Рынок защиты конечных точек в России, Казахстане, Узбекистане: медленный рост, большой потенциал

В N4A Analytics завершена работа над ежегодным обновлением регулярного исследования рынка средств и сервисов защиты конечных точек в России, Казахстане и Узбекистане. Исследование охватывает как базовый функционал безопасности – антивирусы и другие базовые функции платформ защиты конечных точек (EPP), так и продвинутые, в том числе услуги SOC. Рассмотрены конечные точки всех видов: стационарные и мобильные автоматизированные рабочие места, сервера и конечное сетевое оборудование (CPE), устройства Интернета Вещей (IoT).

По итогам 2025 года объем потребления достиг 72 млрд руб., прирост относительно 2024 года в сопоставимых ценах составил 9%. Ожидается, что в 2026 году объем рынка вырастет на 5% в сопоставимых ценах до 75 млрд руб. Среднегодовые темпы роста рынка за период 2021–2026 гг. составят 7% с выраженной тенденцией к замедлению.

Причина замедления – не только в непростой экономической ситуации. В большей степени проблема носит фундаментальный характер: достижимый для существующего на рынке продуктово-сервисного предложения потенциал уже выбран, а для открытия новых рыночных ниш нужны принципиально новые продукты и сервисы.

Главный недостаток существующего предложения – в его поляризации. На рынке представлены только две крайности: базовые конфигурации EPP на одном полюсе, и полнофункциональные системы в составе корпоративных и/или коммерческих SOC на другом. В строгом соответствии с правилом Парето, базовые конфигурации покрывают более 80% защищенных конечных точек, а продвинутые – лишь около 20%. При этом обе конфигурации не являются оптимальными для отражения ATP-атак, представляющих сейчас наибольшую угрозу.

Опрошенные в ходе исследования эксперты были единодушны в своем мнении: скорость развития кибератак выросла скачкообразно – с нескольких дней до менее часа. При этом возросла и тяжесть последствий – в большинстве случаев атаки направлены на полное уничтожение корпоративных приложений и данных, включая бэкап, а основным вектором атаки являются как раз конечные точки. Выросла и интенсивность ATP-атак, основным вектором которых выступают конечные точки, преимущественно – автоматизированные рабочие места (АРМы).

Базовые конфигурации средств защиты конечных точек просты и удобны в использовании, не требуют квалифицированного ИБ-персонала, доступны по цене, но не позволяют даже выявить большинство ATP-атак, не говоря уже об их отражении. Способные на такое полнофункциональные системы в составе SOC не только чрезвычайно дороги, но и ввиду низкого уровня автоматизации и наличия организационных проблем зачастую не справляются с резко возросшей скоростью развития атак.

«Со стороны «упершихся в потолок» роста вендоров и со стороны организаций, испытывающих ограничения в обнаружении и сдерживании ATPатак, назрела потребность в решениях следующего поколения — с широкой автоматической оркестрацией детекции и реагирования на базе LLM и AIагентов, интегрированных с SIEM/SOAR и MDM/EDR», — отметил Андрей Новиков, эксперт по информационной безопасности.

Технически и организационно это чрезвычайно сложная задача, очевидно, требующая широкой кооперации для ее решения, а также перехода на более сложные бизнес-модели, учитывающие экономический эффект от применения средств ИБ.

Потребность в новых бизнес-моделях для вендоров широкого спектра тиражного ПО, используемого для защиты конечных точек, состоит еще и в появлении новых возможностей для внутрикорпоративной разработки, связанной с так называемым вайб-кодингом, то есть с применением LLM и AI-агентов для разработки ПО. При правильной организации вайб-кодинг

действительно позволяет кардинально снизить затраты на разработку и обеспечить высокое качества результата.

Защита конечных точек – это набор процессов. Любое ПО для процессной автоматизации требует глубокой кастомизации и довольно сложного и затратного внедрения. С этой точки зрения ПО для автоматизации ИБ-процессов ничем не отличается от ERP и BI-систем. Если и когда стоимость собственной разработки окажется ниже стоимости кастомизации и внедрения тиражного ПО, то последнее «умрет» как предмет продажи. Причем как ПО, так и программно-аппаратные комплексы (ПАКи). Продавать можно будет только готовый сервис и соглашение об уровне обслуживания (SLA), при этом организации-потребителю сервиса вообще будет не важно, что «под капотом» у этого сервиса, каким ПО достигается заданный SLA – контролироваться и оплачиваться будет результат (параметры SLA), а не средства его достижения.

Следует отметить, что защита конечных точек требует вовлечения не только специализированных средств и сервисов, но и косвенно – почти всех видов средств кибер-безопасности. Поэтому потребность в столь кардинальных изменениях ландшафта ИБ-рынка охватывает не только непосредственно рынок защиты конечных точек, но и ИБ-рынок в целом.