14 мая 2025

Дружба побеждает: для чего нужна совместимость решений по кибербезопасности от разных вендоров

До 80% корпоративных заказчиков сталкиваются с проблемой несовместимости используемых решений по кибербезопасности. Российские вендоры стремятся построить закрытые экосистемы, намеренно ограничивая совместимость с другими производителями, обращают внимание эксперты. О том, как можно обеспечить интеграцию разных решений при построении комплексной системы защиты, – в материале RSpectr.

ИНСТРУМЕНТ КОНКУРЕНЦИИ

Заместитель главы ГК «Гарда» Рустэм Хайретдинов в своем посте в VK подчеркнул, что «самая большая боль крупных корпоративных клиентов – несовместимость используемых ИБ-решений». По его мнению, вендоры намеренно ограничивают совместимость своих продуктов с продуктами других производителей.

«Это делается для того, чтобы продавать собственные решения такого класса, – так называемый экосистемный подход, когда качество второго и последующих продуктов менее приоритетно, чем удобство его интеграции с первым», - прокомментировал RSpectr Рустэм Хайретдинов.

Это, по его мнению, эффективный инструмент конкуренции – именно из-за бесшовной интеграции покупатели выбирают посредственные по качеству и неоправданно дорогие продукты Apple, а из-за легкости переноса данных и настроек – регулярно обновляют их.

Рустэм Хайретдинов, ГК «Гарда»: «Альтернативой экосистемному является подход best of breed, подразумевающий покупку лучших в своем классе решений, но в этом случае покупатель сам занимается их интеграцией».

Он обратил внимание, что сегодня все без исключения российские средства защиты информации выходят на рынок без поддержки других решений.

«Даже те ИБ-продукты, которые должны по своей архитектуре взаимодействовать с другими решениями, например SIEM, «из коробки» не поддерживают все решения других производителей», - отметил эксперт.

Масштаб озвученной проблемы действительно велик, прокомментировал RSpectr инженер по информационной безопасности «Рексофт» Александр Осмехин.

Александр Осмехин, «Рексофт»: «Причин много, от проблем с финансированием (в этом случае аппаратные комплексы или ПО поставляются с несколько иными характеристиками и часто с внедрением множества дополнительных организационных мер) до технической реализации требований уже на стороне заказчика».

Как рассказал RSpectr директор по развитию ИИ и веб-технологий Artezio (группа «ЛАНИТ») Сергей Матусевич, проблема несовместимости ИБ-решений действительно является одной из наиболее острых в корпоративном сегменте.

По его оценке, около 70-80% крупных заказчиков сталкиваются с ней при построении комплексных систем защиты. При этом разработчики стремятся построить закрытые экосистемы, где клиент будет вынужден приобретать все продукты одной линейки.

Сергей Матусевич, Artezio: «Ситуация усугубляется тем, что ни один российский вендор сейчас не может предложить полностью завершенное комплексное решение, которое покрывало бы все аспекты ИБ на уровне лучших мировых практик».

Компаниям, по его словам, приходится комбинировать решения разных производителей. Как правило, они сталкиваются с технической несовместимостью, проблемами интеграции и высокими затратами на адаптацию.

«В некоторых случаях стоимость интеграционных работ может достигать 30-40% от общей суммы внедрения. Это серьезные затраты, которые ложатся на плечи заказчиков и значительно увеличивают совокупную стоимость владения системами безопасности», – отметил эксперт.

Сергей Матусевич уточнил, что крупные компании вынуждены тратить до десятков миллионов рублей на интеграцию несовместимых решений.

Ведущий архитектор по информационной безопасности MONS (ГК «КОРУС Консалтинг») Елена Скалозубова перечислила RSpectr наиболее проблемные классы ИБ-решений:

- SIEM-системы (анализ событий безопасности) – данные из одной системы сложно передать в другую;
- DLP-системы – разные форматы метаданных и протоколов;

- средства криптозащиты (СКЗИ) – несовместимость сертифицированных модулей;
- антивирусы и EDR/XDR – конфликты сигнатур и механизмов мониторинга.

Решать эти вопросы можно с помощью открытых API и стандартов обмена, использования промежуточного ПО (интеграционные шины, конвертеры данных), а также внедрения стандартов ФСТЭК, если они будут детализированы.

Елена Скалозубова,
Ведущий архитектор по информационной безопасности MONS (ГК «КОРУС Консалтинг»)

ПОЙТИ НА КОНТАКТ

Большинство крупных компаний предпочитают не класть все яйца в одну корзину, отметил в беседе с RSpectr эксперт по комплексным проектам информационной безопасности STEP LOGIC Владимир Арышев. Он уверен, что бизнес не хочет строить моновендорную инфраструктуру, чтобы не зависеть от одного производителя.

Данная концепция, по его мнению, противоречит интересам вендоров, которые стремятся расширить свое присутствие в инфраструктуре заказчиков за счет экосистемного подхода и глубоких интеграций собственных продуктов между собой.

Владимир Арышев, STEP LOGIC: «Производители охотно идут на кооперации только с технологическими партнерами, которые могут увеличить продажи, – к примеру, интеграция решений для удаленного доступа и многофакторной аутентификации».

По мнению заместителя генерального директора по инновационной деятельности «СёрчИнформ» Алексея Парфентьева, ИБ-решения редко принципиально несовместимы между собой.

«Чаще всего при их создании используются универсальные технологические стандарты передачи, хранения и обработки данных – протоколы Syslog, NetFlow, SSH и другие, напомнил он RSpectr. С их помощью можно «подружить» системы между собой даже без помощи вендора. Могут встречаться и проблемы, например, несовместимости двух Endpoint-based-решений драйверного уровня. Но такие моменты обычно считаются разработчиком багом, а не доработкой, поэтому по желанию заказчика исправляются довольно оперативно», - пояснил Алексей Парфентьев.

«Мы как разработчик экосистемы ИБ-решений не видим проблемы несовместимости. Потому что всегда идем на контакт с другими вендорами, даже из конкурирующих областей», – сообщил он.

Алексей Парфентьев, «СёрчИнформ»: «Наш опыт показывает, что коллеги всегда открыты к сотрудничеству: за более чем сотню реализованных совместимостей только один вендор прохладно отреагировал на предложение о взаимодействии».

Масштаб проблемы несовместимости ИБ-продуктов преувеличен, поделился с RSpectr глава цифровой платформы «Ракета» Дмитрий Кривошеев. Как правило, интеграция между продуктами построена на API, что позволяет программам сторонних вендоров интегрироваться в экосистему, напомнил он.

Дмитрий Кривошеев, «Ракета»: «Многие молодые вендоры не задумываются об интеграции со сторонними производителями. Основной способ преодолеть такую проблему – это открытое API, которое описывает методы взаимодействия с продуктом».

Оптимальный способ решения проблемы: необходимость предоставления вендорами API для своих решений.

API предоставляет возможность двусторонней интеграции, что упрощает взаимодействие, соглашается руководитель направления «Бизнес-автоматизация» SimbirSoft Виктория Реутская. Но, по ее мнению, просто наличие API в ИБ-решении не решит всей проблемы, потому все методы должны быть правильно документированы и описаны.

Виктория Реутская, SimbirSoft: «Если вендоры будут использовать данный интерфейс для работы, то это позволит в будущем создать максимально универсальные коннекторы для самой распространенной связи ИБ-решений».

РЕГУЛЯТОР КАК МЕТОДОЛОГ

Решение проблемы совместимости ИБ-решений требует скоординированных усилий государства, бизнеса и научного сообщества, подчеркнул в беседе с RSpectr руководитель департамента аудита, консалтинга и оценки соответствия «Кросс технолоджис» Антон Исупов.

Антон Исупов, «Кросс технолоджис»: «Усилия следует направить на разработку и введение госстандартов и обязательных к исполнению нормативно-правовых актов, повышение квалификации разработчиков, развитие технологических платформ и организацию независимых центров тестирования и сертификации».

Руководитель группы защиты инфраструктурных ИТ-решений «Газинформсервис» Сергей Полунин напомнил, что мировой опыт показывает, что жесткое регулирование в этом вопросе не работает.

Он добавил, что формализация стандартов всевозможных протоколов архитектур на международном рынке производится с помощью механизма RFC (Request for Comments).

Сергей Полунин, «Газинформсервис»: «Специалисты публикуют и редактируют эти стандарты, а вендоры сами решают, делать все в соответствии ними или принять риски, что твое решение будет инновационным, но не совместимым со своими «соседями»».

«Чтобы требования к стандартизации не замедляли выход новых решений и не привели к формализму со стороны вендоров, они должны быть унифицированы и понятны, а также следует использовать открытые стандарты и протоколы», - настаивает руководитель группы аналитики и исследований департамента консалтинга «Инфосистемы Джет» Александр Морковчин. И регулятор в этом случае, по его словам, может выступить как центр компетенций и методолог.

Александр Морковчин, «Инфосистемы Джет»: «Обязательная же и жесткая совместимость ИБ-решений может быть полезна для отдельных сегментов рынка: прежде всего для критической инфраструктуры, где риски особенно высоки».