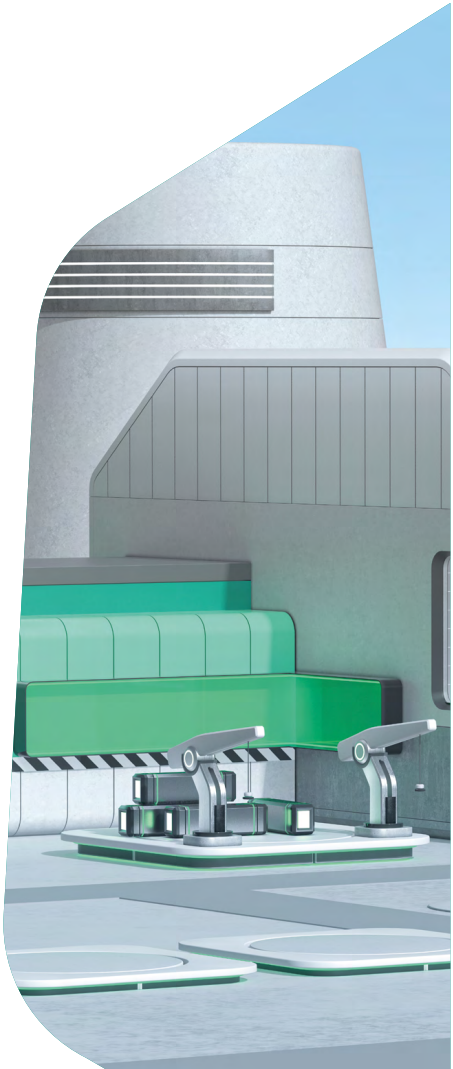
kaspersky

Решения для бизнеса

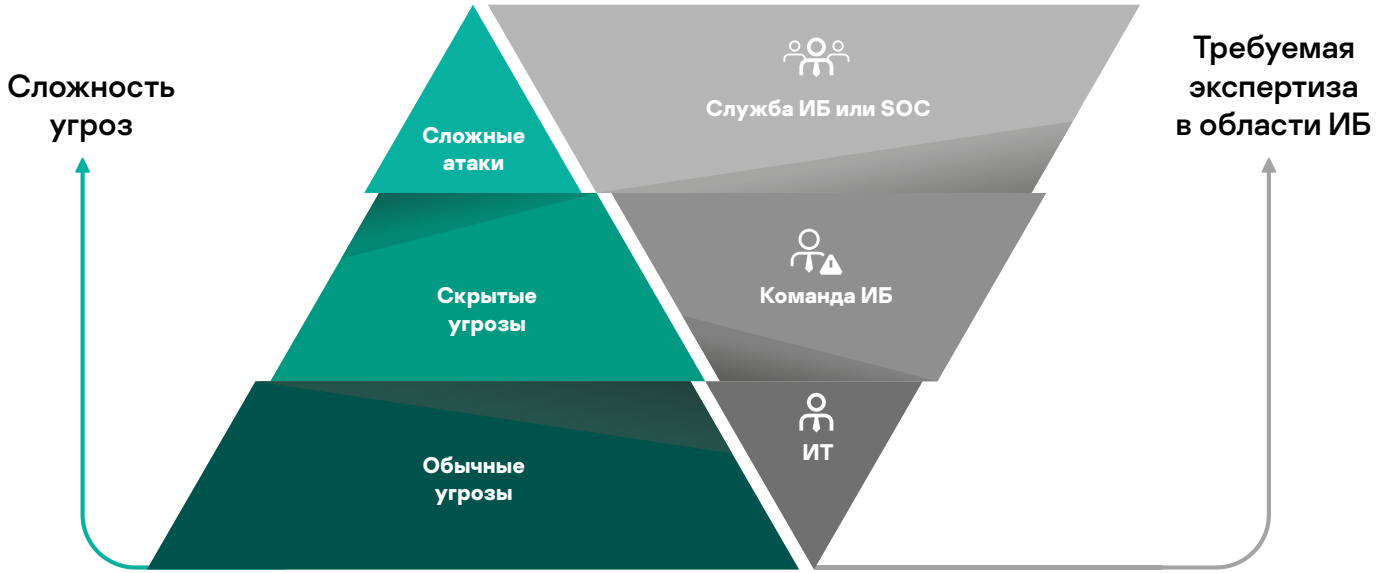
Содержание

Решения «Лаборатории Касперского» для защиты бизнеса

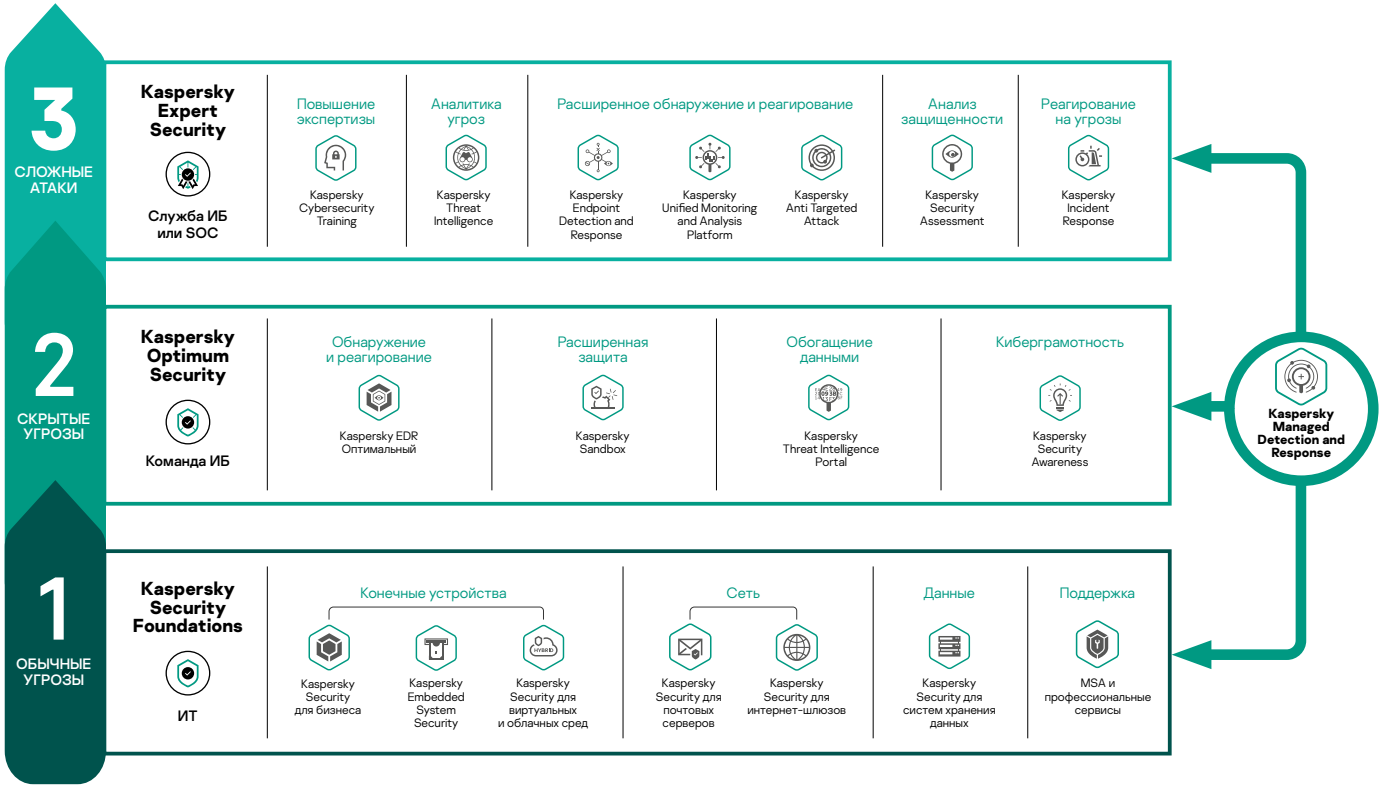
Выбор подходящего продукта или сервиса для обеспечения безопасности вашей организации – лишь самый первый шаг. Для устойчивого развития вашего бизнеса важнее всего разработать продуманную стратегию в области защиты от киберугроз. Решения «Лаборатории Касперского» удовлетворяют потребности современного бизнеса в киберзащите вне зависимости от уровня зрелости организации в области информационной безопасности. Благодаря ступенчатому подходу, включающему различные уровни решений, вы сможете создать долгосрочную стратегию обеспечения безопасности, чтобы эффективно реагировать на атаки любой сложности и предотвращать будущие угрозы.



Виды угроз и уровень экспертизы



Ступенчатый подход к кибербезопасности



Уровень 1
Kaspersky Security Foundations

Основа системы безопасности для компаний любого масштаба и сложности – на этом уровне автоматически отражаются массовые киберугрозы.

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 решение идеально подойдет вам, чтобы:

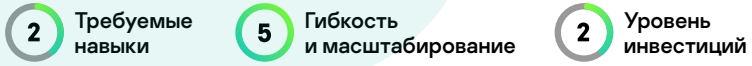
- комплексно защитить инфраструктуру от распространенных киберугроз
- иметь в распоряжении гибкие инструменты контроля конечных точек
- использовать сертифицированное решение, которое объединяет под одной лицензией приложения для защиты различных сред и платформ

Преимущества для бизнеса

- Снижение совокупной стоимости владения за счет автоматизации 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 Endpoint Security для бизнеса Универсальный	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 виртуальных сред				+		
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 попасть на рабочие места, которые из-за человеческого фактора наиболее уязвимы к вредоносному ПО и мошенничеству на основе социальной инженерии. Решение сочетает 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 целевых атак, использующих электронную почту 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

- Усиление безопасности инфраструктуры на уровне почтового сервера
- Усиление защиты почтового сервера без увеличения количества ложных срабатываний
- Предоставление вашим системам обнаружения сложных угроз дополнительных данных и возможностей

Требуемые навыки

Гибкость и масштабирование

Уровень инвестиций

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:

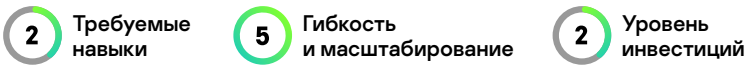
- защитить ваши рабочие места от веб-угроз
- снизить риск заражения и повысить производительность труда сотрудников
- уменьшить нагрузку на ваших IT- и ИБ-специалистов благодаря автоматическому блокированию веб-угроз

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 организации 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 инфраструктуры в публичные облачные службы и обеспечивать их поддержку
- интегрировать процедуры безопасности в процессы DevOps

2 Требуемые навыки

5 Гибкость и масштабирование

2 Уровень инвестиций

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 используются устаревшие 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

2 Требуемые навыки

5 Гибкость и масштабирование

2 Уровень инвестиций

Расширенная техническая поддержка (MSA)

При возникновении инцидента безопасности самое важное – это время, требуемое для выявления причины инцидента и её устранения. Предлагаемые нами программы расширенной технической поддержки специально разработаны, чтобы помочь вам быстро вернуться к привычной работе. Круглосуточный доступ к помощи экспертов, грамотная приоритизация инцидентов, фиксированное время отклика – все, что нужно для оперативного решения ваших задач.

Это решение идеально подойдет вам, чтобы:

- быть уверенными в том, что ваша IT-инфраструктура находится под защитой передовых технологий
- получить доступ к знаниям и опыту экспертов мирового уровня

Преимущества для бизнеса

- Обеспечение непрерывности бизнеса в режиме 24/7
- Ускоренное решение задач, благодаря доступу к приоритетной выделенной линии техподдержки
- Предоставление персонального менеджера по техническим вопросам

Практическое применение

- Быстрая передача критичных проблем профильным специалистам
- Проактивные меры защиты, адаптированные под вашу компанию
- Экономия времени, затрачиваемого на техобслуживание и устранение неполадок

1 Требуемые навыки

5 Гибкость и масштабирование

3 Уровень инвестиций

Профессиональные сервисы «Лаборатории Касперского»

Безопасность стоит немало. Не дайте вложениям пропасть зря: заручитесь поддержкой экспертов, которые помогут оптимизировать инвестиции исходя из потребностей вашей организации. Наши специалисты применяют методы, доказавшие свою эффективность за годы практики, чтобы помочь вам во всех аспектах развертывания, настройки и обновления продуктов «Лаборатории Касперского».

Это решение идеально подойдет вам, чтобы:

- ускорить развертывание защитных продуктов;
- оптимизировать и персонализировать используемое вами решение «Лаборатории Касперского»

Преимущества для бизнеса

- Высокая рентабельность ваших инвестиций в защитные решения
- Сокращение расходов на штатных IT-специалистов
- Сокращение расходов на внедрение нового защитного решения
- Уверенность в том, что любой критичный инцидент будет рассмотрен максимально быстро

Практическое применение

- Снижение вероятности возникновения проблем при внедрении
- Снижение рисков простоев благодаря регулярным аудитам конфигурации продуктов

1 Требуемые навыки

5 Гибкость и масштабирование

3 Уровень инвестиций

Kaspersky Security для систем хранения данных

Kaspersky Security для систем хранения данных защитит ваши корпоративные данные и предотвратит распространение заражения вредоносным ПО благодаря набору мощных технологий, основанных на глобальной аналитике угроз. К ним, например, относится удаленный Анти-Криптор, реализованный благодаря интеграции с API систем хранения данных.

Это решение идеально подойдет вам, чтобы:

- защитить ваши хранилища данных от внешних атак и распространения вредоносного ПО
- обезопасить ценные данные от атак шифровальщиков

Преимущества для бизнеса

- Поддержание непрерывности бизнеса
- Обеспечение соответствия требованиям регулирующих органов
- Экономия времени и ресурсов ваших специалистов благодаря единой консоли

Практическое применение

- Защита систем хранения данных NAS, DAS, SAN или любого их сочетания в вашей инфраструктуре
- Защита как хранилищ данных, так и сервера, используемого для размещения защитного решения
- Предотвращение потерь данных вследствие атак шифровальщиков

Требуемые навыки

Гибкость и масштабирование

Уровень инвестиций

Уровень 2
Kaspersky Optimum Security

Оптимальный уровень для компаний с собственной службой ИБ. Позволяет обнаруживать и блокировать угрозы, обходящие традиционные средства защиты.

Kaspersky EDR для бизнеса Оптимальный

Kaspersky EDR для бизнеса Оптимальный позволяет небольшим службам ИБ эффективно противостоять уклоняющимся от обнаружения угрозам. Решение сочетает все возможности Kaspersky Endpoint Security для бизнеса Расширенный с базовыми инструментами EDR. Это простой в использовании набор инструментов, основанных на упрощенном анализе первопричин, сканировании индикаторов компрометации (IoC) и автоматизированных возможностях реагирования.

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

3 Требуемые навыки

4 Гибкость и масштабирование

3 Уровень инвестиций

Преимущества для бизнеса

- Минимизация финансовых и репутационных рисков за счет блокирования 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 Managed Detection and Response Optimum

Благодаря быстрому развертыванию решение Kaspersky Managed Detection and Response Optimum позволяет активировать передовые функции защиты без необходимости нанимать дополнительных сотрудников и обучать существующих. Запатентованные модели машинного обучения, постоянный доступ к аналитическим данным об угрозах и автоматизированный активный поиск угроз с помощью уникальных индикаторов атаки (IoA) – все это залог того, что ваша организация будет находиться под непрерывной защитой от сложных угроз.

Это решение идеально подойдет вам, чтобы:

- создать и усовершенствовать систему эффективного раннего обнаружения и реагирования с круглосуточным мониторингом
- быстро снизить уровень уязвимости вашей компании к продвинутым угрозам

2 Требуемые навыки

5 Гибкость и масштабирование

4 Уровень инвестиций

Преимущества для бизнеса

- Уверенность в том, что вы находитесь под постоянной защитой даже от самых сложных и изощренных угроз
- Сокращение расходов на безопасность из-за отсутствия необходимости нанимать новых ИБ-специалистов и обучать собственных

Практическое применение

- Реализация системного подхода к безопасности за счет автоматического предотвращения, обнаружения, активного поиска и реагирования на угрозы для ваших сетей
- Быстрое реагирование на инциденты безопасности с сохранением полного контроля над принимаемыми мерами
- Полный обзор в режиме реального времени всех обнаруженных угроз, защищаемых активов и текущего состояния защиты

Kaspersky Sandbox

Песочница Kaspersky Sandbox автоматически защищает вас от новых и неизвестных угроз, способных обходить используемые средства безопасности 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

1 Требуемые навыки

3 Гибкость и масштабирование

2 Уровень инвестиций

Kaspersky Threat Intelligence Portal

Портал Kaspersky Threat Intelligence – это все накопленные нами знания о киберугрозах, собранные в едином веб-сервисе. Он позволяет проверять подозрительные индикаторы угроз, будь то файлы, хеш-суммы файлов, IP- или URL-адреса. Портал анализирует объекты с помощью технологий детектирования сложных угроз, таких как обнаружение на основе репутационных данных, модели анализа структур на основе машинного обучения и расширенное динамическое обнаружение средствами облачной песочницы «Лаборатории Касперского». По результатам анализа объект классифицируется как безопасный, вредоносный или без категории. Предоставляемые контекстные данные позволяют приоритизировать угрозы и более эффективно реагировать на них.

Это решение идеально подойдет вам, чтобы:

- получить бесплатный доступ к надежному источнику аналитических данных об угрозах
- эффективнее приоритизировать инциденты
- ускорить расследование и анализ угроз

Преимущества для бизнеса

- Возможность избежать высоких расходов при использовании коммерческих источников аналитических данных об угрозах
- Обеспечение эффективной защиты ваших сетей благодаря быстрому доступу к достоверным данным

Практическое применение

- Валидация и приоритизация уведомлений
- Немедленное выявление критических важных оповещений
- Отделение реальных угроз от ложных срабатываний
- Простой поиск в базе данных
- Обнаружение ранее пропущенных угроз

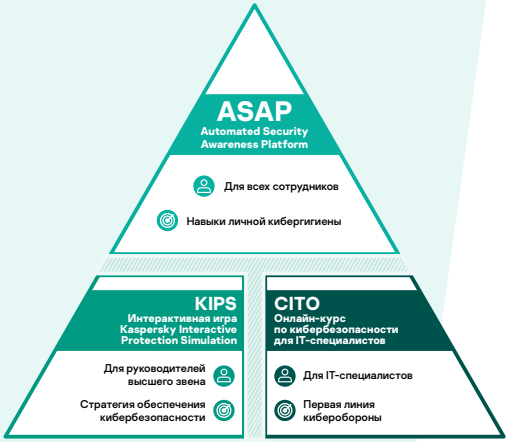
3 Требуемые навыки

4 Гибкость и масштабирование

0 Уровень инвестиций

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.



2 **Требуемые навыки**

4 **Гибкость и масштабирование**

3 **Уровень инвестиций**

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

Уровень 3
Kaspersky Expert Security

Расширенная защита от передовых угроз, централизованный сбор данных, уникальная аналитика угроз и экспертные сервисы – всё это позволяет опытным ИБ-службам противостоять сложным угрозам и целевым атакам.

Единая платформа безопасности

Kaspersky Expert Security позволяет вам взять под контроль сложные угрозы и построить эффективную экосистему информационной безопасности. Мы предлагаем интегрированные между собой продукты для противодействия сложным атакам, экспертную поддержку и тренинги для повышения квалификации ваших ИБ-специалистов.

Это решение идеально подойдет вам, чтобы:

- создать свою экосистему на базе продуктов «Лаборатории Касперского»
- выстроить стратегию обеспечения безопасности, устойчивую к новым угрозам
- соответствовать требованиям регулирующих органов
- вооружить ваших экспертов всем необходимым для борьбы со сложными угрозами

Преимущества для бизнеса

- Полная интеграция продуктов «Лаборатории Касперского», что упрощает управление и снижает стоимость владения
- Устойчивость к новым и сложным угрозам и целевым атакам
- Поддержка на всех этапах внедрения экосистемы

Практическое применение

- Обнаружение сложных и целевых атак
- Повышение экспертизы ИБ-специалистов
- Автоматизация рутинных задач по расследованию инцидентов
- Минимизация количества ложноположительных срабатываний
- Управление из единой консоли

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 готово встроиться в существующую ИТ- и ИБ-инфраструктуру.

Это решение идеально подойдет вам, чтобы:

- 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 Endpoint Detection and Response

Мощное и функциональное EDR-решение, обеспечивающее полную прозрачность, обнаружение угроз на самом высоком уровне и эффективный анализ с быстрым доступом к собранным данным. Расследование инцидентов осуществляется на базе ретроспективного анализа, уникальных индикаторов атаки (IoA) и сопоставления с данными MITRE ATT&CK, а также за счет проактивного поиска угроз и благодаря оперативным данным портала Kaspersky Threat Intelligence. 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

4 Требуемые навыки

3 Гибкость и масштабирование

4 Уровень инвестиций

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 продвинутые атаки на уровне рабочих мест
- Ретроспективный анализ и эффективное расследование собранных данных
- Централизация управления инцидентами за счет контролируемого расследования и реагирования
- Поиск скрытых угроз с использованием возможностей автоматизированного и проактивного поиска угроз

Платформа Kaspersky Anti Targeted Attack

Платформа Kaspersky Anti Targeted Attack объединяет возможности обнаружения продвинутых угроз на уровне сети и технологии EDR. 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

Требуемые навыки

Гибкость и масштабирование

Уровень инвестиций

Managed Detection and Response Expert

Решение Kaspersky Managed Detection and Response Expert позволяет делегировать «Лаборатории Касперского» сложные и ресурсоемкие процессы расследования и анализа инцидентов. Вы получаете всё, что содержит уровень Kaspersky MDR Optimum, но при этом вам доступны и новые возможности: активный поиск угроз силами экспертов «Лаборатории Касперского» и возможность с ними консультироваться, хранение необработанных данных до 3 месяцев, API, упрощающее интеграцию с другими системами.

Это решение идеально подойдет вам, чтобы:

- разгрузить вашу опытную 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»

2 Требуемые навыки

5 Гибкость и масштабирование

5 Уровень инвестиций

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

- Обзор всех защищаемых активов с их текущим статусом в реальном времени
- Сбор улик на хостах и сетевых системах, позволяющих выявить первопричину инцидента и избежать аналогичных инцидентов в будущем
- Организация масштабируемых, быстрых и эффективных процедур реагирования

Kaspersky Threat Intelligence

Сервисы Kaspersky Threat Intelligence предоставляют обширную, достоверную и обогащенную контекстом информацию об угрозах. Уникальные аналитические данные, помогают принимать конкретные меры и готовы к интеграции с вашими процессами безопасности. 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
- Приоритизация уведомлений за счет выявления критичных уведомлений, требующих передачи группам реагирования на инциденты
- Повышение эффективности расследований с участием аналитиков за счет выявления связей между обнаруженными угрозами

4 Требуемые навыки

5 Гибкость и масштабирование

5 Уровень инвестиций

Kaspersky Cybersecurity Training

Киберугрозы постоянно развиваются, поэтому ИБ-специалисты должны постоянно повышать свою экспертизу и овладевать новыми знаниями и навыками. Среди них – обратная разработка вредоносного ПО, реагирование на инциденты, применение правил YARA и работа с цифровыми уликами. Тренинги по кибербезопасности «Лаборатории Касперского» помогут вооружить ваших ИБ-экспертов нужными знаниями для борьбы с постоянно эволюционирующими угрозами.

Это решение идеально подойдет вам, чтобы:

- повысить квалификацию ваших штатных ИБ-специалистов
- сделать более эффективной работу вашего SOC
- развить возможности внутреннего исследования угроз

Преимущества для бизнеса

- Повышение квалификации специалистов SOC позволит сократить ущерб от инцидентов
- Экономия времени и средств на поиск нужных специалистов
- Развитие и мотивация своих сотрудников

Практическое применение

- Оптимизация реагирования на инциденты благодаря анализу вредоносного ПО
- Сбор улик на хостах и сетевых системах, позволяющих выявить первопричину инцидента
- Организация масштабируемых, быстрых и эффективных процедур в области ИБ

4 Требуемые навыки

3 Гибкость и масштабирование

4 Уровень инвестиций

Сервисы кибербезопасности «Лаборатории Касперского»

Сервисы кибербезопасности «Лаборатории Касперского» открывают доступ ко всему арсеналу знаний и накопленному опыту наших экспертов реагирования на инциденты. Информация об уже случившихся и новейших атаках, а также оценка безопасности всей организации с учетом отраслевой специфики помогут вам устранить бреши в защите еще до того, как злоумышленники сумеют воспользоваться ими, а также помогут предотвратить будущие атаки. Сотрудничество с экспертами «Лаборатории Касперского» поможет вашим штатным ИБ-специалистам более эффективно противостоять постоянно усложняющимся угрозам.

Это решение идеально подойдет вам, чтобы:

- заручиться поддержкой опытного партнера, способного подстраховать в случае инцидента
- понять, достаточно ли вы защищены от возможных атак
- проводить цифровые расследования

Преимущества для бизнеса

- Эффективная работа служба ИБ благодаря постоянному доступу к экспертным знаниям
- Значительное снижение затрат, связанных с простоями, и минимизация возможного ущерба
- Полное соответствие нормативным требованиям

Практическое применение

- Быстрое восстановление систем и бизнес-процессов
- Обнаружение попыток компрометации и минимизация ущерба от инцидентов
- Оценка возможностей вашей защиты и выявление слабых мест, требующих внимания

3 Требуемые навыки

5 Гибкость и масштабирование

4 Уровень инвестиций

О «Лаборатории Касперского»

«Лаборатория Касперского» — международная компания, работающая в сфере информационной безопасности с 1997 года. Глубокие экспертные знания и опыт компании лежат в основе защитных решений и сервисов, обеспечивающих безопасность бизнеса, критически важной инфраструктуры, государственных органов и пользователей во всем мире.

Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для широкого круга пользователей. «Лаборатория Касперского» защищает домашних пользователей, небольшие компании, предприятия среднего бизнеса и крупные корпорации от всевозможных киберугроз, предлагая всем при этом удобные инструменты для управления системой безопасности.

«Лаборатория Касперского» понимает потребности небольших компаний и предлагает им многоуровневые решения, эффективные и простые в управлении. Компания также отвечает всем запросам крупных предприятий, предоставляя им комплексную платформу, которая защищает от всех типов киберугроз, обнаруживает самые сложные атаки, реагирует на любые инциденты и предвидит развитие угроз.

Кроме того, компания предлагает набор специализированных решений, которые защищают все узлы корпоративной сети, включая мобильные устройства, а также способны обеспечить безопасность центров обработки данных и индустриальных сред.

Технологии «Лаборатории Касперского» защищают более 400 миллионов пользователей и 250 тысяч корпоративных клиентов, помогая сохранить то, что для них важно.

Более подробная информация доступна на www.kaspersky.ru.

Награды и независимые оценки

Больше тестов. Больше наград.

«Лаборатория Касперского» получает больше первых мест в независимых тестах, чем другие поставщики. Год за годом мы демонстрируем неизменно высокие результаты: kaspersky.ru/top3.

Эффективность решений «Лаборатории Касперского» подтверждена оценкой MITRE | ATT&CK®

Логотип GARTNER PEER INSIGHTS CUSTOMERS' CHOICE является товарным и сервисным знаком Gartner Inc. и (или) ее аффилированных компаний и используется в настоящем документе с разрешения владельца. Все права защищены. Рейтинг Gartner Peer Insights Customers' Choice составляется на основе субъективных мнений отдельных конечных пользователей, а также отзывов, рейтингов и данных, собранных в соответствии с утвержденной методологией. Рейтинг не отражает позицию и не содержит рекомендации Gartner или ее аффилированных компаний.

«Лаборатория Касперского» в 2020 году в очередной раз получила награду Gartner Peer Insights Customer's Choice в категории «Платформы для защиты рабочих мест».

«Лаборатория Касперского» получила награду Gartner Peer Insights Customer's Choice в категории Voice of the Customer: EDR Solutions (Выбор клиентов: EDR-решения)

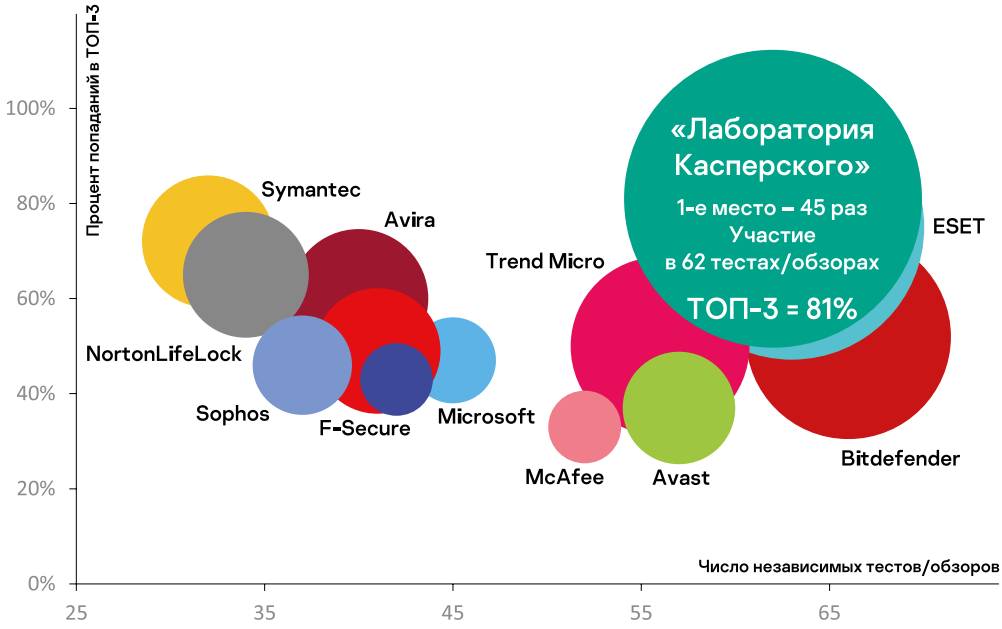
«Лаборатория Касперского» получила награду Gartner Peer Insights Customers Choice 2020 г. в категории Secure Web Gateways (Защита интернет-шлюзов)

Надежность. Открытость. Независимость.

Максимальная прозрачность

«Лаборатория Касперского» демонстрирует уникальный уровень открытости и независимости в отношении своих данных. Доверенные партнеры могут проверить исходный код наших продуктов в Центрах прозрачности.

Больше тестов. Больше наград. Больше защиты.*



В 2020 году продукты «Лаборатории Касперского» приняли участие в 62 независимых тестах и обзорах. Они заняли первое место в 45 случаях и 50 раз вошли в тройку лучших (ТОП-3).

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

* Примечания.

- По сводному результату независимых тестов корпоративных, потребительских и мобильных продуктов за 2020 год.
- В обзор вошли тесты, проведенные следующими независимыми лабораториями: AV-Comparatives, AV-TEST, SE Labs, ICSA Labs, NSS Labs, MRG Effitas, Virus Bulletin, PCSL.
- Тестировались все доступные технологии защиты от известных, неизвестных и комплексных угроз.
- Диаметр круга соответствует числу занятых первых мест.
- Больше тестов, чем у других поставщиков, в любой временной период от 2019–2020 до 2013–2020 гг.

www.kaspersky.ru/top3

Подробнее о продуктах и сервисах «Лаборатории Касперского»:

Для среднего и малого бизнеса – kaspersky.ru/business.

Для крупного бизнеса – kaspersky.ru/enterprise.

kaspersky

© 2021 АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.