EDR

ЗАЩИЩЕННОСТЬ КОНЕЧНЫХ УСТРОЙСТВ В РОССИЙСКИХ КОМПАНИЯХ

positive technologies

СОДЕРЖАНИЕ

ЦЕЛИ, МЕТОДЫ И УЧАСТНИКИ ИССЛЕДОВАНИЯ

Исследование основано на результатах интервью с представителями ИТ и ИБ подразделений различных организаций. Опросы проводились с помощью анкет и по телефону. В сравнении с публикацией раннего исследования [1] в 2024 году, данное включает расширенный набор вопросов для респондентов.

Цель исследования — узнать, насколько российские компании защищены от целевых атак, как они выстраивают защиту конечных точек (компьютеров, серверов и сетевого оборудования), как смотрят на бюджетирование средств защиты, с какими трудностями сталкиваются и на какие функции продуктов ИБ обращают внимание в первую очередь. В опросе, проведенном в конце 2024 года, приняли участие 392 специалиста по ИБ и ИТ из более чем 350 российских компаний малого, среднего и крупного бизнеса. Мы, как и другие аналитические агентства следим за трендами рынка , и здесь конкретно фокусируемся на защите конечных устройств.

Размер компании (количество сотрудников)

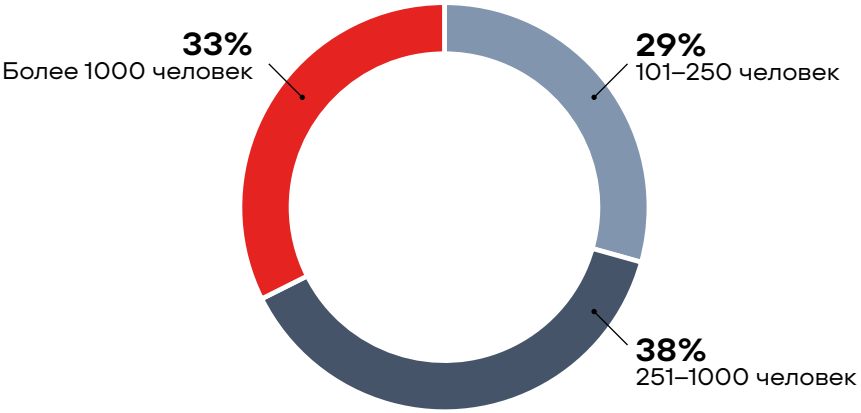

Рисунок 1. Размер компаний-участников опроса

Должность респондента

89%
Специалисты по ИБ

11%
Руководители ИТ/ ИБ

14%
принимают решения по информационной безопасности

[1]

Отрасль компании

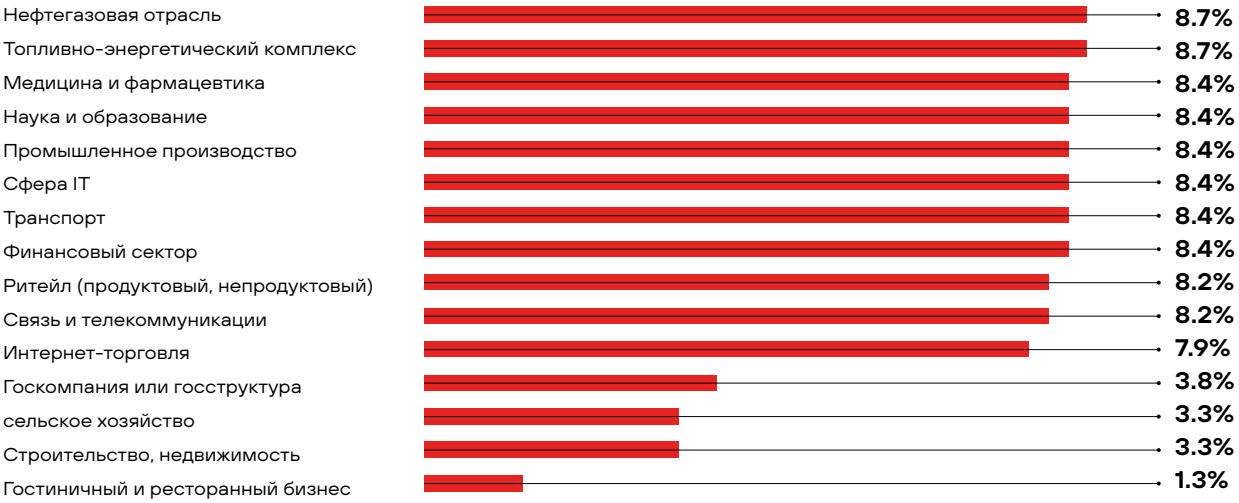

Рисунок 2. Сфера деятельности компаний-участников опроса

ОСНОВНЫЕ РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

84% респондентов используют для защиты устройств организации комбинацию СЗИ. Этот показатель на 8 п.п. выше, чем в прошлом году

3.2 среднее число применяемых средств защиты конечных точек в опрошенных компаниях

56% респондентов считают главной задачей обнаружение и предотвращение целенаправленных APT-атак

313 инцидентов в месяц в среднем приходится обрабатывать респондентам

62% инцидентов были задействованы компьютеры сотрудников, при этом **39%** респондентов из крупных компаний назвали среди атакуемых устройств компьютеры топ-менеджеров

12 часов — среднее время расследования инцидентов*

44% крупных компаний тратят усилия на разбор более 10 сложных атак в месяц

*По данным исследования команды Incident Response PT ESC среднее время от начала инцидента до обнаружения нелегитимной активности (TTD) — 17 дней [2]

Согласно исследованию Positive Technologies [3], в IV квартале 2024 года вредоносное ПО оставалось главным оружием злоумышленников: оно применялось в 66% успешных атак на организации и в 51% атак на частных лиц. Против организаций чаще всего использовались шифровальщики (42%) и ВПО для удаленного управления (38%), против частных лиц — шпионское ПО (48%).

В прошлом году мы писали об инструментах [4] и ВПО для удаленного управления [5], которые нередко использовались в успешных атаках. Стоит отметить и техники Bring Your Own Vulnerable Driver (BYOVD), распространение шпионского ПО через рекламные сервисы, портирование шифровальщиков под отдельные среды виртуализации, использование ИИ для написания зловредного кода и скриптов PowerShell. Все это помогало злоумышленникам обходить имеющиеся средства защиты и дольше оставаться в сети атакуемой организации.

Растет количество успешных атак на Linux-системы (25% в IV квартале 2024 года против 20% в III квартале), но Windows продолжает оставаться основной целевой ОС (79% в IV квартале) для атакующих.

2

3

4

5

ПОДХОДЫ К ЭШЕЛОНИРОВАННОЙ ЗАЩИТЕ

Исследование в очередной раз подтвердило, что уровень защищенности напрямую связан с размером организации. Это можно объяснить как более развитой функцией ИБ, так и большими бюджетами на средства защиты.

Так, в организациях с численностью до 250 человек 42% опрошенных указали, что полагаются только на антивирусную защиту. В компаниях более чем с 1000 сотрудников в 100% случаев используется несколько классов решений.

84% **опрошенных компаний применяют комплексный подход для защиты устройств**

3.2 **среднее количество используемых классов решений**

Рисунок 3. Среднее количество используемых классов решений для защиты конечных устройств в компаниях-участниках опроса

Наиболее универсальными инструментами являются EPP- и HIPS-системы. По сравнению с прошлым годом на 35% вырос запрос респондентов на EPP-решения.

Решения других типов обычно используются крупными компаниями. Заметно увеличилась доля организаций, применяющих для защиты EDR- и XDR-решения (на 37 и 39 процентных пунктов соответственно).

Какие средства Вы используете для защиты конечных устройств?

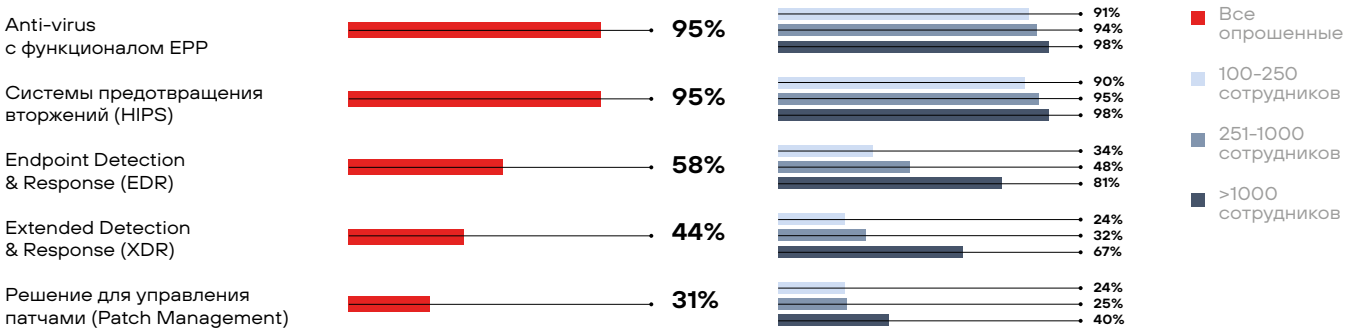

Рисунок 4. Средства защиты конечных устройств, использующиеся в компаниях

28% КОМПАНИЙ ПЛАНИРУЮТ ВНЕДРЕНИЕ EDR ДЛЯ ЗАЩИТЫ КОНЕЧНЫХ УСТРОЙСТВ В 2025 ГОДУ

Решения класса EDR чаще всего планируются к покупке, в основном это наблюдается в компаниях со штатом менее 1000 сотрудников. Около половины компаний (52%) не планируют внедрение новых решений в 2025 году. В случае с крупными организациями, отсутствие инвестиций в решения для защиты конечных точек объясняется зрелыми процессами SOC и наличием EDR-, XDR-систем и MDR-сервисов. Для средних и малых компаний ключевым фактором являются бюджетные ограничения и отсутствие соответствующей экспертизы.

Планируется ли в Вашей компании внедрение какого-либо из перечисленных средств в 2025 году?

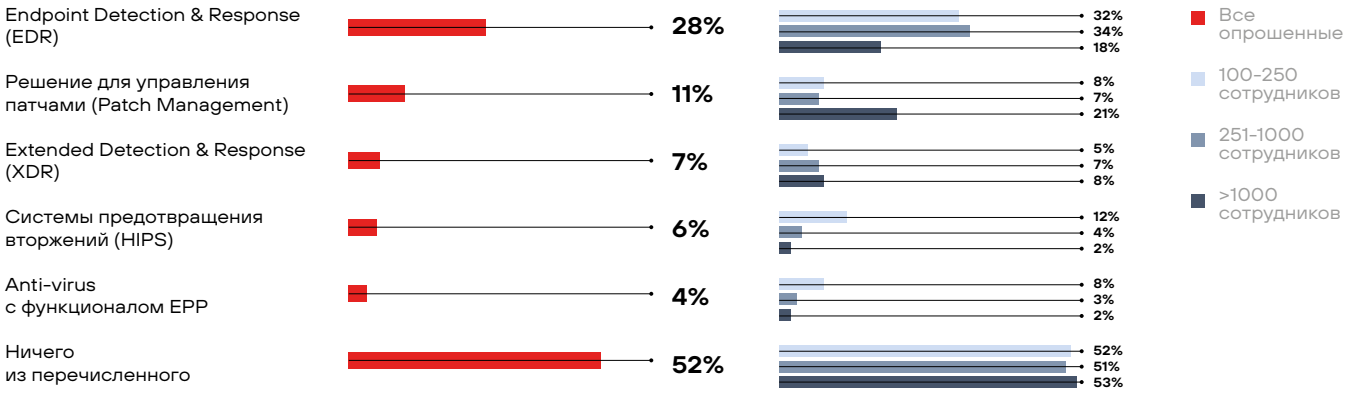

Рисунок 5. Планы по внедрению средств защиты конечных устройств в 2025 году

По-прежнему наблюдается тренд на импортозамещение. Подавляющее большинство опрошенных компаний используют для защиты конечных точек отечественные продукты (преимущественно EDR и XDR). В топ-3 популярных решений входит только одно иностранное.

Интересно, что чаще всего респонденты используют агенты EDR на 100% устройств. Даже показатели установки антивирусов в крупных инфраструктурах не всегда близки к полному покрытию. Это связано с тем, что EDR-агенты зачастую используются SOC в качестве легковесных сенсоров для SIEM-систем.

Рисунок 6. Что нравится респондентам в выбранном решении

ПЛАНИРОВАНИЕ РАСХОДОВ НА СЗИ

Около половины компаний численностью до 1000 человек планируют заложить на продукты класса EDR менее 5 млн рублей. 75% крупных компаний планируют потратить больше 5 млн. По сравнению с прошлым годом бюджеты выросли или остались неизменными.

Какая сумма забюджетирована у вас на EDR решение в следующем году

(вопрос задавался только использующим или планирующим покупку EDR)

Как эта сумма изменилась по сравнению с прошлым годом?

(вопрос задавался только использующим EDR)

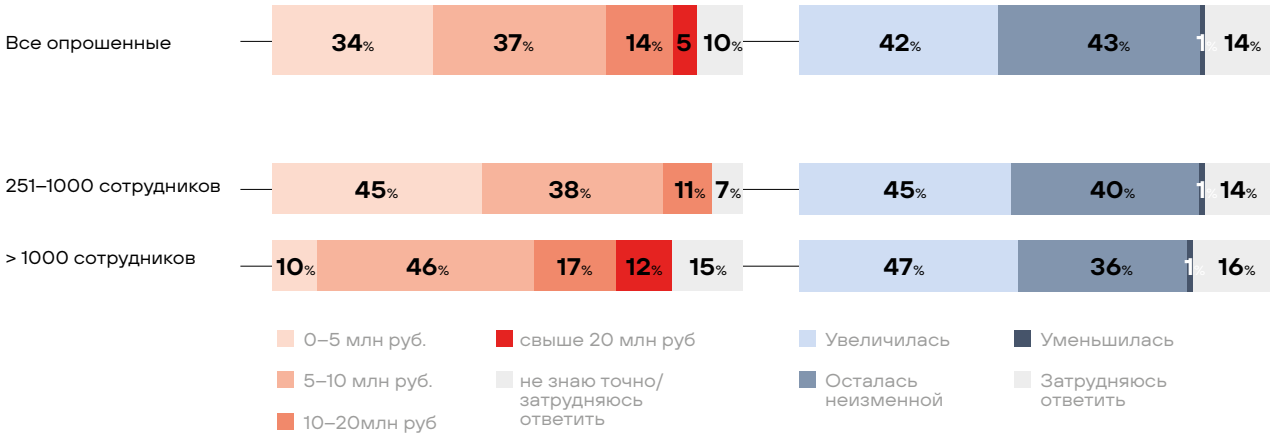

Рисунок 7. Планы бюджетов на EDR-решения в 2026 году

Очевидно, что кроме организаций, планирующих инвестировать в СЗИ для защиты конечных устройств, есть и те, кому EDR-система не нужна. Среди причин отмечаются нехватка бюджетов, негативный опыт использования и дефицит специалистов, готовых работать с продуктом. По сравнению с прошлым годом заметно выросло число компаний, которые тестируют решения такого класса и находятся в процессе принятия решения (21% против 12% в 2023 году). Доля организаций, которые видят ценность таких продуктов, но не используют их в силу бюджетных ограничений, увеличилась с 30% в 2023 году до 42% в 2024 году.

Почему не планируют покупку EDR

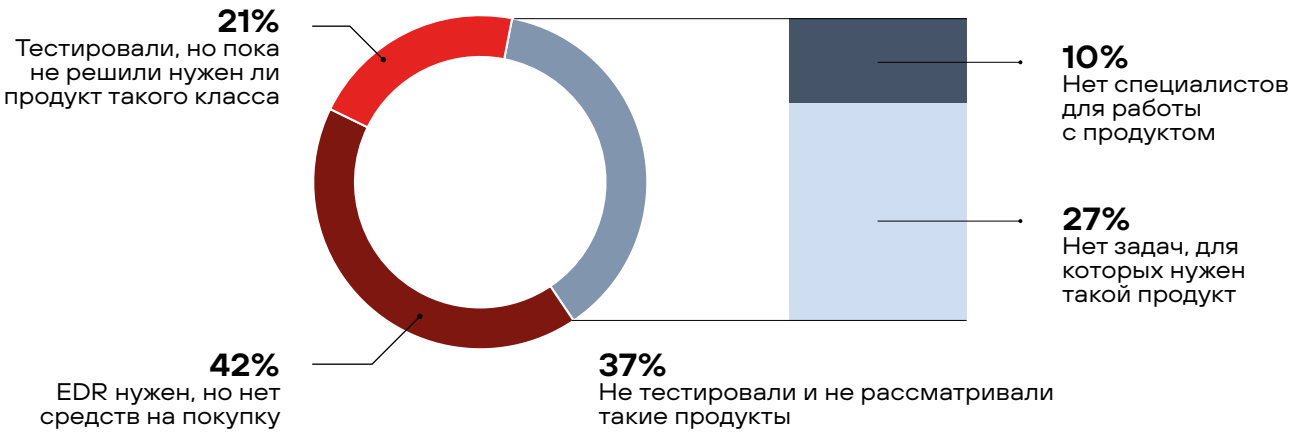

Рисунок 8. Причины отказа от покупки EDR-решений

КЛЮЧЕВЫЕ ЗАДАЧИ И СЛОЖНОСТИ

К любому средству защиты конечных устройств предъявляется масса требований. Для качественной работы нужно легкое развертывание, широкое покрытие разных типов устройств и семейств ОС, незаметная (не вызывающая нагрузки или повышения времени отклика приложений) работа для пользователя устройства, будь то ноутбук, стационарное или виртуальное рабочее место. Это же относится и к серверам, где агенты тщательно проверяются с точки зрения совместимости и нагрузки на критически важные бизнес-системы. Хорошо, когда EDR-решения можно настраивать под профиль устройства, а их архитектура дает пользователям гибкость настройки индивидуальных агентов. Это позволяет соблюсти баланс между набором необходимых функций, задачами SOC и особенностями инфраструктуры.

ГЛАВНОЙ ЗАДАЧЕЙ ПРИ ОРГАНИЗАЦИИ ЗАЩИТЫ КОНЕЧНЫХ УСТРОЙСТВ ЯВЛЯЕТСЯ ОБНАРУЖЕНИЕ И ПРЕДОТВРАЩЕНИЕ ЦЕЛЕВЫХ АТАК.

ДЛЯ КРУПНЫХ КОМПАНИЙ ВАЖНО КОНТРОЛИРОВАТЬ АКТИВНОСТЬ ПОЛЬЗОВАТЕЛЕЙ И ПОЛУЧАТЬ ДАННЫЕ О СОСТОЯНИИ УСТРОЙСТВ В ЕДИНОМ ОКНЕ.

Какие задачи наиболее актуальны для вас при организации защиты конечных точек?

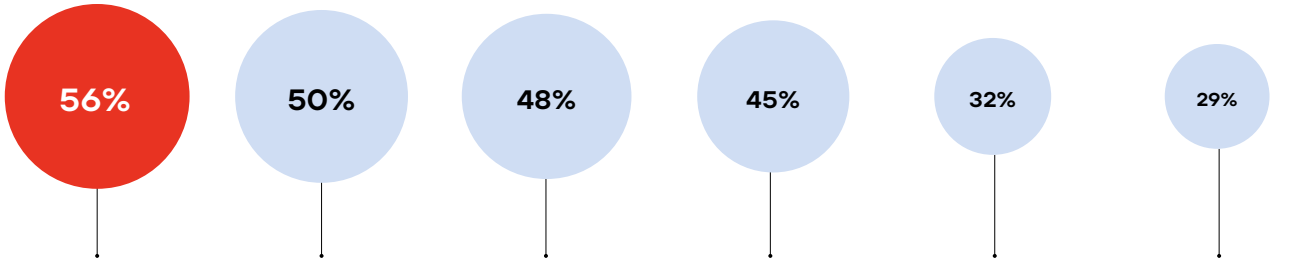

Рисунок 9. Задачи при организации защиты конечных устройств, по мнению участников исследования

С какими сложностями вы сталкиваетесь при построении защиты конечных точек имеющимися средствами?

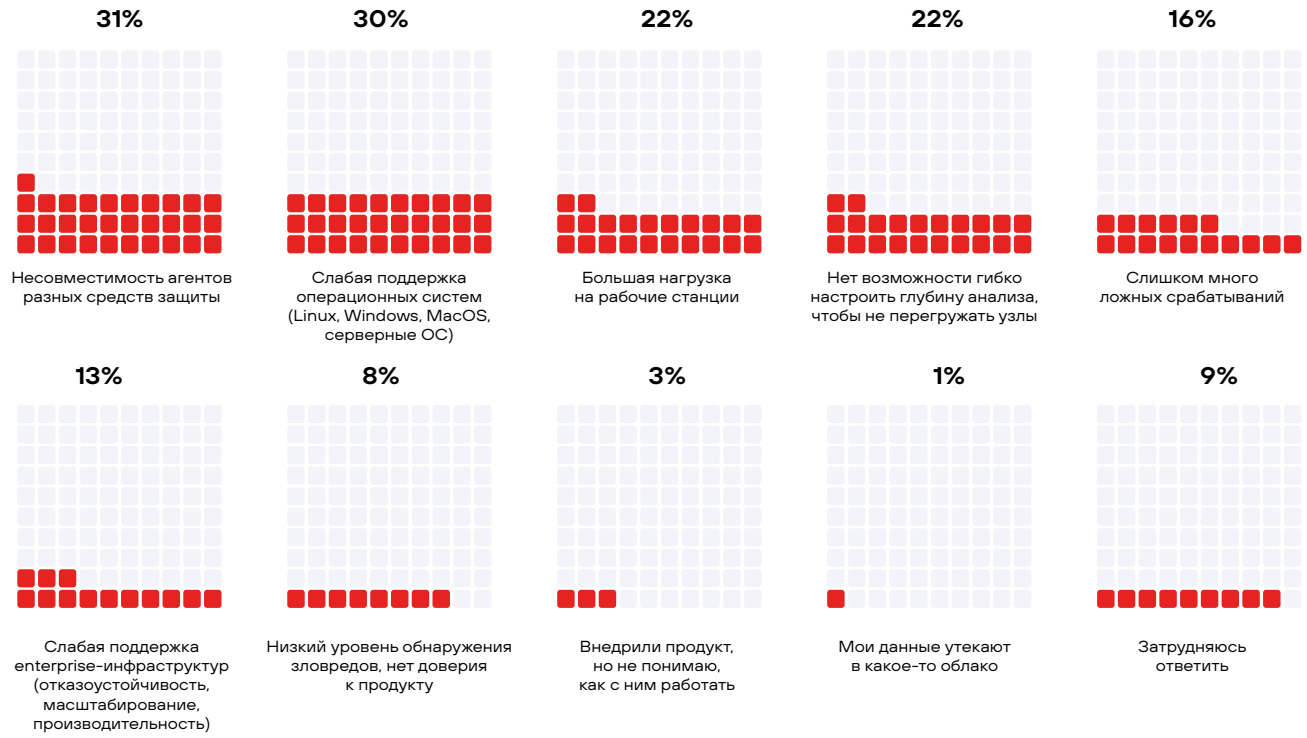

Рисунок 10. Сложности при построении защиты конечных устройств

Несовместимость агентов различных СЗИ стала ключевой сложностью для респондентов в этом году, переместившись со второго на первое место. Проблема с поддержкой ОС также получила больший приоритет (на втором месте в этом году, ранее была на пятом) и отклик у 30% респондентов.

В целом, все участники сходятся в том, что решения на устройствах не должны быть заметны конечному пользователю, не инвазивны и не приводить к каким-либо ограничениям для бизнес-процессов. Важно не только поддерживать различные операционные системы, но и достигать паритета по функциональности, например иметь те же возможность по реагированию с EDR на Windows и Linux системах.

ИНЦИДЕНТЫ И АТАКИ НА КОНЕЧНЫЕ УСТРОЙСТВА

Ясно, что компании применяют решения для защиты конечных устройств чтобы уверенно противостоять современным киберугрозам. Чем крупнее компания, тем больше инцидентов ей приходится обрабатывать — в среднем около 313 в месяц. Большинство компаний говорят о том, что конечные устройства оказываются задействованы более чем в 20% инцидентов. А среднее количество сложных атак, которые совершаются на компанию в месяц, составляет 13.

Сколько инцидентов ИБ Вы обрабатываете в месяц? (Открытый вопрос)

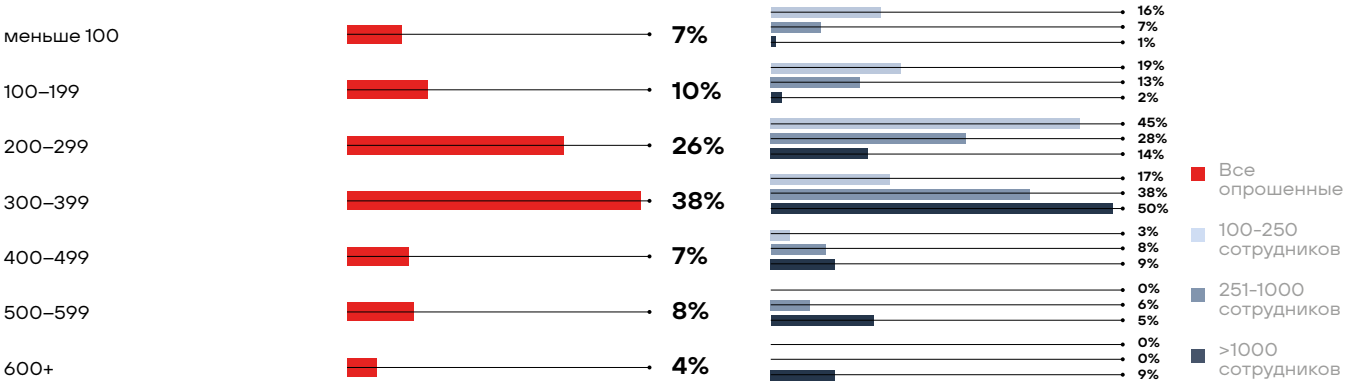

Рисунок 11. Количество инцидентов в месяц, обрабатываемое опрошенными компаниями

В каком % инцидентов были задействованы и скомпрометированы конечные устройства?

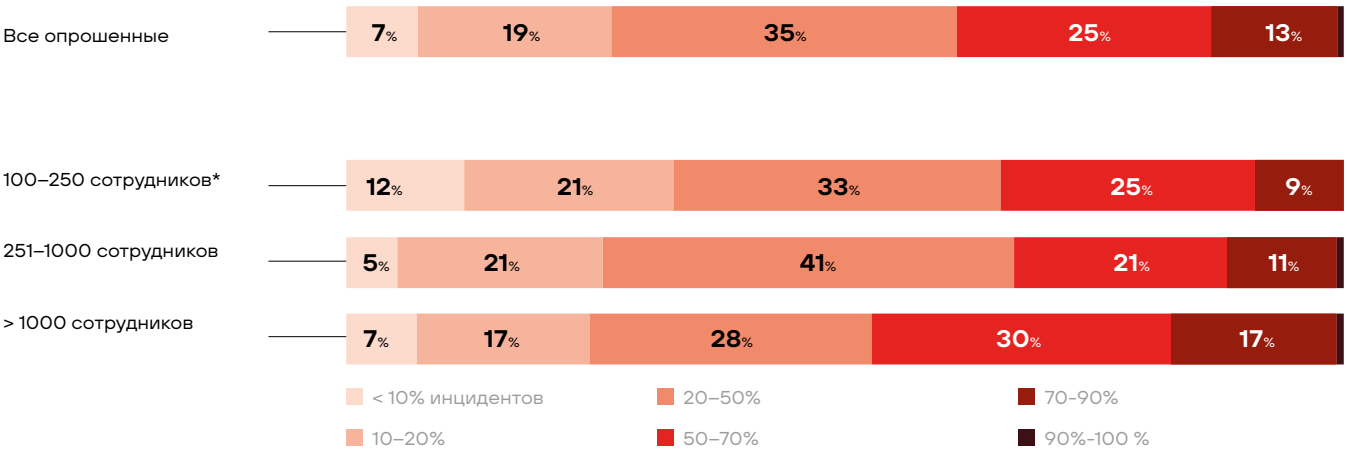

Рисунок 12. Количество инцидентов, в которых были скомпрометированы конечные устройства

Сколько сложных атак происходит в месяц в среднем? (Открытый вопрос)

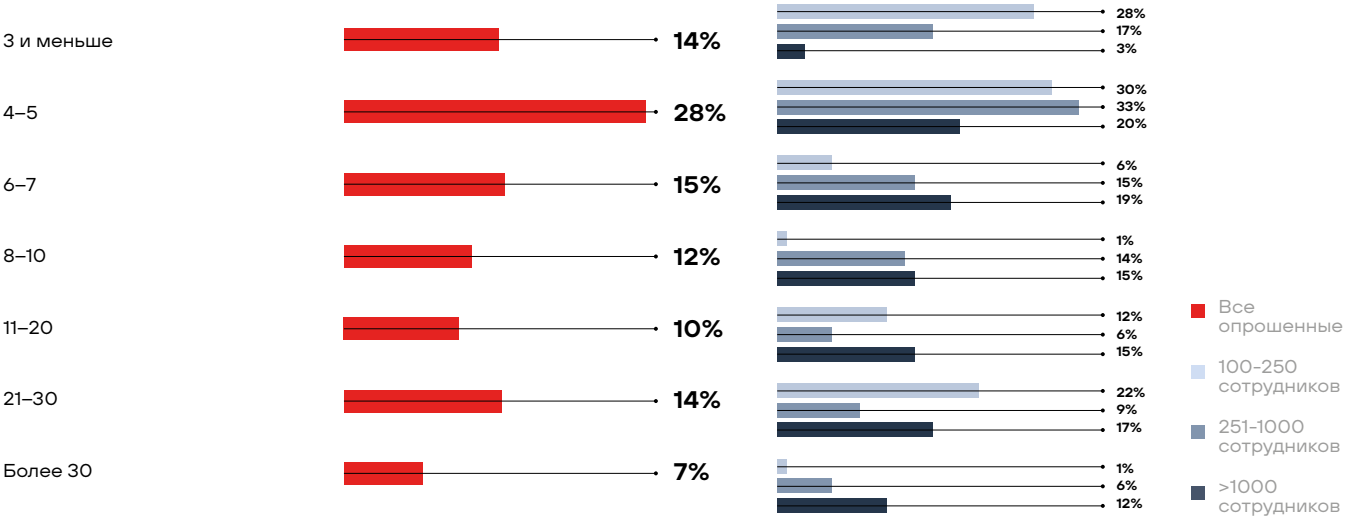

Рисунок 13. Количество инцидентов, в которых были скомпрометированы конечные устройства

Выбирая EDR-решения, компании ожидают снижения потока событий и инцидентов ИБ, желают получить инструменты для снижения числа ложноположительных срабатываний, для кастомизации системы обнаружения, добавления собственной экспертизы, а также богатый выбор действий для реагирования. Кроме того, участники исследования заинтересованы в автоматизации реагирования, позволяющей избавить аналитиков от рутинных действий, которые занимают немало времени.

Среднее время, затрачиваемое на расследование инцидента и предотвращение атаки, составляет 12 часов. Чем крупнее компания, тем больше времени она тратит.

СОТРУДНИКИ ПОЧТИ ПОЛОВИНЫ КРУПНЫХ КОМПАНИЙ (44%) ОТМЕЧАЮТ, ЧТО ОТРАЖАЮТ БОЛЕЕ 10 СЛОЖНЫХ АТАК В МЕСЯЦ.

При значительном среднем времени на расследование и предотвращение это оборачивается многими усилиями специалистов, а нередко и сторонних организаций.

Одна из ключевых задач EDR в том, чтобы для предотвращения угрозы даже на удаленном устройстве требовалось не несколько часов и командировка специалистов, а несколько кликов в интерфейсе.

Сколько в среднем времени у вас уходит на расследование инцидента и предотвращение атаки?

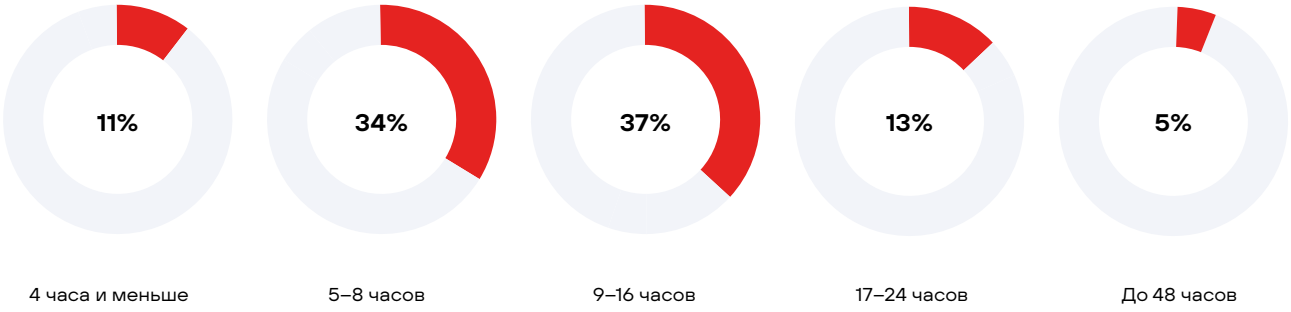

Рисунок 14. Среднее время на расследование инцидента и предотвращение атаки

Какие устройства были задействованы

Рисунок 15. Устройства, ко которые была нацелена хакерская активность

Какие действия из перечисленных вы предпринимали для расследования и предотвращения атаки?

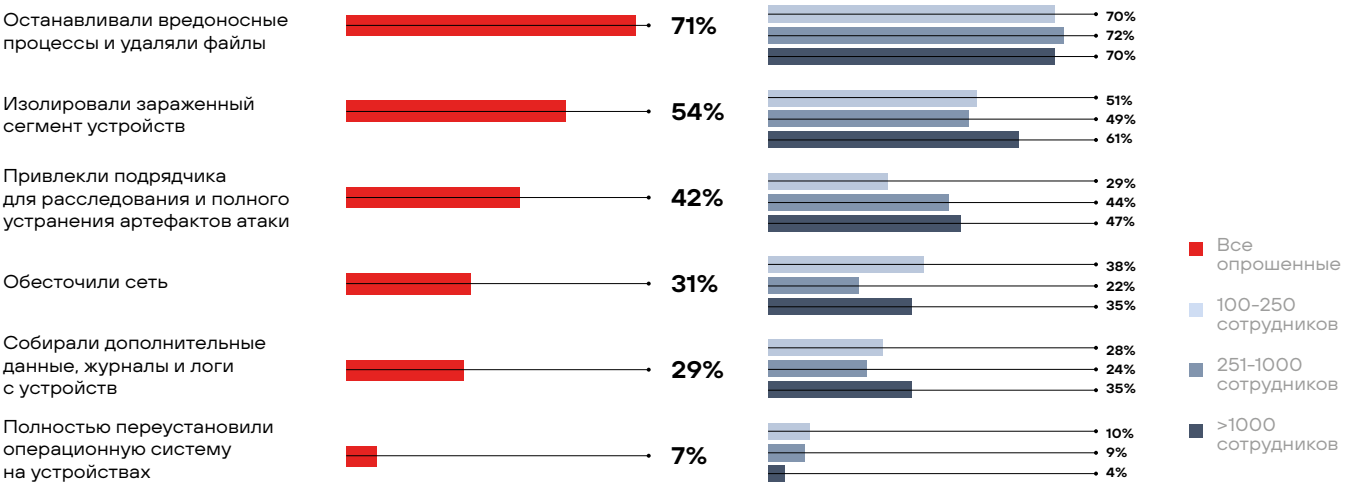

Рисунок 16. Действия, которые предпринимались для расследования инцидентов и предотвращения атак

6

Мы также спросили у респондентов, какие категории угроз они встречали в последнее время. Оказалось, что наиболее часто компании сталкиваются с шифровальщиками и атаками, связанными с цепочкой поставок (supply chain). На третьем месте оказались инциденты, возникшие по причине нарушения политик безопасности или несоблюдения регуляторных требований.

Если обратиться к модели адаптивной безопасности 6, то обнаружение и реагирование — еще не все составляющие успешного процесса. Для защиты конечных устройств также важно уметь прогнозировать и предотвращать угрозы. Поэтому к СЗИ нередко предъявляются такие требования, как возможность поиска уязвимостей, проверки корректной настройки конфигураций, патч-менеджмента и базового харденинга. В ответ на это некоторые вендоры стали придерживаться интегрированного подхода к управлению и реагированию на уязвимости (VMDR) в своих решениях.

Расскажите про последний инцидент: какой был инцидент?

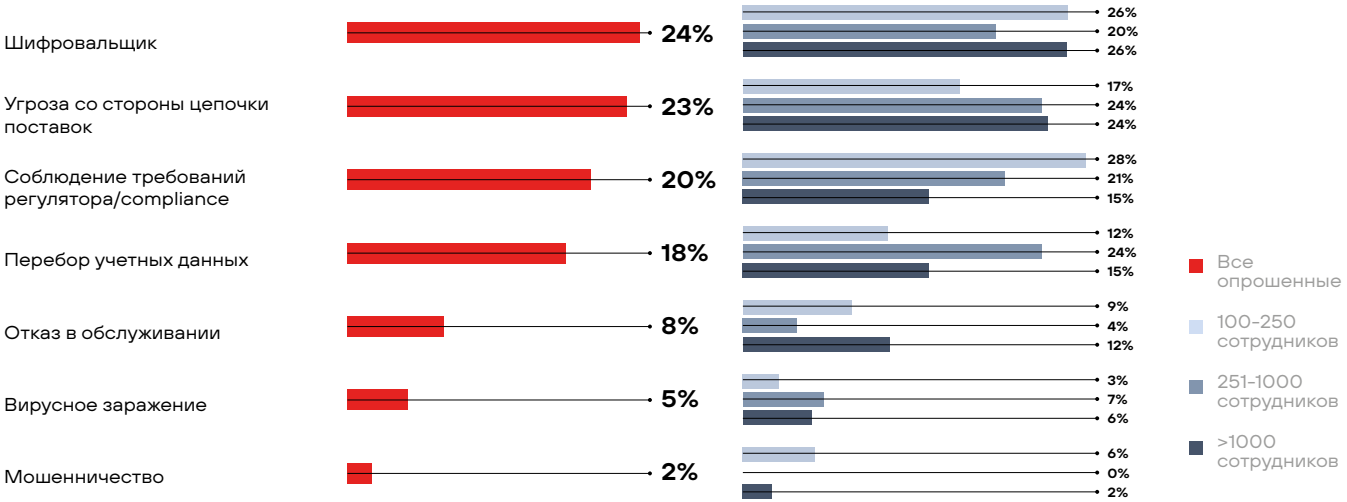

Рисунок 17. С какими угрозами был связан последний обнаруженный инцидент

КАК ПОВЫСИТЬ КАЧЕСТВО ЗАЩИТЫ КОНЕЧНЫХ УСТРОЙСТВ

Российские компании согласны с необходимостью защищать устройства сотрудников, рабочие компьютеры, серверы и виртуальные машины, но трактуют эту защиту по-разному. Большинство использует только антивирус, тогда как ландшафт угроз требует внедрения эшелонированной защиты и более продвинутых решений.

Для лучшего результата при выборе EDR-решения обращайте внимание на такие факторы, как поддержка популярных ОС, включая Linux, отсутствие чрезмерной нагрузки на конечные точки, возможность легко встроиться в гетерогенные среды и автономная работа агента. Глубина и тонкость настройки пользовательских правил и политик позволят системе гибко встраиваться в инфраструктуру компании, не нарушая привычные процессы и не расходуя ресурсы ИТ-департамента. Кроме того, важно выстроить в компании процесс threat hunting, чтобы выявлять кибератаки, которые не могут обнаружить традиционные средства защиты. Для этого необходимы продукты, которые будут собирать максимум телеметрии в своих сегментах и по возможности дополнять друг друга, обогащая информацией, необходимой для принятия качественных решений по инцидентам.

MaxPatrol EDR дает полную картину происходящего на узлах, позволяет выстроить цепочку атаки, обнаружить и моментально отреагировать на сложные современные угрозы, в том числе на атаки нулевого дня.

ГЛОССАРИЙ

Конечное устройство – физическое или виртуальное устройство, которое подключается к компьютерной сети и обменивается с нею данными.

Инцидент – нарушение или неизбежная угроза нарушения политик ИБ, политик допустимого использования или стандартных практик ИБ.

Патч-менеджмент – управление обновлениями или патчами для приложений, важный аспект кибербезопасности. Включает в себя идентификацию, получение, установку и проверку программных приложений и исправлений систем.

Сложная атака – хорошо организованная, тщательно спланированная кибератака, направленная на конкретную компанию или целую отрасль. В ходе нее злоумышленник получает несанкционированный доступ к сети, закрепляется в инфраструктуре и надолго остается незамеченным.

Endpoint Protection Platform, EPP – класс решений, предназначенный для предотвращения и блокирования известных угроз, обнаружения вредоносной активности. Имеет возможности антивирусной защиты.

Endpoint Detection and Response, EDR – класс решений, предназначенный для обнаружения и реагирования на продвинутые угрозы.

Extended Detection and Response, XDR – унифицированная платформа обнаружения и реагирования на инциденты безопасности, которая автоматически собирает и сопоставляет данные от нескольких компонентов безопасности.

Managed Detection and Response, MDR – сервис по обнаружению киберугроз, реагированию на них и расследованию киберинцидентов.

Host-based Intrusion Prevention System (HIPS) – это система защиты от вторжений на уровне отдельно стоящего узла (IP-адреса). Технология применяется в современных средствах антивирусной защиты, реализуя поведенческий анализ процессов на устройствах.