McAfee Data Exchange Layer

Простая интеграция приложений в рамках модели «один ко многим» и мгновенный обмен данными

McAfee DXL изменит динамику работы вашей системы безопасности

Ускорение рабочих процессов жизненного цикла защиты от угроз
Практически мгновенный обмен информацией и координирование задач позволяют значительно сократить время, затрачиваемое на обнаружение, сдерживание и устранение выявленных новых угроз.

Сокращение задержек, облегчение и упрощение интеграции защитных продуктов различных производителей
Наша открытая платформа позволит вам объединить защитные продукты различных производителей с вашими собственными приложениями и инструментами без необходимости согласования с производителями. Вы обрели свободу выбора.

Повышение ценности развернутых вами приложений
Теперь приложения могут обмениваться генерируемыми ими полезными данными об угрозах и немедленно выдавать рекомендации и предпринимать контрмеры.

Теперь предприятия и разработчики могут легко объединять приложения, обмениваться данными и координировать задачи по обеспечению безопасности всех приложений, используя систему интеграции приложений в режиме реального времени. Новый открытый пакет средств разработки программного обеспечения (SDK) позволяет упростить процесс интеграции, снизить уязвимость и сократить время задержек, которые сказываются на эффективности мер по обеспечению кибербезопасности.

Все это напоминает уплату своеобразного «налога на интеграцию». Интеграция в рамках модели «один к одному», создание скриптов вручную и планирование процессов — наиболее распространенные методы интеграции приложений, используемые отделами информационной безопасности и их поставщиками. Эти методы не способны предоставить необходимой эффективности, точности и быстроты, которые требуются специалистам по кибербезопасности для достижения максимальной производительности. Они ограничивают возможности обмена информацией об угрозах, расследования инцидентов и реагирования на атаки.

Что же мешает? До сих пор в отрасли безопасности не существовало простого и безопасного способа осуществлять непрерывный обмен данными в режиме реального времени.

- Инфраструктура безопасности и ИТ создавалась в течение многих лет на базе разрозненных технологий от разных производителей и собственных приложений.
- Интеграция отдельных продуктов по API-интерфейсу занимает много времени и легко нарушается при установке новых версий продуктов и переходе на новые форматы данных.
- Для интеграции двух защитных продуктов необходимо, чтобы два поставщика обсудили, согласовали и внедрили соответствующие решения.
- Такие традиционные модели как опросы и плановая публикация данных вызывают дополнительные задержки при каждом обмене.

Открытый стандарт и единая экосистема

Есть лучший способ, который постепенно становится открытым отраслевым стандартом в рамах инициативы Открытый уровень обмена данными Open Data Exchange Layer (OpenDXL). Целями инициативы OpenDXL являются повышение гибкости интеграции, упрощение интеграционных процессов и предоставление новых возможностей для разработчиков, а также повышение эффективности операций по обеспечению безопасности в организациях, где развернуто

данное решение. В рамках первой фазы инициативы OpenDXL предоставляется пакет средств разработки программного обеспечения (SDK), который позволит новым разработчикам и участникам получить расширенный доступ к уровню обмена данными McAfee Data Exchange Layer (DXL) и полноценно использовать его, что обеспечит экспоненциальный рост ценности интеграции или развертывания DXL.

Разработчики будут использовать пакет SDK для создания и интеграции приложений, работающих через коммуникационную систему DXL, что является безопасным способом в реальном времени координировать данные и действия в разнообразных приложений различных производителей, а также в приложениях собственной разработки. Такой подход позволяет нам избежать многократно повторяющихся процессов интеграции каждого продукта в отдельности.

Рис. 1. DXL — это модель высокоскоростной интеграции и коммуникационная система, работающая в реальном времени.

Приложения просто публикуют темы сообщений и подписываются на них или запрашивают службы DXL в режиме запрос-ответ подобно API-интерфейсам RESTful. Система мгновенно передает сообщения и запросы, объединяя инфраструктуру безопасности, ИТ и собственные решения в единую четко работающую систему.

С момента выхода DXL на рынок в 2014 году в эту экосистему были интегрированы десятки решений различных поставщиков. Предприятия, поставщики услуг и государственные учреждения уже используют ее для оптимизации процесса принятия решений и сокращения времени реагирования на угрозы. Использование системы позволяет снизить эксплуатационные расходы, оптимизировать процессы обеспечения защиты и реагирования на инциденты, а также освободить ценных специалистов по безопасности от выполнения ручных операций и проведения тактических учений.

Интеграция — одна на всех!

В отличие от традиционной интеграции, каждое приложение устанавливает связь с универсальной коммуникационной системой DXL. Таким образом процесс интеграции, предусматривающий ранее несколько операций, сводится к однократному действию. OpenDXL будет поддерживать целый ряд языков, позволяя разработчикам создавать интеграционные

решения в предпочитаемых ими средах разработки. Если одно приложение публикует сообщение или запрашивает службу, то одно или несколько приложений получают такое сообщение или отвечают на запрос службы. Взаимодействие осуществляется независимо от собственной архитектуры каждой интегрируемой технологии, что является целью любого стандарта. Такое абстрагирование от индивидуальных API-интерфейсов и требований отдельных поставщиков намного упрощает интеграцию.

В дополнение к интеграции в рамках системы DXL, разработчики могут также настроить свои службы на взаимодействие с DXL или настроить API-интерфейс коммерческого продукта на публикацию данных в DXL. Другие службы могут прослушивать сообщения и запросы DXL, что позволяет им расширить свою функциональность за счет новейших данных или принять необходимые меры защиты. В целях более тщательной настройки с учетом специфики приложения такие действия могут быть объединены в единый скрипт, способный вызвать целый каскад или выполняемый одновременно пакет действий.

На предприятиях развертывание стандартизированного уровня интеграции и обмена информацией осуществляется посредством установки небольшого клиента DXL на каждом узле и одного DXL-посредника, который будет управлять обменом сообщениями. Весь DXL-трафик осуществляется только в рамках внутренней сети предприятия, сохраняя конфиденциальность данных и оперативный контроль. Модель с поддержкой брандмауэра сохраняет соединение между клиентом и сервером, обеспечивая непрерывный доступ к новейшей информации, осуществляемый через DXL. Если что-либо меняется в самом публикующем или принимающем приложении, уровень абстракции DXL изолирует остальную сеть от этих изменений, снижая риски и затраты на обслуживание интеграционных решений.

Улучшенное ядро кибербезопасности

Доступ к ранее недоступным типам данных «вплоть до последней минуты» меняет правила игры в сфере безопасности. Ваши специалисты по анализу, реагированию и сотрудники отделов эксплуатации с нетерпением ждут возможности получать данные, анализировать и реагировать на них в самые кратчайшие сроки. Ваши поставщики и разработчики были бы рады помочь, но интеграция может завязнуть в трясине технических сложностей или обязательств вашего поставщика перед своими деловыми партнерами.

Теперь все эти препятствия исчезли, вернув вам контроль над ситуацией и свободу выбора.

Отныне успеху ваших операций по обеспечению безопасности будут способствовать такие данные как:

- события, вызванные угрозами мошенничества;
- изменения репутации файлов и приложений;
- обнаруженные мобильные устройства и активы;
- изменения в поведения пользователей и сети;
- высокоточные оповещения;
- данные об уязвимостях и признаках взлома.

Поставщикам программного обеспечения и решений следует воспринимать систему DXL как мощный механизм, ускоряющий работу отделов безопасности и ИТ и открывающий новые возможности в их программных продуктах и организациях их клиентов. Новые типы данных будут способствовать более комплексную анализу данных. Его выводы дадут возможность немедленно принимать надлежащие меры, такие как эскалация запросов, сдерживание, устранение или блокирование атак. Если рассматривать систему DXL с точки зрения обмена данными в режиме реального времени и практически безболезненной интеграции процессов, то нельзя не увидеть открывающиеся новые возможности.

Чтобы начать работу, перейдите на сайт **www.mcafee.com/ru/solutions/data-exchange-layer.aspx**.

McAfee. Part of Intel Security.
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной»,
Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.intelsecurity.com