Правда или вымысел? 5 самых распространенных мифов о решениях EDR

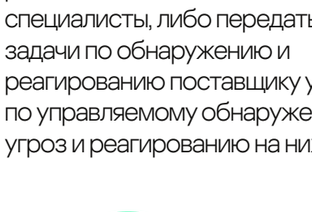
Аналитики оценивают объем рынка решений для обнаружения угроз и реагирования на них на уровне конечных точек (Endpoint Detection and Response, EDR) по-разному, однако большинство сходятся во мнении, что рынок растет приблизительно на 25% в год. Это означает, что технологии EDR играют все более важную роль в защите рабочих мест. Но несмотря на это, не все понимают, в чем ценность EDR, и о решениях этого класса есть немало мифов. Опровергаем самые распространенные.

Миф №2

Решение класса EDR может компенсировать недостатки слабого EPP-решения

Миф

Наше решение для защиты рабочих мест недостаточно эффективно – EDR поможет укрепить защиту.



Реальность

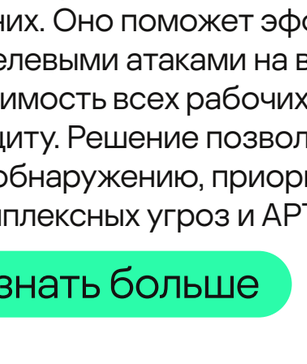
Пытаться укрепить защиту рабочих мест с помощью EDR-решения, не разобравшись в причинах неэффективности решения для защиты конечных точек – это все равно что строить высотку в зыбучих песках. Слабое EPP-решение может свести на нет все преимущества EDR. Сильное решение EDR строится только на надежном фундаменте EPP.

Миф № 4

Нельзя комбинировать EDR и MDR

Миф

Если вам требуется защита класса EDR, нужно либо приобрести EDR-решение, с которым будут работать ваши собственные специалисты, либо передать задачи по обнаружению и реагированию поставщику услуг по управляемому обнаружению угроз и реагированию на них (MDR).



Реальность

Одно не исключает другого. У EDR и MDR разные преимущества, зачастую оптимальный вариант – их сочетание. Например, малому и среднему бизнесу, а также не очень крупным предприятиям MDR-решение поможет быстро укрепить IT-безопасность и защититься от скрытых угроз. При этом компании не придется вкладывать средства в персонал или другие ресурсы. Предприятия со зрелым подходом к безопасности смогут передать основные задачи по приоритизации и расследованию инцидентов внешним экспертам, позволив своим ИБ-специалистам сосредоточиться на детальном расследовании и последующем реагировании с помощью EDR.

Решения класса EDR «Лаборатория Касперского»

Злоумышленникам почти ничего не стоит организовать атаку. А вот ущерб от нее может быть очень велик. Нехватка ресурсов и ограниченные возможности контроля в организации играют на руку преступникам. **Kaspersky EDR для бизнеса Оптимальный** с базовыми функциями EDR – это удобное решение с функциями расширенного обнаружения и автоматизированного реагирования, которое упростит повседневную работу ИБ-специалистов и защитит бизнес от новейших угроз.

Узнать больше

Решение экспертного уровня **Kaspersky EDR Expert** дает командам ИБ максимум возможностей для расследования инцидентов и реагирования на них. Оно поможет эффективно справиться со сложными угрозами и целевыми атаками на вашу инфраструктуру. Обеспечит полную видимость всех рабочих мест в корпоративной сети и их эффективную защиту. Решение позволит автоматизировать повседневные задачи по обнаружению, приоритизации, расследованию и нейтрализации комплексных угроз и APT-атак.

Узнать больше

Миф № 1

Нам хватит решения для защиты рабочих мест – EDR нам не нужен

Миф

Киберпреступников не интересуют такие компании, как наша, – нам не страшны угрозы, от которых защищает EDR.

Реальность

На первый взгляд может показаться, что небольшие компании – непривлекательная цель для киберпреступников, однако им зачастую приходится сталкиваться с теми же угрозами, что и крупным предприятиям. 90% инцидентов связаны с простыми, массовыми угрозами, большую часть оставшихся 10% составляют новые, неизвестные и скрытые угрозы, способные обходить технологии защиты рабочих мест (EPP). Такие угрозы тяжело обнаружить: они задействуют множество техник обхода защиты, например используют легитимные и системные инструменты. Чем дольше такие угрозы остаются незамеченными, тем глубже они могут внедриться в инфраструктуру компании и тем больший ущерб нанести, будь то утечка данных, их шифрование, шпионаж или прямое вмешательство в бизнес-процессы.

Миф № 3

Работать с EDR могут только эксперты по кибербезопасности

Миф

У небольших компаний нет экспертизы, чтобы разобраться с инструментами для обнаружения скрытых угроз, организовать реагирование на них и выстроить дальнейшеее расследование.

Реальность

Первые EDR-решения были сложными, а для их использования требовались специальные навыки. Но сейчас появились и более простые в использовании решения с базовыми функциями EDR, которые оптимально подходят небольшим командам ИБ. Они помогают не только отреагировать на инцидент, но и провести анализ первопричин, а также проверить инфраструктуру с помощью индикаторов комппрометации. И все это в удобном, автоматизированном формате.

Миф № 5

EDR генерирует слишком много событий безопасности и усложняет работу

Миф

Есть мнение, что EDR генерирует слишком много оповещений и ложных срабатываний. У IT-отделов нет ни времени, ни ресурсов для их обработки.

Реальность

В современных EDR-решениях многие процессы автоматизированы. Вы сможете отслеживать все происходящее в инфраструктуре и получите полный обзор рабочих мест и контроль над ними. За счет автоматизации и прозрачности отслеживать события безопасности становится проще.

kaspersky