Kaspersky®
Anti Targeted
Attack

Как снизить риски кибербезопасности в эпоху цифровой трансформации

В современных условиях корпоративная служба информационной безопасности должна стать фундаментом цифровой бизнес-стратегии организаций, заранее выявлять и сокращать риски ИБ и применять комплексный подход к защите от быстро растущего количества сложных угроз и целевых атак, чтобы уменьшить вероятность их разрушительного влияния на критически важные данные организаций и непрерывность существующих бизнес-процессов.

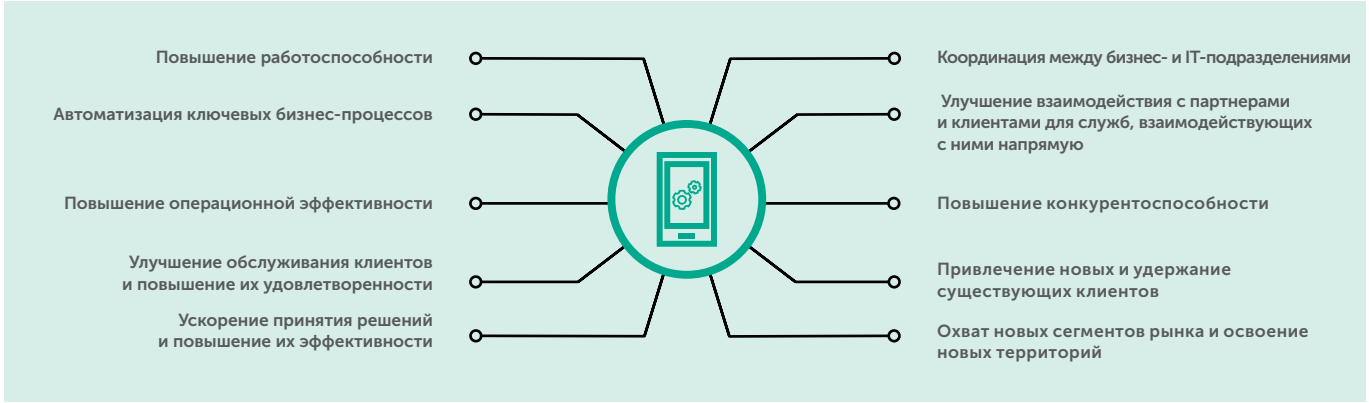
Преимущества платформы Kaspersky Anti Targeted Attack:

- Прозрачность всех теневых IT-ресурсов и скрытых угроз
- Автоматизация задач по расследованию инцидентов и реагированию на них и, как следствие, оптимизация затрат на ресурсы служб ИБ и на SOC-команду
- Помощь в соблюдении требований внутренних служб ИБ, внешних регулирующих органов и действующего законодательства в сфере ИБ

Корпоративная стратегия по предотвращению цифровых угроз

Благодаря растущему числу цифровых технологий, таких как облачные сервисы, большие данные, мобильные устройства, интернет вещей и искусственный интеллект, организации получают массу новых возможностей. Однако при этом, по мере расширения цифровых связей между всеми элементами корпоративной инфраструктуры, становится все сложнее обеспечить информационную безопасность, защитить данные и соответствовать требованиям внешних и внутренних регуляторов.

Бизнес-цели цифровой трансформации



Взаимодействие с существующими системами

- Защитные решения могут быть дополнены новым контекстом и вердиктами по обнаруженным угрозам
- Правила блокирования могут направляться в межсетевые экраны нового поколения (NGFW) и в решения по защите рабочих мест (EPP)
- Данные о событиях взлома или утечки могут передаваться в SIEM-систему
- Защищенные веб-шлюзы (SWG) могут быть расширены информацией об уникальных URL-адресах и доменах

«Лаборатория Касперского» рекомендует придерживаться единой стратегии по построению комплексной корпоративной защиты от сложных угроз и целевых атак. В дополнение к собственным многоуровневым превентивным технологиям или защитным решениям других производителей «Лаборатория Касперского» предлагает платформу Kaspersky Anti Targeted Attack как ключевой элемент единого интегрированного комплекса по обнаружению и противодействию передовым угрозам. Kaspersky Anti Targeted Attack позволяет автоматизировать процесс сбора данных, сократить ручное обнаружение угроз и автоматизировать процесс анализа найденных инцидентов, используя новейшие технологии, глобальную аналитику и возможность корреляции событий на базе машинного обучения.

Запатентованная технология для изолированных сетей

«Лаборатория Касперского» предоставляет вариант полностью изолированного режима работы решения, без потери качества обнаружения, через интеграцию с Kaspersky Private Security Network, которое является полностью локальной версией Kaspersky Security Network и позволяет использовать в работе все преимущества глобального репутационного центра без передачи какой-либо информации за пределы периметра организации и без нарушений требований IT-безопасности для изолированных сетей.

Как работает платформа

Автоматическое агрегирование данных со всей сети

За счет проверки сетевого трафика в режиме реального времени в сочетании с анализом поведения подозрительных объектов в песочнице и проактивной защитой рабочих мест платформа Kaspersky Anti Targeted Attack дает полное представление о том, что происходит в масштабах даже географически распределенной корпоративной IT-инфраструктуры. Это позволяет обнаруживать угрозы на самых ранних этапах и комплексно реагировать на инциденты любой сложности. Сбор вредоносных объектов может осуществляется по протоколам SPAN, ICAP, POP3S или SMTP; также они могут извлекаться и из сторонних систем для проведения последующего анализа.

Доказанная эффективность

В ходе независимых тестов Advanced Threat Defense за 2017 год, проводимых международной компанией ICSA Labs, платформа Kaspersky Anti Targeted Attack показала 100% результат обнаружения угроз, не допустив во время тестов ни одного ложного срабатывания.

«Платформа Kaspersky Anti Targeted Attack позволяет обнаружить комплексные угрозы на всех этапах целевой атаки: первоначальное заражение, коммуникации с командными центрами, дальнейшее распространение заражения и извлечение данных».

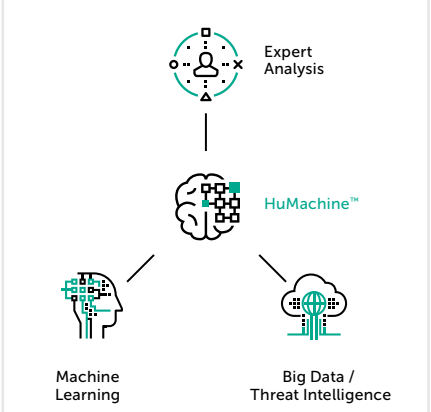
Сравнительный анализ решений для защиты от APT-угроз, Radicati Group, 2018.

Передовые многоуровневые механизмы обнаружения

Платформа Kaspersky Anti Targeted Attack разработана на основе передовых технологий аналитики и машинного обучения. Для корреляции инцидентов, поиска индикаторов компрометации и обнаружения даже самых сложных целевых атак эта платформа объединяет данные с сети и конечных точек, а также использует передовую песочницу и проводит глубокий анализ угроз. Собирая общую картину инцидента из разрозненных данных, платформа формирует детальное представление обо всей цепочке спланированной злоумышленниками атаки.

Автоматическое предотвращение передовых угроз и комплексное реагирование на инциденты

Платформа Kaspersky Anti Targeted Attack может автоматически обмениваться вердиктами с другими защитными решениями «Лаборатории Касперского». Kaspersky Anti Targeted Attack, Kaspersky Private Security Network, Kaspersky Secure Mail Gateway, Kaspersky Security для бизнеса и Kaspersky Endpoint Detection and Response тесно интегрированы между собой на всех уровнях, что позволяет применять своевременные меры реагирования сразу после обнаружения инцидента и обеспечить комплексную защиту от сложных угроз и целевых атак.



www.kaspersky.ru

#ИстиннаяБезопасность