КАК НАЛАДИТЬ БЕСПЕРЕБОЙНУЮ РАБОТУ ИНФРАСТРУКТУРЫ В НОВЫХ УСЛОВИЯХ

КОНСТАНТИН САВЧЕНКО

Растерянность на рынке, связанная с уходом иностранных ИТ-компаний и поисками российских аналогов недоступных решений, постепенно проходит. Одни заказчики решают свои задачи путем точечного замещения оборудования или ПО для закрытия первоочередных потребностей, другие смотрят в сторону параллельного импорта. Но необходимость подобрать аналог — это только вершина айсберга. Все чаще возникают вопросы о замещении технологических стеков и обеспечении совместимости внутри этих стеков, а также проведении грамотной миграции данных при переходе на российский софт. С подобными проблемами сталкивается большинство компаний — как коммерческих, так и государственных. Помочь протестировать и наладить совместимость различных ИТ может решение «Демосфера».

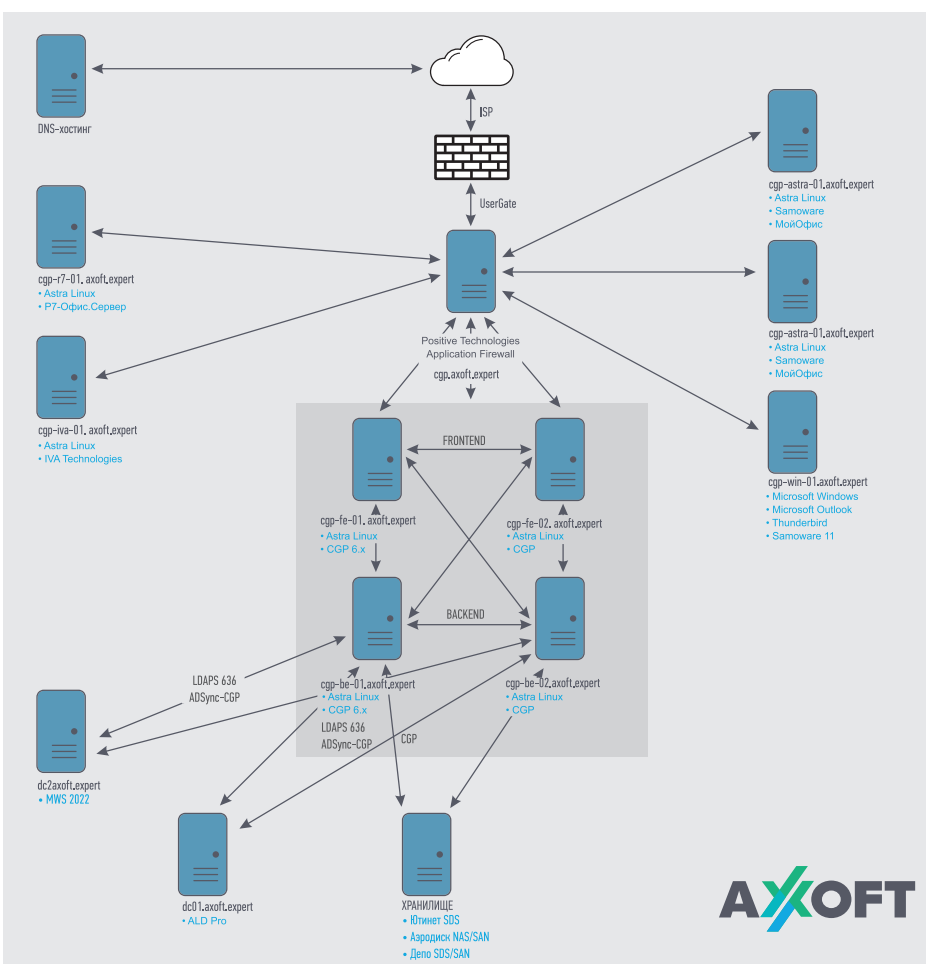

РИС. 1. ▲ Сценарий демонстрации решений

Сегодня перед многими компаниями довольно остро стоит вопрос оперативного перехода на отечественное ПО и обеспечение информационной безопасности. Для решения таких задач требуется комплексный индивидуальный подход, который базируется в первую очередь на экспертизе и технологическом сотрудничестве основных участников ИТ-рынка. На основе этих принципов компания Axoft разработала сервис «Демосфера». Это виртуальное пространство, в котором представлены технологии российских разработчиков как для управления инфраструктурой (ОС, офисные пакеты, коммуникационное ПО, виртуализация, облачные технологии), так и для обеспечения кибербезопасности (SIEM, NGWF, WAF, сканеры безопасности и т. д.). На виртуальном стенде можно протестировать отдельные сервисы, приложения, а также целые стеки решений, и увидеть, как взаимодействуют различные системы, включая ПО и серверное оборудование.

КАК ВСЕ УСТРОЕНО

Инфраструктура — сердце любого бизнеса, поэтому важно грамотно подобрать конфигурацию решений, чтобы обеспечить отказоустойчивость системы. В «Демосфере» развернут базовый прототип, который включает операционные системы, прикладные офисные программы,

почтовый сервер, LDAP-сервер, базы данных и сервер видеоконференцсвязи. Рассмотрим один из самых популярных запросов, с которым к нам приходят, — замена экосистемы Microsoft Exchange + AD+ Teams.

У нас уже есть готовый сценарий демонстрации решений (рис. 1), который на практике может выглядеть так:

1. Разворачиваем отказоустойчивый кластер CommuniGate из четырех серверов на ОС Astra Linux.
2. Подключаем серверы CGP к системе хранения данных Huawei. Подключение к серверам контролируется UserGate NGFW и балансируется через PT Application Firewall.
3. Запускаем синхронизацию CommuniGate с Active Directory.
4. Тестируем синхронизацию с ALDPro.
5. Настраиваем групповую работу с документами в CGP на базе Р7-Офис.
6. Создаем автоматизированное рабочее место пользователей на базе отечественных ОС (Astra, RedOS, BasAlt, Rosa) с прикладным офисным ПО (Мой Офис, 1С, Abby), антивирусом Kaspersky и почтовым клиентом Samoware, подключенным к CGP.
7. Настраиваем интеграцию CGP с Telegram для коммуникации в чатах.
8. Устанавливаем и настраиваем ВКС Iva.
9. Проводим миграцию баз данных с MS SQL Server на PostgrePro.

Это лишь один из доступных сценариев. С помощью инженеров в виртуальном пространстве можно тестировать совместимость самых разных решений. Платформа обладает гибкостью, есть возможность подключать новые продукты и сервисы. Таким образом, каждый может подобрать уникальное сочетание инструментов, которое подойдет для решения конкретных бизнес-задач.

«У компании уже есть успешно реализованные проекты по переходу на российские инфраструктурные решения. Один из последних — внедрение коммуникационной платформы CommuniGate Pro Центром информационных технологий Волгоградской области. Реализация проекта длилась полгода и была разбита на два этапа. Сперва инженеры устанавливали и настраивали ПО под инфраструктуру и задачи заказчика, а затем производили миграцию пользователей на новую почтовую систему», — отмечает Юлия Хвостова, руководитель отдела технического консалтинга и инженерной поддержки Axoft.

БЕЗОПАСНОСТЬ ПРЕЖДЕ ВСЕГО

Обеспечение информационной безопасности на данный момент является приоритетом на федеральном уровне. Отечественную защиту стремятся внедрить не только госсектор и объекты критической информационной структуры, но и коммерческий сектор. Бизнес стремится избавиться от иностранных решений, позволявших избегать киберугроз. Один из частых запросов в сфере сетевой безопасности — миграция с Palo Alto, Cisco, Fortigate.

Благодаря большому опыту специалистов компании Axoft в обеспечении кибербезопасности и широкому портфелю решений, в «Демосфере» можно не только увидеть работу продуктов и возможность их совмещения с другими системами, но и отыграть различные сценарии, например обнаружение фишинговой атаки (рис. 2), построенный следующим образом:

1. Атакующий формирует фишинговое письмо.
2. Письмо проходит через разные эшелоны защиты:
   - KSMG — почтовый шлюз с возможностью проверки на вредоносное ПО, фишинг, спам;
   - CGP — MDA;
   - UserGate — NGFW с включенной системой обнаружения вторжений;
   - ПК с установленной ОС Astra Linux и Агентом EDR от Kaspersky.
3. PT Network Attack Discovery (PT NAD) проводит поведенческий анализ сетевого трафика.
4. KATA осуществляет динамический анализ.
5. Происходит отправка событий в SIEM с настроенными правилами.

«По нашему мнению, сегодня невозможно обойтись без решений, которые консолидируют данные об инцидентах, связанных с ИТ и информационной

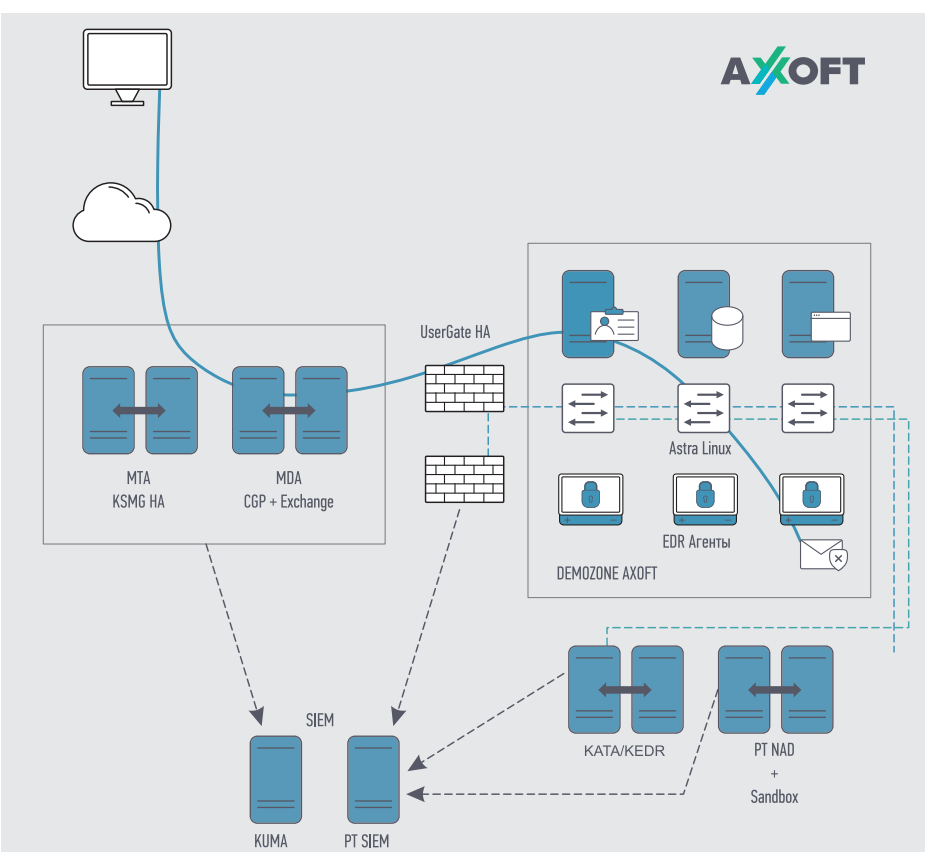

РИС. 2. Сценарий обеспечения информационной безопасности

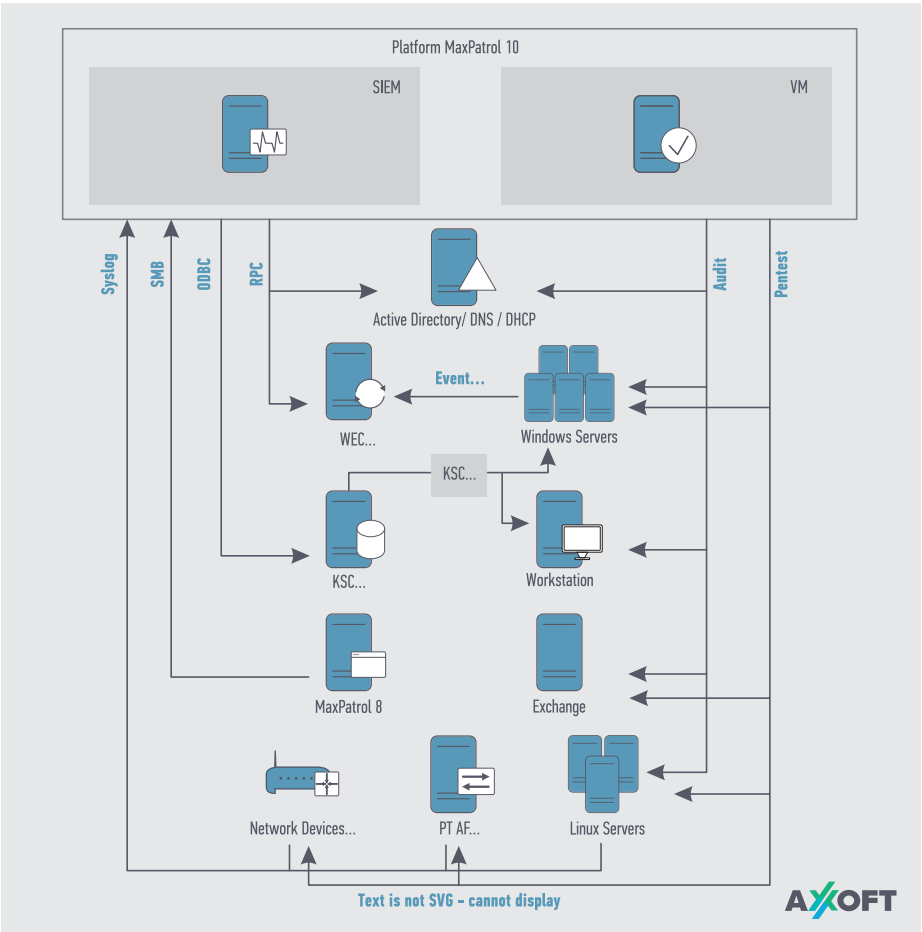

РИС. 3. ▲ Сценарий использования Active Directory

безопасностью. К примеру, у нас развернута система мониторинга и анализа событий обеспечения кибербезопасности на базе MaxPatrol SIEM, поэтому аналитики могут наблюдать за уязвимостями в онлайн-режиме и своевременно на них реагировать. При этом с помощью средств SIEM можно обнаружить угрозы на узлах, на которые сложно или невозможно установить дополнительные средства защиты», — дополняет Денис Фокин, руководитель отдела консалтинга и инженерной поддержки направления по информационной безопасности Axoft. Например, вот несколько сценариев для Active Directory (рис. 3):

- Обнаружена неудачная попытка входа от имени отключенной или несуществующей учетной записи.
- Обнаружено обращение к общим ресурсам узла (например, ADMIN$, C$, IPC$).
- Обнаружена смена логина учетной записи (объекта в Active Directory) на логин, не содержащий символа $ в конце.
- Обнаружена выгрузка списка доменных (локальных) пользователей или групп пользователей.

ЗАКЛЮЧЕНИЕ

Представленные сценарии — малая часть примеров комплексного подхода к импортозамещению в ИТ-инфраструктуре и информационной безопасности. На рынок все чаще выходят новые системы, серверное, аппаратное оборудование, которое мы стремимся сразу испытывать на совместимость с другими решениями в «Демосфере». Работа отдельных продуктов сегодня мало кому интересна — важно видеть, как эти инструменты взаимодействуют между собой, можно ли будет построить работающую экосистему и встроить ее в существующую инфраструктуру максимально безболезненно. Только через технологическое партнерство, взаимодействие со всеми участниками ИТ-рынка, постоянное совершенствование методологий и разработку новых, собственных инициатив мы можем достичь позитивной динамики в продвижении к импортонезависимости. ⬣