky Anti Targeted Attack

Kaspersky Endpoint Detection and Response

Kaspersky Managed Detection and Response

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Threat Intelligence

Kaspersky Incident Response

Kaspersky Security Assessment

- Защита от сложных и целевых атак
- Расширенное обнаружение угроз и реагирование на них
- Достоверные аналитические данные об угрозах
- Поддержка в процессе реагирования
- Анализ защищенности и тестирование на проникновение
- Централизованный сбор и корреляция данных
- Экосистемный подход и тесная интеграция решений
- Помощь в обеспечении соответствия требованиям регулирующих органов

Kaspersky Symphony

Kaspersky Symphony

Сложность и интенсивность угроз для бизнеса неизменно растут. Чтобы отражать актуальные угрозы и успешно противодействовать сложным кибератакам, необходим комплексный, системный подход к построению защиты бизнеса.

Kaspersky Symphony — это линейка решений, которая даёт организациям всё необходимое для постепенной или одночастной реализации этого подхода и построения надежной и адаптивной системы кибербезопасности. Все элементы этой экосистемы дополняют и усиливают друг друга.

Состав Kaspersky Symphony

Базовая защита

Kaspersky Symphony Security: мощная защита рабочих мест – как физических, так и виртуальных.

Продвинутая защита

Расширенные возможности в области противодействия сложным угрозам на основе собственной экспертизы (Kaspersky Symphony EDR) или с помощью внешних экспертов (Kaspersky Symphony MDR).

Всесторонняя защита

Kaspersky Symphony XDR обеспечивает надежную защиту от кибератак и помогает соответствовать требованиям законодательства, в том числе благодаря встроенному модулю ГосСОПКА.

Всеобъемлющий подход к защите бизнеса для компаний, которые стремятся быть первыми и делают шаг в безопасное будущее.

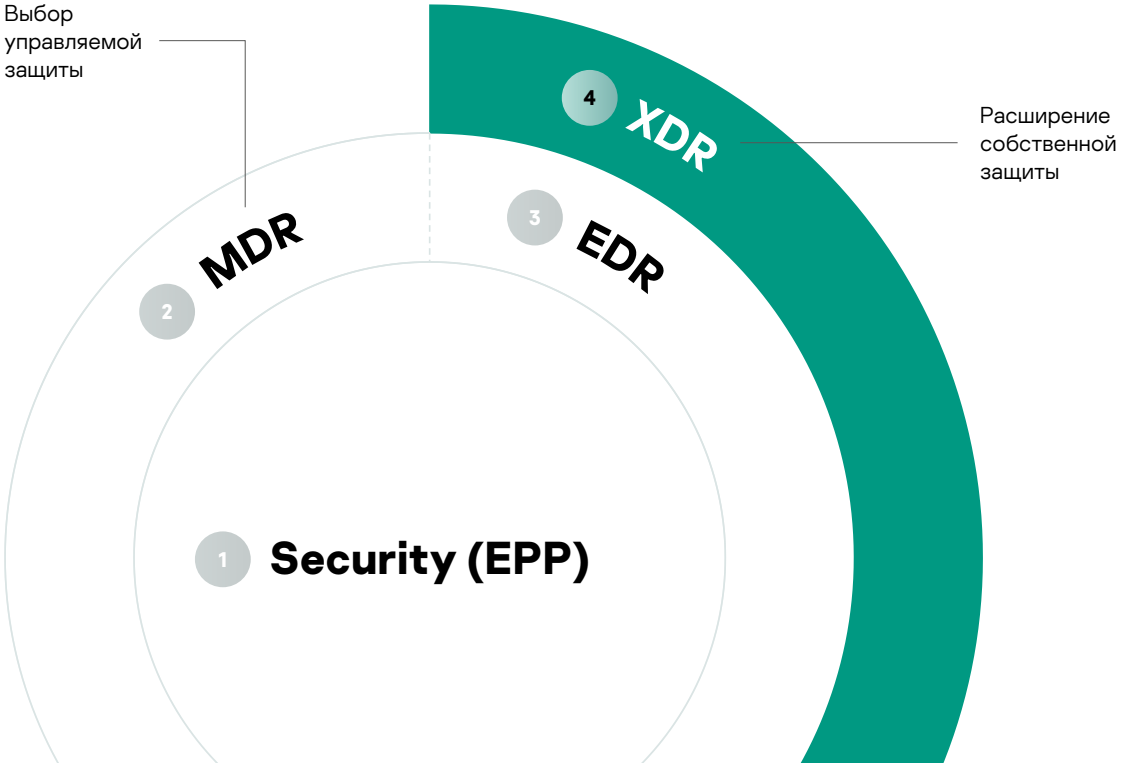
Функциональное сравнение уровней Kaspersky Symphony

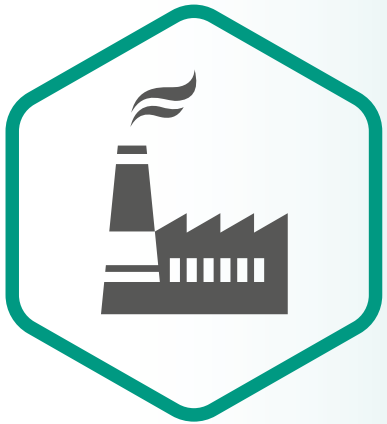
Kaspersky Symphony — это гибкая линейка решений для компаний с разными потребностями в области информационной безопасности. Вы можете выбрать то решение, которое лучше всего отвечает вашим задачам, а затем масштабировать защиту, перейдя на другой уровень.

Kaspersky Symphony	Security	EDR	MDR	XDR
Уровень защиты	Базовая собственная защита	Передовая собственная защита	Передовая управляемая защита	Расширенная собственная защита
Автоматическая защита конечных точек (физических, мобильных и виртуальных) от массовых угроз	●	●	●	●
Передовое обнаружение сложных угроз на уровне конечных точек и реагирование на них		●	●	●
Защита электронной почты и анализ сетевого трафика				●
Комплексный мониторинг и корреляция событий ИБ (+ модуль ГосСОПКА)				●
Управление аналитическими данными о киберугрозах				●
Повышение киберграмотности				●

Гибкий выбор

Подберите уровень защиты, который подходит вашему бизнесу





Kaspersky Industrial CyberSecurity

Комплексная кибербезопасность промышленных предприятий и объектов критической инфраструктуры

Kaspersky Industrial CyberSecurity

Ответ на актуальные вызовы в области промышленной кибербезопасности

Устойчивое развитие промышленных предприятий и объектов критической инфраструктуры напрямую зависит от стабильности производственных и бизнес-процессов, надежной защиты важных активов и безопасности операционной (OT) и IT-инфраструктуры. Постоянный рост количества и увеличение сложности киберугроз в эпоху четвертой промышленной революции, глобализация информационной среды и необходимость соответствия требованиям регулирующих органов — все это побуждает организации задуматься о комплексном подходе к обеспечению кибербезопасности.

Тренды промышленной кибербезопасности:

- **Увеличение количества точек входа злоумышленников в инфраструктуру, которая находится на стыке OT- и IT-сред**
- **Усиление регуляторных требований в отношении защиты КИИ**
- **Рост количества атакованных компьютеров АСУ**
- **Основные источники угроз для компьютеров в технологической инфраструктуре — интернет, съемные носители и электронная почта**

Экосистема решений для промышленной безопасности

Kaspersky Industrial CyberSecurity

- Kaspersky Industrial Cybersecurity for Nodes
- Kaspersky Industrial Cybersecurity for Networks
- Kaspersky Security CAD
- Kaspersky Machine Learning for Anomaly Detection
- Kaspersky ICS Threat Intelligence
- Kaspersky IoT Secure Gateway
- Kaspersky ICS CERT Services
- Kaspersky Unified Monitoring and Analysis Platform

- Защита рабочих станций в рамках промышленной сети
- Анализ трафика на уровне промышленных протоколов
- Обнаружение отклонений в технологическом процессе
- Цифровое моделирование системы ИБ
- Мониторинг и защита систем интернета вещей
- Информирование об угрозах для АСУ ТП
- Экспертные сервисы

Международное признание

«Лаборатория Касперского» активно участвует в независимых тестированиях и взаимодействует с ведущими аналитическими агентствами. Наши технологии и продукты признаны во всем мире и удостоены многочисленных международных наград.

Доказанная эффективность наших технологий и экспертных знаний

БОЛЬШЕ ТЕСТОВ
БОЛЬШЕ НАГРАД
БОЛЬШЕ ЗАЩИТЫ
*kaspersky.ru/top3

«Лаборатория Касперского» признана победителем в категории Endpoint Protection Platforms в 2021 году по версии Gartner Peer Insights Customers' Choice

MITRE | ATT&CK®

Качество обнаружения угроз подтверждено оценкой MITRE ATT&CK

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

Исследовательская компания Radicati Group назвала «Лабораторию Касперского» ведущим игроком (Top Player) в отчете APT Protection Market Quadrant 2022

GREAT GLOBAL RESEARCH & ANALYSIS TEAM

В решениях заложены знания о масштабных APT-атаках, полученные Глобальным центром исследования и анализа угроз «Лаборатории Касперского» (GReAT)

FORRESTER®

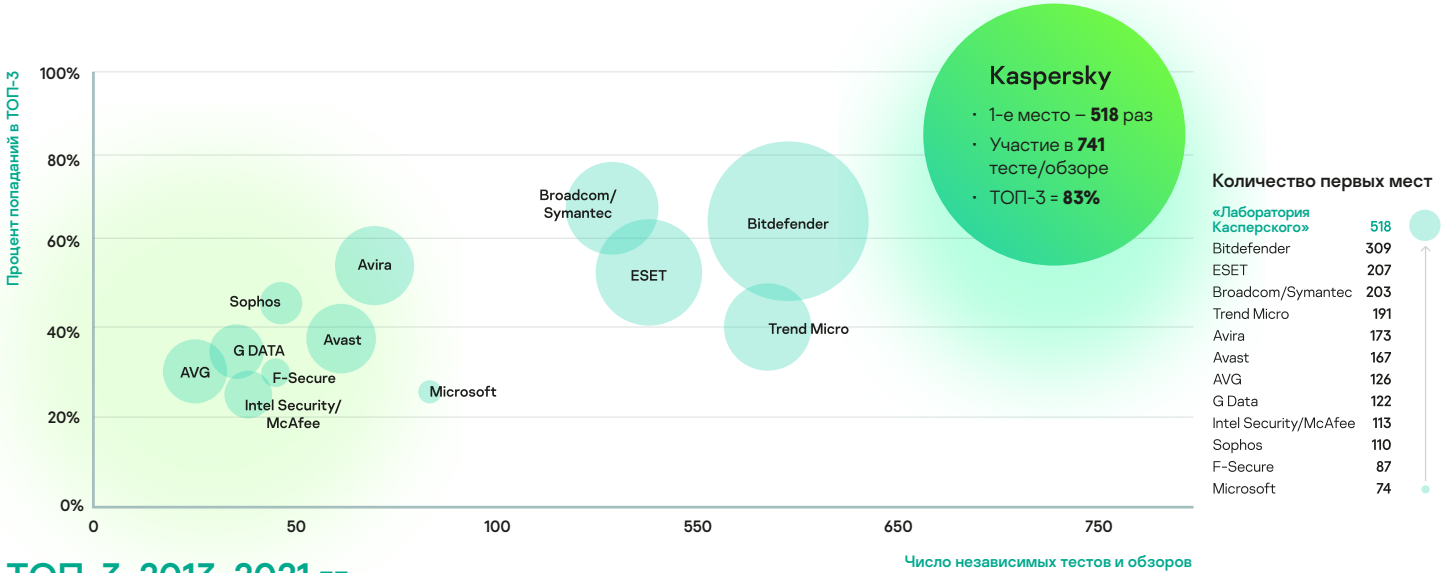
«Лаборатория Касперского» признана лидером по результатам исследования Forrester Wave: External Threat Intelligence Services (Внешние услуги по анализу угроз), 2021

Больше тестов. Больше наград. Больше защиты.*

С 2013 по 2021 год продукты «Лаборатории Касперского» приняли участие в 741 независимом тесте/обзоре. В 518 случаях они заняли первое место.

БОЛЬШЕ ТЕСТОВ
БОЛЬШЕ НАГРАД
БОЛЬШЕ ЗАЩИТЫ
*kaspersky.ru/top3

Подробнее о методике:
kaspersky.ru/top3



ТОП-3, 2013-2021 гг.

Цифры говорят больше слов

>400 млн

пользователей используют наши защитные решения

>240 тыс.

компаний по всему миру мы оберегаем от киберугроз

>$10 трлн

сумма бизнес-активов, защиту которых мы обеспечиваем

>380 тыс.

уникальных вредоносных объектов мы обнаруживаем ежедневно

>650 млн

кибератак было остановлено нашими решениями в 2021 году

>$3,5 трлн

заработали организации под нашей защитой за 2021 год

Подробнее о продуктах и сервисах «Лаборатории Касперского»:

для среднего и малого бизнеса – kaspersky.ru/business

для крупного бизнеса – kaspersky.ru/enterprise

www.kaspersky.ru

kaspersky