Решение ваших текущих и будущих ИБ-задач

Ступенчатый подход к кибербезопасности

kaspersky

kaspersky.ru

Выбор подходящего продукта или сервиса для обеспечения безопасности вашей организации – лишь самый первый шаг. Для успеха вашего бизнеса в долгосрочной перспективе критически важно разработать продуманную корпоративную стратегию киберзащиты.

Решения «Лаборатории Касперского» удовлетворяют потребности современного бизнеса в безопасности вне зависимости от уровня ИБ-зрелости организации. Благодаря ступенчатому подходу, включающему различные уровни защиты от киберугроз всех типов, можно обнаруживать сложнейшие атаки, быстро и эффективно реагировать на любые инциденты и предотвращать будущие угрозы.

Типы угроз и зрелость службы ИБ

По мере увеличения масштаба IT-инфраструктур компании сталкиваются со всё более сложными угрозами. Чтобы эффективно противостоять им, необходимо постоянно развивать киберзащиту, а также накапливать опыт и знания.

Современные киберугрозы можно разделить на три основных класса. Большинство из них находится в основании пирамиды. Это угрозы общего характера, для противодействия которым достаточно базовых защитных механизмов и соблюдения основополагающих правил IT-безопасности. По мере движения вверх по пирамиде мы видим все более продвинутые угрозы, способные избегать превентивного обнаружения за счет известных тактик, методов и процедур (TTP). Организаторы подобных атак могут, к примеру, заполучить в свое распоряжение достаточно сложный инструментарий, ранее разработанный их более опытными «коллегами». Большинство инцидентов безопасности находится именно в этой категории.

И наконец, на самой вершине пирамиды находятся сложные APT-угрозы и атаки с использованием неизвестных TTP. Организаторы атак в этой категории располагают практически неограниченными ресурсами для разработки очень сложных инструментов и методов, как правило, предназначенных для целенаправленных атак на конкретные цели.

Рис 1. Типы угроз и квалификация сотрудников

Чтобы продолжать развиваться и сохранять конкурентоспособность, компании вынуждены все больше полагаться на информационные технологии. В процессе цифровой трансформации и с увеличением количества взаимосвязанных систем потенциальная поверхность атаки постоянно увеличивается. По мере увеличения масштаба IT-инфраструктур компании сталкиваются со все более сложными угрозами. Чтобы эффективно противостоять им, необходимо развивать киберзащиту, а также накапливать опыт и знания.

Ступенчатый подход к кибербезопасности

Учитывая возрастающее количество и сложность угроз, уровень зрелости IT-безопасности, навыки персонала в сфере кибербезопасности и имеющиеся бюджеты, компании приходят к осознанию необходимости всеобъемлющей и гибкой стратегии безопасности.

С учетом наблюдаемых нами угроз и разных возможностей кибербезопасности наших клиентов мы разделили все наши решения на три уровня.

На первом уровне мы предоставляем продукты для предотвращения угроз вместе с расширенной технической поддержкой и профессиональными сервисами, чтобы клиенты могли извлечь из наших технологий максимум выгоды.

На втором уровне возрастает потребность в противостоянии угрозам, обходящим существующие механизмы предотвращения. Для обеспечения защиты от продвинутых и маскирующихся угроз в условиях ограниченных ресурсов мы предоставляем базовые инструменты класса EDR и песочницу, которые помогают специалистам по безопасности эффективнее обнаруживать и анализировать особо опасные трудноуловимые угрозы и реагировать на них.

На третьем уровне вероятность столкнуться с реальной APT-атакой значительно возрастает, и организациям требуется эффективная защита от сложных атак. Для удовлетворения запросов развитых ИБ-департаментов и команд SOC «Лаборатория Касперского» предоставляет единую платформу безопасности, которая позволяет справиться со сложнейшими современными угрозами и целевыми атаками.

Решение Kaspersky Managed Detection and Response позволяет активировать передовые функции защиты без необходимости нанимать дополнительных сотрудников и обучать существующих. В частности, оно дает возможность делегировать «Лаборатории Касперского» поиск угроз и реагирование на инциденты, чтобы можно было направить ограниченные ресурсы штатных ИБ-специалистов компании на решение других важных задач.

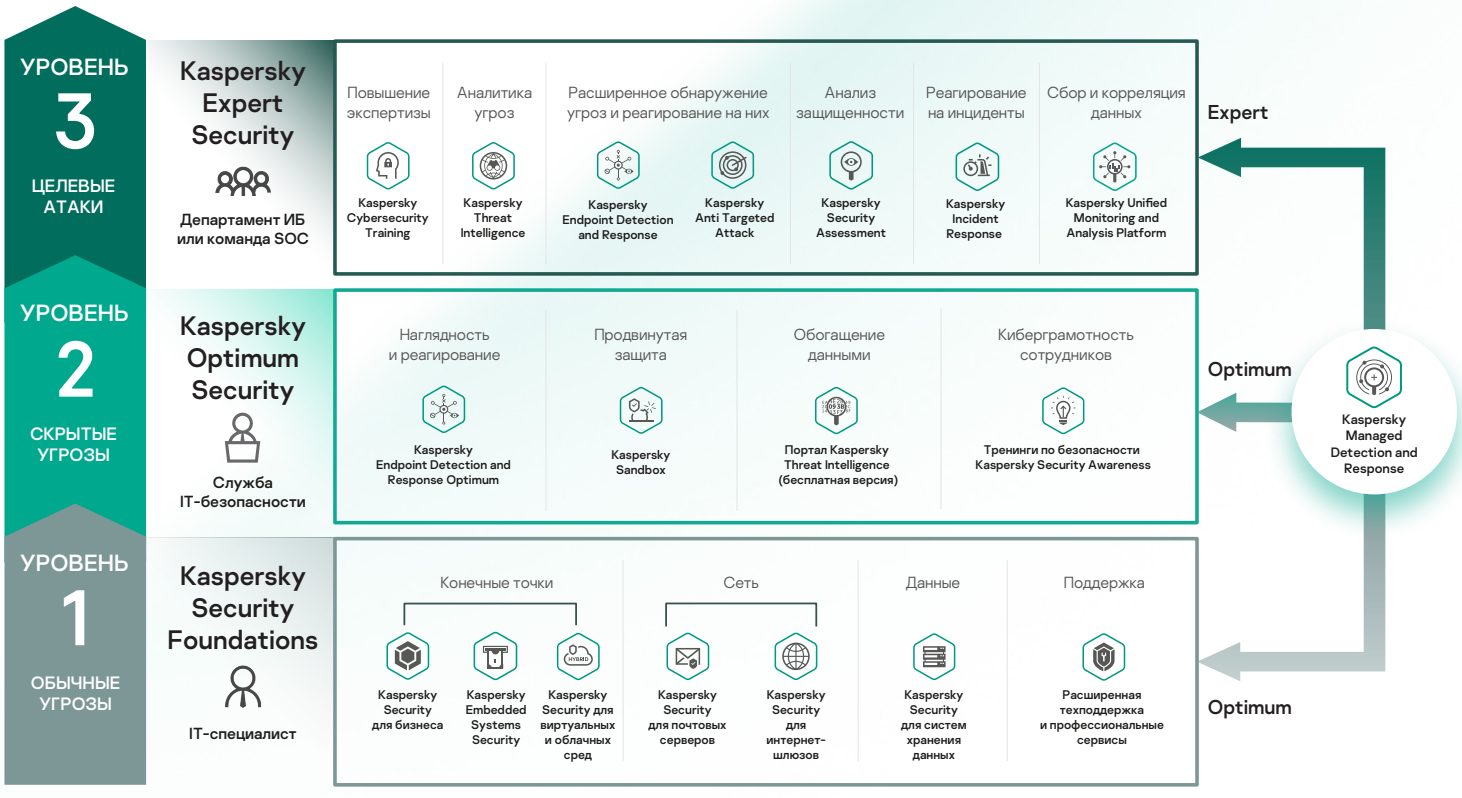

Рис 2. Ступенчатый подход к кибербезопасности

Kaspersky Security Foundations

Автоматическое блокирование максимально возможного числа угроз.

Kaspersky Security Foundations – это базовый этап организации безопасности для компаний любого масштаба с инфраструктурой любой сложности, заключающийся в создании интегрированной стратегии защиты от сложных угроз. На этом уровне обеспечивается многовекторное автоматическое предотвращение большого числа возможных инцидентов безопасности, вызванных обычными угрозами. Обычно этого достаточно для не очень крупных компаний, в которых есть только IT-отдел.

Компании не могут пропустить этот этап и сразу перейти к использованию более продвинутых технологий обнаружения и реагирования. Дело в том, что большинство этих технологий подразумевает вовлечение специалистов, что, во-первых, сопряжено с немалыми затратами, а во-вторых, требует значительного опыта. В итоге высокооплачиваемые ИБ-специалисты просто утонут в море оповещений об инцидентах, а большинство угроз так и не будут предотвращены. Вместо проактивного поиска маскирующихся угроз и реагирования на инциденты безопасности ИБ-специалисты вынуждены будут заниматься сортировкой и приоритизацией оповещений, причем большинство из них так и не будет расследовано.

Рис 3. Основные характеристики уровня 1

Kaspersky Optimum Security

Упор на продвинутое обнаружение и оперативное реагирование на угрозы, пропущенные средствами превентивной защиты.

IT-среды, поддерживающие развитие организаций и рост бизнеса, становятся все крупнее и сложнее, что, в свою очередь, увеличивает потенциальную поверхность атаки. Они становятся более привлекательными целями для злоумышленников. У них возрастает риск столкнуться с продвинутыми угрозами, которые могут обойти автоматические защитные механизмы.

Чем выше вероятность потенциальной поверхности атаки, тем очевиднее необходимость внедрения хотя бы базовых инструментов реагирования на инциденты безопасности. Поэтому компании направляют часть своих IT-ресурсов на решение проблем кибербезопасности, но их штатные специалисты еще не готовы к таким задачам. Небольшие ИБ-отделы нуждаются в инструментарии для автоматического обнаружения продвинутых угроз и централизованного реагирования – это своего рода фундамент их дальнейшего развития. Также крайне важно обучать сотрудников для повышения общей осведомленности об угрозах в вашей организации: тренинги помогут обратить их внимание на киберугрозы и расскажут о мерах борьбы с ними, даже если сотрудники полагают, что это не входит в их непосредственные обязанности.

Решение Kaspersky Optimum Security – это продолжение Kaspersky Security Foundations. Оно позволяет организациям с развивающейся IT-инфраструктурой защищаться от обычных атак и угроз, способных обходить существующие механизмы предотвращения. Это решение создано с учетом ограниченности ресурсов и идеально подходит небольшим ИБ-отделам, обладающим базовыми знаниями и опытом. На этом этапе клиенты могут улучшить систему обнаружения угроз и реагирования на них, а также воспользоваться преимуществами круглосуточной защиты, управляемой экспертами. В то же время наши тренинги по основам кибербезопасности помогут выработать у сотрудников навыки кибергигиены и мотивировать их следовать безопасному поведению.

- Успешное внедрение Kaspersky Security Foundations
- IT-инфраструктура растет и усложняется, что ведет к увеличению поверхности атаки
- Имеется небольшой отдел IT-безопасности с некоторым опытом
- Эффективное реагирование на инциденты имеет большое значение

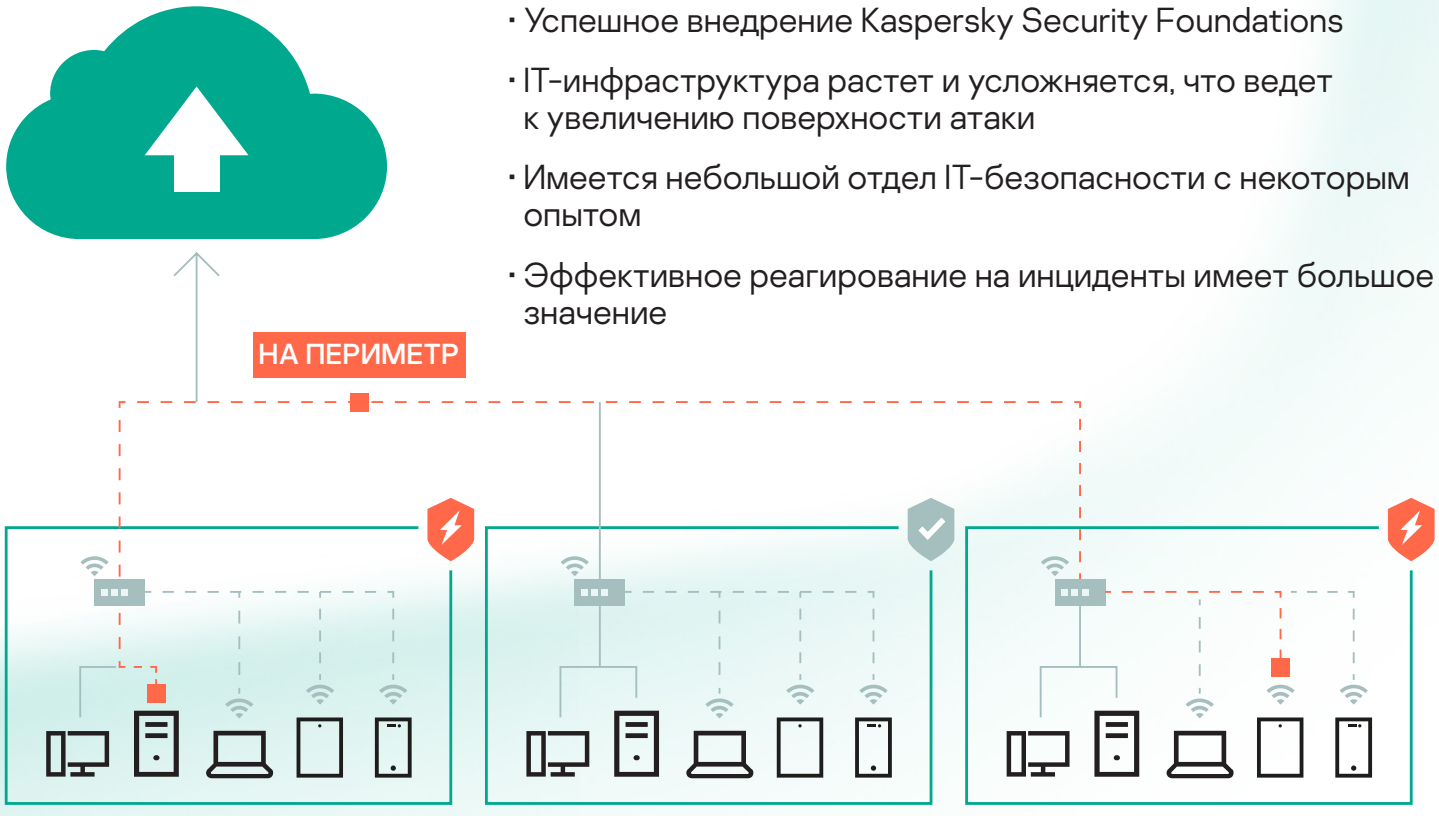

Рис 4. Основные характеристики уровня 2

Kaspersky Expert Security

Способность противостоять сложным угрозам и APT-атакам.

Компании с развитой службой ИБ или команды SOC могут развернуть полноценную экосистему комплексной защиты на основе интегрированных решений «Лаборатории Касперского». Центральным элементом единой платформы безопасности является решение класса SIEM — Kaspersky Unified Monitoring and Analysis Platform.

Для борьбы с угрозами и целевыми атаками Kaspersky Unified Monitoring and Analysis Platform собирает и анализирует данные из всех подключённых к нему источников — продуктов «Лаборатории Касперского» и решений сторонних производителей.

Компоненты экосистемы дополняют друг друга и обмениваются информацией. В итоге ИБ-специалисты получают полную картину происходящего в инфраструктуре и оперативно отражают кибератаки любой сложности.

- IT-среды становятся все более сложными и распределенными
- ИБ-отдел обладает достаточным уровнем подготовки, или в компании есть SOC
- Устойчивость бизнеса к сложным и целевым атакам является приоритетной задачей
- Соблюдение нормативных требований имеет большое значение

Рис 5. Основные характеристики уровня 3

www.kaspersky.ru