



Kaspersky® Threat Management & Defense

Развитие стратегии защиты бизнеса от комплексных угроз и целевых атак

Цифровая трансформация и глобализация информационной среды приводят к повышенной важности информационной безопасности для современных организаций. Чтобы получить конкурентные преимущества и добиться лояльности клиентов и партнеров, компаниям необходимо обеспечить непрерывность бизнеса, надежную защиту критически важных активов, безопасность корпоративных данных и ИТ-инфраструктуры, в том числе критической информационной инфраструктуры (КИИ), а также соблюдение требований внешних регулирующих органов. Все эти условия требуют от организаций развития действующей стратегии информационной безопасности.

Kaspersky Threat Management and Defence позволяет:

- сократить прямые потери от целенаправленных действий злоумышленников;
- снизить риски информационной безопасности;
- сократить количество ручных операций;
- повысить продуктивность работы ИТ и ИБ служб по выявлению, расследованию и реагированию на сложные киберинциденты;
- обеспечить помощь в соответствии требованиям внутренних политик безопасности и внешних регулирующих органов.

Передовые программные технологии

Kaspersky Anti Targeted Attack – обнаружение и расследование комплексных угроз и целевых атак на уровне сети.

Kaspersky Endpoint Detection and Response – обнаружение, расследование и реагирование на киберугрозы, направленные на рабочие станции и серверы.

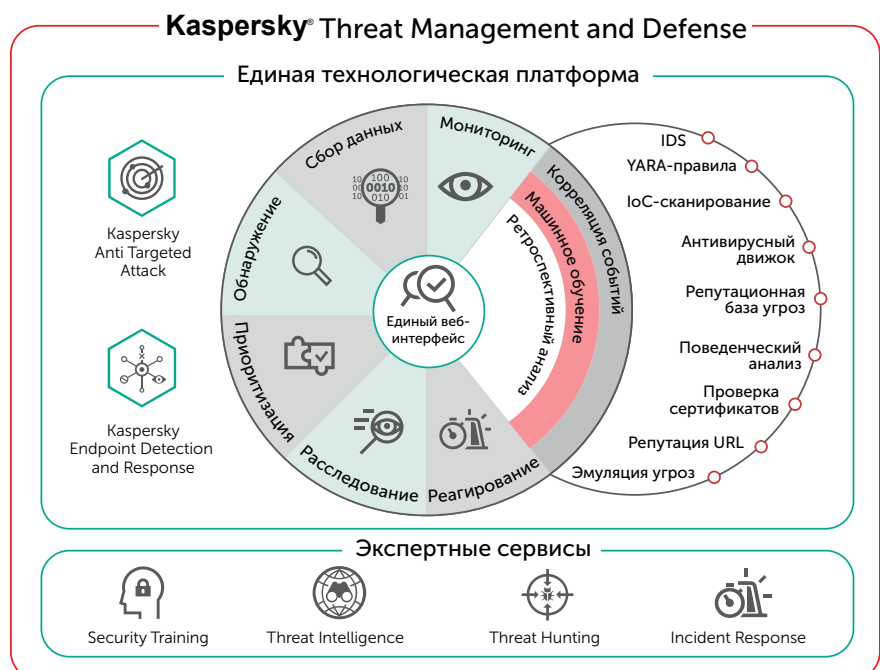
Передача знаний и экспертная помощь

В зависимости от потребностей конкретной организации, наличия у нее собственных ресурсов и квалификации ее специалистов «Лаборатория Касперского» предлагает следующие экспертные сервисы:

- Kaspersky Threat Intelligence – предоставление данных об угрозах;
- Kaspersky Threat Hunting – мониторинг и активный поиск угроз;
- Kaspersky Security Training – тренинги по кибербезопасности;
- Kaspersky Incident Response – сервис реагирования на инциденты.




Kaspersky Threat Management and Defense – важный шаг на пути к стабильности и росту бизнеса

Уникальный специализированный комплекс взаимосвязанных технологических средств, экспертных сервисов и образовательных тренингов «Лаборатории Касперского» способствует эффективному противодействию комплексным кибератакам на всех этапах их реализации за счет своевременного обнаружения сложных многоступенчатых действий злоумышленников и оперативного реагирования на них.



С помощью взаимосвязанных передовых программных средств и сервисов Kaspersky Threat Management & Defense предоставляет комплексный подход к защите бизнеса от направленных действий злоумышленников.

Результат для бизнеса

-  Снижение рисков ИБ
-  Сокращение трудозатрат
-  Увеличение продуктивности
-  Оптимизация затрат
-  Помощь в соответствии требованиям

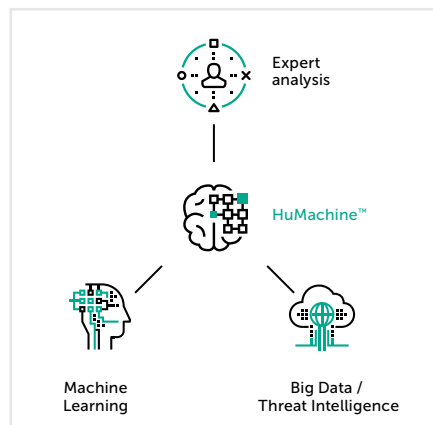
Независимая международная оценка



Качество защитных технологий, предлагаемых «Лабораторией Касперского», подтверждено результатами многочисленных тестов. По данным тестирования Advanced Threat Defense за 2017-2018 гг., проводимых международной компанией ICSA Labs, платформа Kaspersky Anti Targeted Attack показала 100% результат обнаружения угроз при полном отсутствии ложных срабатываний.



По результатам сравнительного анализа рынка решений для защиты от АРТ-угроз, от Radicati Group в 2018 г., решение «Лаборатории Касперского» по противодействию целевым атакам продолжает уверенно занимать ведущую позицию в категории новаторов, постепенно улучшая свое положение по сравнению с предыдущими годами, что дает основание предполагать дальнейший переход решения в категорию лидеров рынка.



Сертифицированное решение по обнаружению сложных угроз на уровне сети

Kaspersky Anti Targeted Attack – программная платформа специализированного комплекса Kaspersky Threat Management and Defense, отвечающая за противодействие комплексным угрозам на уровне сети. Kaspersky Anti Targeted Attack включает набор передовых технологий обнаружения, динамический анализ и эмуляцию угроз на базе высокопроизводительной песочницы и анализатор целевых атак. Анализатор целевых атак использует поведенческий анализ для самостоятельного обнаружения аномальных действий в инфраструктуре, а также динамическое машинное обучение для сопоставления вердиктов, полученных от механизмов обнаружения, с ретроспективными данными и данными, получаемыми в режиме реального времени. Это позволяет значительно ускорить расследование продолжительных многоступенчатых атак.

Передовая технология защиты рабочих мест от комплексных угроз

Kaspersky Endpoint Detection and Response – агентское решение в составе специализированного комплекса Kaspersky Threat Management and Defense, реализованное на той же технологической платформе, что и Kaspersky Anti Targeted Attack. Оно предназначено для обнаружения, анализа, расследования и оперативного реагирования на новейшие киберугрозы, нацеленные на рабочие станции и серверы организации. Единая централизованная консоль обеспечивает наглядное представление информации о событиях безопасности на всех рабочих местах, что способствует оперативному обнаружению угроз и реагированию на них, а также значительной экономии трудозатрат служб ИТ и ИБ.

Надежность и полная конфиденциальность

Если в организации действуют строгие политики конфиденциальности в отношении обработки данных, передачи их в облако и обратной связи с ним, «Лаборатория Касперского» предоставляет вариант полностью изолированного режима работы Kaspersky Threat Management and Defense без потери качества обнаружения. Это достигается за счет:

- интеграции с запатентованной технологией Kaspersky Private Security Network – локальной версией глобальной репутационной базы угроз «Лаборатории Касперского»;
- использования локально размещаемой платформы динамического анализа и эмуляции угроз (высокопроизводительной песочницы);
- предоставления специализированных сервисов проактивного поиска угроз и реагирования на инциденты.

Круглосуточная служба анализа событий ИБ и реагирования на инциденты

Kaspersky Managed Protection предоставляет организациям эффективный и гибкий сервис обнаружения, анализа и защиты от активных атак, куда входит:

- сбор и анализ данных;
- оперативное выявление инцидентов и уведомление сотрудников службы ИБ для принятия необходимых мер;
- ретроспективный анализ событий безопасности и расследование инцидентов;
- рекомендации по предотвращению угроз и устранению их последствий.

www.kaspersky.ru

#ИстиннаяБезопасность

© АО «Лаборатория Касперского», 2018. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.