kaspersky АКТИВИРУЙ БУДУЩЕЕ

Интегрированный подход к защите рабочих мест от сложных угроз

Kaspersky Endpoint Detection and Response

Проведенный «Лабораторией Касперского» опрос представителей ИТ- и ИБ-департаментов крупнейших компаний России и стран СНГ показал значительный рост количества и сложности инцидентов. Опрошенные компании особо отметили факт участившихся комплексных атак на рабочие станции и серверы, которые, по статистике, остаются основными мишенями злоумышленников. Большинство организаций понимают, что подобные инциденты нарушают стабильность их бизнеса. Однако часть компаний не готовы к детальному расследованию подобных случаев, другие – к анализу большого количества сложных инцидентов и реагированию на них. Это приводит либо к неэффективному использованию и перегрузке служб ИТ и ИБ, либо к игнорированию проблемы.

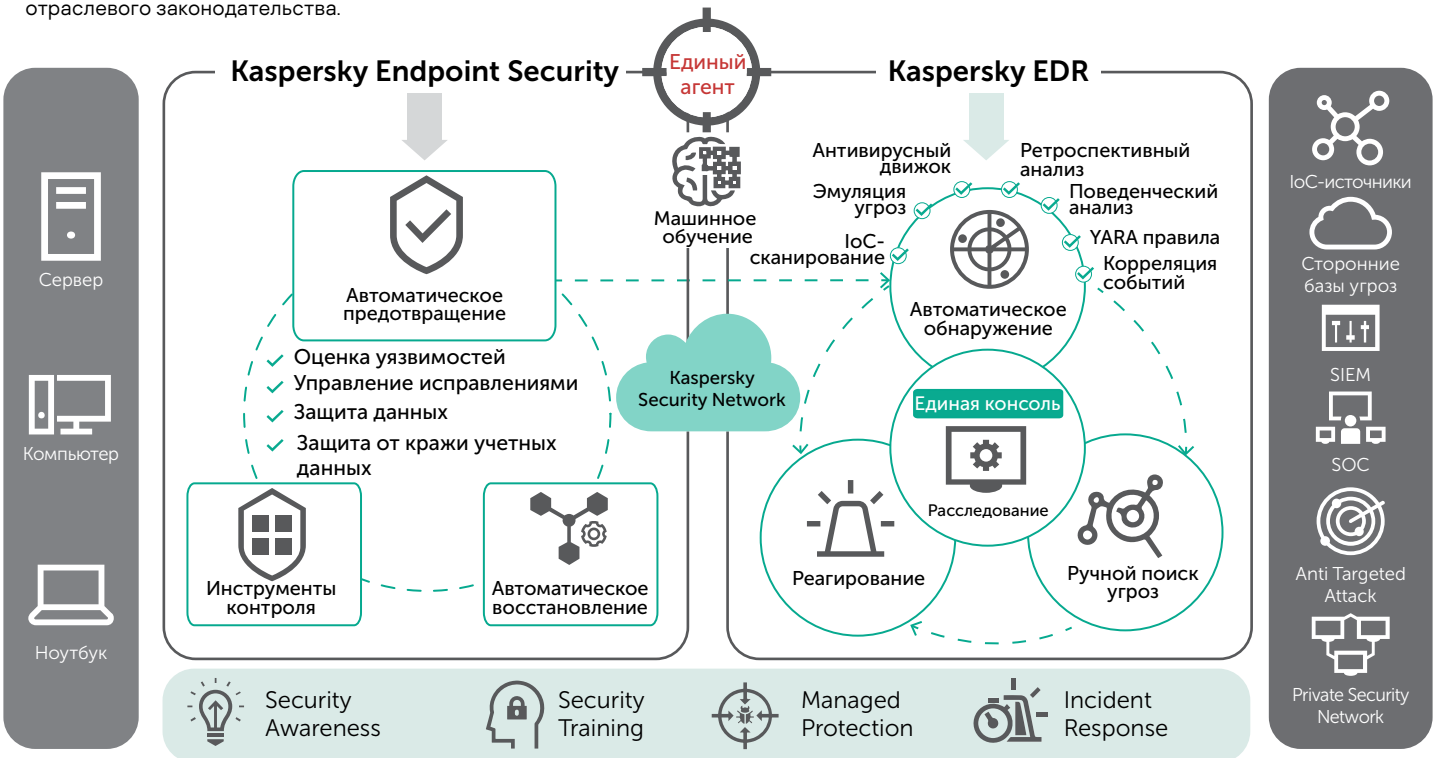
Актуальные проблемы ИТ-безопасности:

- необходимость ручного разбора и анализа большого числа инцидентов;
- эксплуатация средств ИБ, которые не взаимодействуют друг с другом и управляются из разных консолей;
- принятие решений без использования средств для наглядного централизованного представления информации;
- выполнение сложных задач в условиях нехватки квалифицированных кадров и экспертизы;
- несоответствие требованиям внешних регулирующих органов и действующего отраслевого законодательства.

Развитие существующей защиты

Интегрированный подход «Лаборатории Касперского» к защите рабочих мест обеспечивает эффективное противодействие новейшим угрозам и целевым атакам. При этом осуществляется автоматическое предотвращение рядовых угроз, обнаружение и приоритизация сложных угроз, а также детальное расследование инцидентов и реагирование на них.

В рамках данного подхода используются интегрированные программные решения Kaspersky Endpoint Security и Kaspersky EDR. Они могут быть дополнены экспертными сервисами и обучающими тренингами «Лаборатории Касперского», которые подбираются индивидуально в зависимости от потребностей конкретной организации, наличия у нее собственных ИБ-специалистов и уровня их квалификации.



Kaspersky EDR предоставляет полную картину событий безопасности в корпоративной ИТ-инфраструктуре и позволяет автоматизировать выполнение рутинных задач по выявлению, приоритизации, расследованию и нейтрализации сложных угроз.

Использование Kaspersky EDR позволяет эффективно решать следующие задачи:

- Формирование организацией целостного подхода к выявлению, расследованию и централизованному реагированию на инциденты;
- Повышение уровня вовлеченности ИБ-специалистов и увеличение общего числа обрабатываемых инцидентов за счет автоматизации процессов и использования интуитивно понятного веб-интерфейса;
- Следование рекомендациям ФинЦЕРТ и данным об угрозах от других источников благодаря возможности загрузки в решение полученных индикаторов компрометации (IoC) и последующего автоматического сканирования рабочих станций и серверов;
- Мониторинг и проактивный поиск аномальной активности, индикаторов компрометации (IoC) и иных признаков вредоносных действий на всех рабочих местах (Threat Hunting);
- Повышение эффективности внутренних расследований за счет обогащения SIEM/SOC дополнительным контекстом с возможностью сопоставления результатов анализа данных, поступивших с рабочих мест, с событиями, полученными от иных систем;
- Оперативное реагирование и сдерживание комплексных инцидентов, устранение последствий атаки на отдельных рабочих местах и восстановление их работоспособности без влияния на работу пользователей;
- Следование нормативам внешних регулирующих органов, стандартам банковской отрасли, PCI DSS, а также требованиям российского законодательства в отношении использования решений по расследованию сложных угроз (Федерального закона «О безопасности КИИ РФ» N 187-ФЗ и Указа Президента РФ №31с «О создании ГосСОПКА»).

Преимущества Kaspersky EDR

Единый агент для надежной защиты и контроля рабочих мест

Для организаций, уже использующих решение Kaspersky Endpoint Security, функционал Kaspersky EDR по обнаружению, расследованию и реагированию на сложные угрозы предоставляется в рамках уже установленного единого программного агента. Это позволяет избежать дополнительной нагрузки и снижения производительности рабочих мест, упростить процесс контроля и обеспечить полноценную защиту рабочих станций и серверов организации от сложных угроз.

Централизованное хранение данных

Сбор, запись и централизованное хранение информации о событиях безопасности на всех рабочих местах позволяет обеспечить оперативный доступ к ретроспективным данным при расследовании продолжительных атак, даже в условиях недоступности рабочих мест или компрометации/уничтожения необходимых данных. Компании также могут оказывать содействие службе реагирования и регулирующим органам, предоставляя им необходимую информацию об обнаруженных угрозах.

Автоматизация работы ИБ-службы

Автоматический сбор, анализ и сопоставление данных позволяет организациям автоматизировать выполнение ручных операций, связанных с процессами обнаружения, расследования и реагирования на инциденты и оптимизировать трудозатраты своих высококвалифицированных специалистов.

Единая централизованная консоль для оперативного реагирования на угрозы

Наглядное представление информации об инфраструктуре рабочих мест в централизованной веб-консоли позволяет сотрудникам служб ИБ оперативно реагировать на инциденты, минимизирует количество ручных задач и сокращает общие трудозатраты на мероприятия по реагированию с часов до минут.

Комплексная многоуровневая защита

В рамках единой специализированной платформы для защиты от целевых атак и новейших угроз решение Kaspersky EDR может поставляться совместно с сертифицированной ФСТЭК и ФСБ платформой Kaspersky Anti Targeted Attack для противодействия сложным угрозам на уровне сети, что позволяет обеспечить более комплексный подход к защите ИТ-инфраструктуры организации на всех уровнях.

Защита инфраструктуры с повышенными требованиями к изоляции

В организациях со строгим политиками конфиденциальности решение может использовать для получения сведений об угрозах запатентованную технологию Kaspersky Private Security Network. Это дает возможность получать все преимущества глобальной репутационной базы угроз «Лаборатории Касперского», не передавая какую-либо информацию за пределы организации.

www.kaspersky.ru