WAF и Anti-DDoS в России ускоряют темпы роста

В 2025 г. объем потребления WAF и Anti-DDoS в России вырос на 19% и достиг 11 млрд руб. Аналитики прогнозируют ускорение роста сегмента до 25% CAGR в 2026-2028 гг. за счет роста числа облачных приложений, развития fintech и e-commerce, а также усложнения атак. Потенциал дополнительного роста рынка они оценивают в 7 млрд руб. ежегодной выручки.

Анна Швецова (mailto:Shvetsova@comnews.ru)

26.01.2026

Об этом ComNews рассказал сооснователь аналитической компании N4A Александр Герасимов. По предварительным оценкам N4A, потребление продуктов и сервисов WAF и Anti-DDoS в России выросло на 19% по сравнению с 2024 г. и достигло 11 млрд руб. "Это почти в пять раз меньше, чем объем крупнейшего сегмента рынка сетевой безопасности - средств защиты периметра, достигшего в 2025 г. 47 млрд руб. В целом соотношение один к пяти соответствует распределению объема хранимых и обрабатываемых корпоративных данных между пользовательскими устройствами внутри локальных периметров и публичными и частными дата-центрами", - сказал Александр Герасимов.

При этом он отметил, что пространство для импортозамещения в сегменте было небольшим: на протяжении многих лет в сегменте WAF и Anti-DDoS были сильны позиции российских разработчиков, в отличие от сегмента средств защиты периметра. "Примечательно, что лидирующие позиции российских разработчиков не были продиктованы регуляторными преференциями, а некоторые из них успешны и на зарубежных рынках", - также отметил Александр Герасимов.

Он объяснил, что в сегменте WAF и Anti-DDoS превалирует облачная модель предоставления и подписочная модель монетизации - причем не только у глобальных игроков, но и у ведущих российских. Преимущества таких моделей - эластичность и возможность оплаты по фактическому потреблению. "В отличие от средств защиты периметра, объем сегмента WAF и Anti-DDoS сформирован в основном потоком рекуррентных платежей. Это выгодно потребителям, для которых характерен постоянный рост нагрузки на онлайн-приложения. Также это повышает устойчивость бизнеса провайдеров", - объяснил Александр Герасимов.

N4A ожидает ускорения темпов роста сегмента с 19% в 2025 г. до 25% CAGR в период 2026-2028 гг. В целом потенциал прироста сегмента в России N4A оценивает в 7 млрд руб. ежегодной выручки, причем большую часть этого потенциала можно будет монетизировать в ближайшие годы при минимальной доработке существующего продуктово-сервисного предложения.

Среди факторов роста Александр Герасимов назвал увеличение количества приложений в облаках и рост нагрузки на них. Главный драйвер - устойчивый рост бизнеса fintech и ecom.

Другой фактор - рост потребностей в защите из-за усложнения атак на онлайн-ресурсы. "Обычный Anti-DDoS, работающий на уровне L4, уже перестал справляться - провайдерам Anti-DDoS пришлось идти на уровень логики приложений (L7). В результате фактически произошло слияние Anti-DDoS и WAF в единый сервис защиты онлайн-приложений, - пояснил Александр Герасимов. - По мере формирования цифровых экосистем активно развивается и функционал защиты API, так называемый WAAF, а многие провайдеры добавляют функции защиты облачных нагрузок в стандартное предложение WAF/Anti-DDoS".

Что думает рынок

Прогнозируемый среднегодовой темп роста мирового рынка оценивается в 15%, отметил директор Ideco (ООО "Айдеко") Дмитрий Хомутов. В России значительная часть сервисов, по-прежнему не обеспечена достаточным уровнем защиты, поэтому Дмитрий Хомутов считает, что тут темп роста будет более высоким.

Многие ИБ-эксперты, опрошенные ComNews, считают, что основной драйвер роста сегмента WAF и Anti-DDoS - увеличение количества и сложности атак. А по мере цифровизации критически важных сервисов увеличивается и потенциальный ущерб от подобных инцидентов, обратил внимание Дмитрий Хомутов.

"Самый важный драйвер роста - изменение характера угроз. Массовые L4-атаки не единственный сценарий, и бизнесу приходится защищаться на уровне логики приложений, API и пользовательских сценариев. Это автоматически тянет за собой рост потребления более сложных, а значит, и более дорогих сервисов защиты", - считает руководитель отдела технического пресейла IT TASK (ООО "АйТи Таск") Михаил Тимаев.

Также эксперты подтвердили, что все больше компаний используют приложения, из-за чего увеличивается спрос на их защиту. "Чаще всего веб-приложение опубликовано для доступа не только локально, но и в интернете. За период III квартал 2024 г. - III квартал 2025 г. в 1,7 раза возрос уровень бот-активности. Также в 2025 г. рост вредоносного трафика составил 70%, в 2023 г. - 50%, злоумышленники автоматизированно анализируют технологии и перебирают известные уязвимости для получения несанкционированного доступа. Мы знаем успешные случаи подобных атак, и поэтому WAF, как последний барьер обороны, не теряет актуальности" , - объяснил менеджер по развитию UserGate WAF (ООО "Юзергейт") Виталий Абрамович.

Также эксперты отметили, что меняется отношение бизнеса к простоям. "Даже кратковременная недоступность онлайн-сервиса сегодня напрямую конвертируется в финансовые и репутационные потери", - отметил проджект-менеджер MD Audit (SL Soft FabricaONE.AI, акционер - ГК Softline) Кирилл Левкин. При этом растет критичность онлайн-каналов для основной выручки бизнеса. А руководитель отдела сетевых технологий Angara Security (ООО "Ангара Секьюрити") Денис Бандалетов считает, что атаки стали не только более сложными, но и более "бизнес-ориентированными" - с фокусом на простой сервисов, API и клиентские веб-приложения.

Также среди факторов роста рынка эксперты назвали регуляторные изменения, в том числе приказ ФСТЭК России от 11.04.2025 №117, который утвердил новые требования к защите информации, содержащейся в государственных информационных системах и других информационных системах госорганов, предприятий и учреждений. На это обратил внимание руководитель отдела прикладных систем Angara Security Алексей Варлаханов.

Также в целом российские решения стали зрелыми и могут сравниться по функционалу и эффективности с западными, что повышает осведомленность заказчиков и сформировало устойчивый спрос, считает коммерческий директор

компании "Код безопасности" (ООО "Код Безопасности") Федор Дбар.

Среди других причин роста сегмента руководитель направления информационной безопасности "Онланта" (ООО "Онланта") Дмитрий Заболотный назвал подорожание услуг и лицензий в этой области, глубину проникновения и рост средней стоимости владения (за счет того, что заказчики все чаще выбирают комплексную услугу управления, что дороже, и за счет сложности интеграции в комплексную платформу безопасности компании).

Дмитрий Хомутов утверждает, что потенциал импортозамещения в данном сегменте во многом уже реализован - примерно на 70%. Но говорить о полном исчерпании этого потенциала преждевременно, считают опрошенные ComNews представители ИБ-компаний. Например, Михаил Тимаев отметил, что остались узкие ниши, где зарубежные решения пока востребованы - как правило это сложные международные инфраструктуры или специфические требования корпораций.

Часть опрошенных ComNews представителей ИБ-компаний подтвердили, что российские решения в сегментах Anti-DDoS и WAF уже достаточно зрелые. "В целом они сопоставимы с зарубежными аналогами по базовой функциональности и устойчивости к массовым атакам. За последние годы отечественные вендоры существенно усилили экспертизу, улучшили качество фильтрации и адаптацию под локальный ландшафт угроз", - сказал Денис Бандалетов.

Но российские решения продолжают уступать ведущим зарубежным вендорам по ряду параметров - в частности, по широте функциональности и показателям производительности, отметил Дмитрий Хомутов. Об этом также говорили и другие эксперты, опрошенные ComNews. Но при этом, по словам Дмитрия Хомутова, они уже способны обеспечивать необходимый уровень защиты.

"Это связано с большим проектным опытом и более долгим развитием зарубежных продуктов, но тем не менее российские продукты лишены устаревших технологий и поддержки legacy. Также за рубежом довольно большой сегмент средств защиты информации представлен в виде ПАК, в российском сегменте он гораздо уже", - сказал бизнес-партнер по инновационному развитию компании "Гарда" (ООО "Гарда Технологии"), участник рабочей группы ООН по управлению данными Лука Сафонов.

Виталий Абрамович утверждает, что отечественные решения с каждым годом приближаются к паритету по базовому функционалу, но набор функций действительно отличается. Из положительного - в них нет лишнего. "Зачастую из-за

уровня зрелости зарубежные решения включают избыточный функционал, с которым работает узкий круг лиц, или технологии, которые пока не используются массово. Это подтверждают эксплуататоры отечественных компаний", - сказал Виталий Абрамович.

При этом Виталий Абрамович отметил, что у многих заказчиков на данном этапе находится несколько решений: зарубежное и российское - тем самым они осуществляют плавный переход. В целом, по его мнению, отечественные решения вскоре полностью заместят зарубежные.

"Потенциал массового волнового замещения западных коробочных продуктов и облачных сервисов в корпоративном и государственном сегментах действительно близок к исчерпанию. Основной объем клиентов, для которых это было критически важно, уже перешел на отечественные решения", - считает Дмитрий Заболотный. По его словам, ниши, где зарубежные решения сохраняют присутствие, обусловлены не их превосходством, а спецификой. Например, российские компании с развитым международным бизнесом, чьи инфраструктуры вплетены в глобальные облачные и сетевые сервисы, могут сохранять элементы зарубежных решений на периферии или в иностранных юрисдикциях.

Сессия о сетевой безопасности состоится в рамках Форума "Территория Безопасности 2026: все pro ИБ (https://www.comnews-conferences.ru/ru/conference/tb2026)" 2 апреля 2026 года в Москве. Это — ежегодное новаторское мероприятие, состоящее из четырех конференций и выставки отечественных технологий ИБ.

Обсуждение