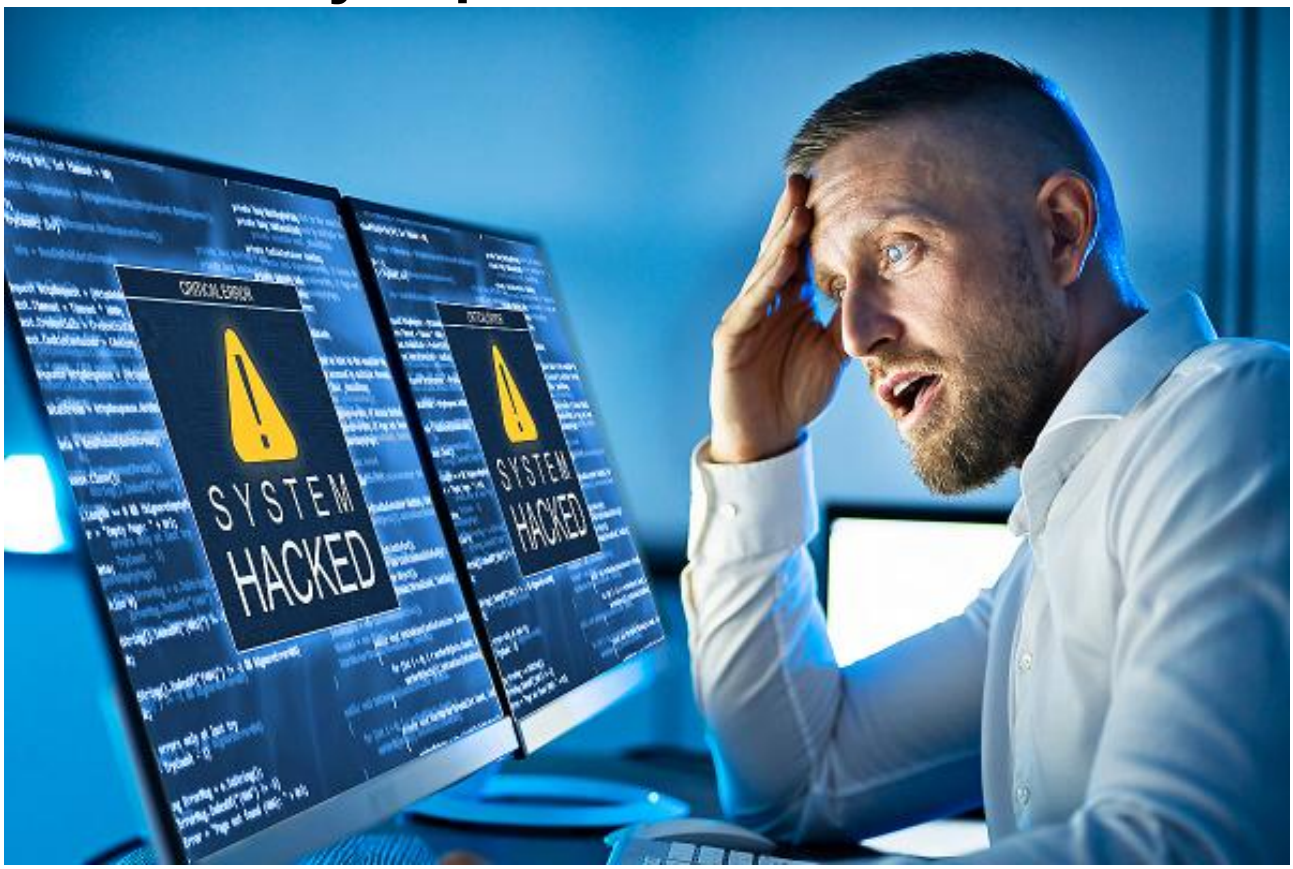
Рынок защиты конечных точек в России, Казахстане и Узбекистане уперся в потолок



Объем рынка защиты конечных точек в России, Казахстане и Узбекистане по итогам 2025 г. достиг 72 млрд руб., показав рост в 9%. Однако темпы замедляются: рынок столкнулся с фундаментальным вызовом. Существующие продукты не могут эффективно противостоять таргетированным APT-атакам, скорость которых выросла с нескольких дней до часа.

Алексей Миколенко

02.07.2026

.

Вендоры и заказчики ждут решений на базе больших языковых моделей (LLM) и ИИ-агентов, а также перехода к сервисным моделям, где оплачивается достижение параметров соглашения об уровне обслуживания (SLA), а не покупка программного обеспечения.

Защита конечных точек (Endpoint Security) - это комплексный подход к обеспечению безопасности всех устройств, которые подключаются к корпоративной сети или обмениваются данными с ней. Проще говоря, это защита точек входа: ноутбуков, смартфонов, планшетов, серверов, а в современных инфраструктурах - еще и устройств интернета вещей (IoT: умных колонок, камер, термостатов).

Сооснователь аналитической компании N4A Александр Герасимов сообщил порталу ComNews, что эксперты N4A Analytics завершили ежегодное обновление исследования рынка средств и сервисов защиты конечных точек в России, Казахстане и Узбекистане. Аналитики компании оценили объем потребления в 2025 г. в 72 млрд руб., что на 9% больше, чем в 2024 г. в сопоставимых ценах. Ожидается, что в 2026 г. рост замедлится до 5%, а объем рынка составит 75 млрд руб. Среднегодовой темп роста за период 2021–2026 гг. - 7%.

Причина замедления не только в экономике. Как отмечают авторы исследования, достижимый для существующего продуктово-сервисного предложения потенциал уже выбран. Для открытия новых рыночных ниш нужны принципиально новые продукты и сервисы.

Главный недостаток текущего предложения - поляризация. На рынке представлены две крайности: базовые конфигурации EPP (закрывают более 80% защищенных конечных точек) и полнофункциональные системы в составе SOC (около 20%). Обе конфигурации неоптимальны для отражения APT-атак, представляющих наибольшую угрозу. Александр Герасимов рассказал, что мешает вендорам и

заказчикам сдвинуть этот баланс в сторону более сложных продуктов: "Мешает высокая начальная стоимость и необходимость найма большого количества квалифицированного ИБ-персонала, что в совокупности дает такой TCO (Total Cost of Ownership - совокупная стоимость владения), который даже не все крупные компании и организации могут себе позволить. Фактически для защиты конечных точек от APT нужен полноценный SOC (Security Operations Center - это центр мониторинга информационной безопасности). А это очень дорого и сложно организационно".

Скорость развития кибератак выросла скачкообразно - с нескольких дней до менее чем часа. Атаки чаще всего нацелены на полное уничтожение корпоративных приложений и данных, включая бэкапы, а основным вектором служат конечные точки, прежде всего автоматизированные рабочие места (АРМ).

Базовые решения не позволяют даже выявить большинство APT-атак. Полнофункциональные системы в составе SOC чрезвычайно дороги, а из-за низкого уровня автоматизации и организационных проблем часто не справляются с резко возросшей скоростью атак.

Технический директор отдела продаж АО "Лаборатория Касперского" в России Евгений Бударин пояснил, что APT-атака подразумевает под собой нацеленность злоумышленника на конкретного человека или компанию: "При этом он может использовать различный вредоносный инструментарий, как массовые угрозы, так и специально разработанный инструментарий под конкретную атаку или конкретную уязвимость (0-day). Отсутствие современного антивируса на конечном узле упрощает злоумышленнику задачу и делает стоимость атаки значительно низкой. Поэтому важно использовать комплекс современных ИБ-решений для EPP, способных обеспечить максимальный

уровень автоматизированной защиты, который дает максимальную видимость происходящего на конечных устройствах. Речь идет о связке антивируса и EDR (Endpoint Detection and Response - в переводе "обнаружение и реагирование на конечных точках")".

Больная тема

Старший партнер ИТ-интегратора "Энсайн" Алексей Постригайло выделил в инфобезе самую серьезную проблему - разрыв между скоростью атаки и скоростью реакции компании: "Чаще всего злоумышленники заходят через украденные учетные данные или вредоносные вложения. Дальше они используют штатные инструменты системы, поэтому активность долго выглядит как обычная работа сотрудника. Риск усиливают компьютеры без централизованного контроля и избыточные права пользователей. Даже хороший защитный продукт здесь мало помогает, если событие заметили через несколько часов и никто сразу не изолировал устройство".

Архитектор по информационной безопасности ООО "Гетмобит" (Getmobit) Султан Салгапаров рассказал, что самая больная тема защиты конечных точек - это недостаток ресурсов: "На сравнительно слабом оборудовании дешевых тонких клиентов полноценные EDR-системы функционировать не смогут. Приходится обходиться базовыми мерами защиты вроде статически настроенных межсетевых экранов. Мы с коллегами в Getmobit дополняем эту систему элементами XDR, когда на основе телеметрии центральный сервер принимает решения и динамически управляет конечными устройствами".

Интерес к сервисной модели растет

Руководитель центра компетенций Kaspersky "Софтлайн Решения" (ГК Softline) Евгений Подмарев уже видит устойчивый рост интереса заказчиков к сервисной модели

предоставления услуг информационной безопасности: "В первую очередь это касается компаний среднего бизнеса и организаций, которым экономически нецелесообразно создавать SOC и содержать команду профильных специалистов. При этом говорить об оплате исключительно за количество отраженных атак, на мой взгляд, пока преждевременно. В информационной безопасности результат значительно шире, чем просто предотвращенные инциденты".

"К сервисной модели мы готовы, когда результат можно однозначно измерить и проверить. Платить за количество отраженных атак я бы не стал: поставщик сам определяет, что считать атакой, поэтому такая метрика легко превращается в красивый отчет. Для нас важнее время обнаружения и время изоляции зараженного устройства. Сервис также должен давать понятный разбор инцидента и фиксировать ответственность сторон. Без этого заказчик покупает обещание, которое сложно проверить после сбоя", - отметил Алексей Постригайло.

Ведущий инженер-аналитик лаборатории технологий искусственного интеллекта аналитического центра кибербезопасности ООО "Газинформсервис" Ирина Меженева отметила, что идея оплаты за результат в информационной безопасности (ИБ) выглядит привлекательно только в маркетинговых презентациях; на практике она упирается в невозможность однозначно верифицировать этот самый результат. "Если критерием эффективности сделать "количество успешно отраженных атак", то вендору выгоднее всего искусственно завышать чувствительность детекторов, что неизбежно приведет к лавине ложноположительных срабатываний и блокировке легитимных бизнес-процессов. Кроме того, для современных APT-атак конечная точка - это лишь один из этапов: если атака закрепилась и ушла вглубь сети, эндпоинт может выглядеть чистым, хотя инфраструктура уже

скомпрометирована. Переход на такие модели возможен только при наличии прозрачных, обоснованных метрик и независимого аудита, иначе это остается просто скрытой формой подписки на софт без реальной ответственности за защищенность", - подчеркнула аналитик.

Директор по развитию ООО "Сайберлимфа" (UDV Group) Максим Хараск отметил, что рынок движется в сторону сервисных моделей, но формат оплаты строго за результат, например, за количество успешно отраженных атак, пока выглядит сложным: "В такой модели может возникать слишком много спорных ситуаций: как считать результат, где проходит граница ответственности поставщика, какие инциденты учитывать, а какие нет. При этом сервисная модель уже востребована в другом формате. На базе наших решений оказываются услуги мониторинга, оповещения и дальнейшего реагирования, в том числе для технологических сетей передачи данных. В таком подходе заказчик получает не просто продукт, а работающий контур наблюдения и реагирования. Ключевым критерием здесь становится время реакции на атаку. Time to response (время до ответа) показывает, сколько времени требуется компании, чтобы перейти от выявления реальной угрозы к действиям по ее локализации и устранению. Для современных атак это критический показатель".

Руководитель направления информационной безопасности ГК "Корус Консалтинг" Олег Андреев отметил, что схема, в рамках которой бизнес платит за количество успешно отраженных атак, неоднозначна: "С одной стороны, это может быть выгодно для многих компаний, поскольку тогда пропадает необходимость содержать в штате ИБ-команду или SOC, а подрядчик предоставляет защиту как услугу и отвечает за ее качество. С другой стороны, всегда возможен сговор с атакующим, который ведет постоянные brute-force-атаки (метод подбора паролей или ключей шифрования) - тогда компании придется платить за каждый инцидент. При

этом ИБ-подрядчик будет отвечать только за каждую успешную атаку, которую он не сумел предотвратить, но вернуть упущенную прибыль или восстановить репутацию бизнесу будет трудно. Если же такой сервис был бы запущен именно в указанном виде, то логично считать основными критериями среднее время выявления атак и реагирования, а также стоимость данной услуги".

Заочно согласен

Технический директор ООО "Стахановец" Сергей Щербаков согласен с диагнозом исследования: рынок поляризован - базовые EPP-конфигурации дешевы, но не выявляют APT-атаки, а полнофункциональные SOC дороги и из-за низкой автоматизации не успевают за атаками, которые разворачиваются за час, а не за дни. "Чаще всего мы сталкиваемся с комбинированными атаками, где конечная точка - лишь точка входа, а дальше в дело вступает инсайдерский фактор: скомпрометированный или недобросовестный пользователь, действия которого классический EPP/EDR не отличает от легитимной активности, - именно на стыке защиты конечных точек и поведенческой аналитики (UBA) находится главное слепое пятно рынка", - сказал Сергей Щербаков.

Руководитель отдела экспертизы MaxPatrol EDR Positive Technologies (АО "Позитив Текнолоджиз") Валерий Слезкинцев рассказал, что быстрее всего проходят атаки с конкретной целью: "Вывод из строя целевой организации, кража конкретных данных или вымогательство. Атаки, связанные со шпионажем, подразумевают максимально долгое незаметное присутствие в сети жертвы. На время выполнения атаки влияет уровень защиты целевой организации, скорость применения обновлений безопасности и квалификация атакующих. Скорость выполнения атак растет за счет развития ИИ-технологий: стало проще генерировать код, находить векторы для

проникновения и дальнейшего распространения внутри сети и выбирать правильные инструменты для реализации кибератаки. Для киберустойчивых организаций время развития кибератаки особо не изменилось, а для компаний с неполным покрытием средств защиты информации (СЗИ), уязвимым софтом, старыми операционными системами (ОС), отсутствием парольной политики, перегруженным SOC и др. оно сократилось".