ОБЗОР РЕШЕНИЯ, IDC

Оценка преимуществ, обеспечиваемых решениями по безопасности ЦОД на основе SDN

При поддержке: Cisco

Пит Линдстром (Pete Lindstrom) Ричард Л. Вилларс (Richard L. Villars)
Мэтью Марден (Matthew Marden)
18 мая 2015 г.

Обзор

Основная цель любой компании состоит в том, чтобы повышать качество обслуживания заказчиков и улучшать бизнес-результаты. Для этого необходимы ресурсы ЦОД, которые способны обрабатывать самый разный контент, проводить аналитику больших данных и архивировать информацию в рамках решения общих задач по хранению данных и получению аналитических выводов. Необходимо расширять существующие ЦОД, ускорять строительство новых центров в новых регионах, а также использовать весь потенциал современных, передовых ЦОД, проектируемых, создаваемых и управляемых поставщиками услуг. В терминологии компании IDC такое преобразование бизнеса и ЦОД называется «переходом на третью платформу».

Сегодня буквально все инновации в сфере бизнеса основаны на третьей платформе. Благодаря ей деловой мир может пользоваться сотнями тысяч и даже миллионами невероятно полезных, революционных решений и услуг, способных существенно повысить удобство работы конечного пользователя. Такое изменение касается всех составляющих деятельности ИТ-отдела, включая операции закупки, проектирования, эксплуатации, разработки и управления данными и ресурсами в долгосрочной перспективе. Среда нового центра обработки данных более динамична и способна обрабатывать больше данных, но таит в себе большие риски для бизнеса, которые необходимо учитывать и преодолевать. Таким образом, архитектура сети нового поколения становится критически важным компонентом.

Эта новая архитектурная модель должна решать проблемы технологических и эксплуатационных ограничений традиционных сетевых архитектур и соответствовать требованиям ЦОД к обработке рабочих нагрузок для третьей платформы. Так, например, программно-определяемая сеть (SDN), которая характеризуется разделением уровня управления сети и уровня передачи данных, обеспечила сети адаптивность и гибкость, необходимые организациям для создания сред облачных вычислений.

Инфраструктура Cisco ACI, ориентированная на приложения, помогает удовлетворить потребность операторов ЦОД в автоматическом выделении ресурсов, программируемом управлении и комплексной оркестрации. Вместо того чтобы отделять уровень управления от уровня передачи данных, инфраструктура ACI применяет модель политик, разработанную для учета требований приложений и автоматизации развертывания в сети, для всех приложений – как виртуализированных, так и выполняемых без ОС. Такой подход Cisco называет «декларативной моделью управления» – это означает, что отдельные люди и агенты могут сотрудничать и сообщать свои цели на условиях выполнения взаимных обязательств. Эти цели могут быть вполне абстрактными: например, политика приложений может содержать требования, а базовая инфраструктура (например, коммутаторы ЦОД) должна определить, как лучше всего удовлетворить эти требования, исходя из имеющихся возможностей.

Еще один вариант сети для облачных вычислений предоставляется OpenStack. Для пользования сетевыми сервисами заказчикам предлагается стандартная архитектура Neutron, а также набор северных и южных API-интерфейсов. Эта модель имеет гибкую модульную архитектуру, то есть каждый заказчик может выбирать, какое устройство лучше всего ему подходит. Некоторые заказчики сначала внедряют эталонную модель, а затем добавляют в нее расширения в зависимости сценариев использования и требований своей сети.

Основные факторы, влияющие на изменение ЦОД

Эксплуатация ЦОД и объем инвестиций в него прямо или косвенно зависит от множества внешних факторов. Они делятся на три группы: коммерческие, культурно-социальные и технологические.

- **Коммерческие факторы.**
  - **«Все как услуга».** Модели финансирования физических и цифровых ресурсов меняются, что приводит к реструктуризации внутреннего бюджетирования, затрат и методов инвестирования.
  - **Дигитализация отрасли.** В результате перехода от физической бизнес-модели к цифровой значительно повысилась скорость роста данных, требования к производительности и функционалу ИТ.
  - **Сложность бизнеса.** Расширение экосистем компаний приводит к необходимости стандартизации способов взаимодействия и обмена данными между организациями и отраслями.
- **Культурно-социальные факторы.**
  - **Нормативы использования данных.** Требования к сбору, хранению и использованию персональных данных и интеллектуальной собственности как со стороны физических лиц, так и государственных учреждений, стали быстро меняться и перестали быть единообразными.
  - **Неправомерное использование данных.** Корпорации, организованные преступники и целые государства официально стали на тропу кибервойны.
  - **Взаимодействие с заказчиками.** Социальные сети создают среду для прямого взаимодействия заказчиков друг с другом и с бизнесом, а это, в свою очередь, приводит к постоянной потребности в самой последней, актуальной информации.

- **Технологические факторы.**
  - **Модульная ИТ-структура.** Облачные, конвергированные, программно-определяемые и гипермасштабируемуемые пакетные модели меняют методы закупки основных ИТ-позиций и управления ими.
  - **Плотность данных.** Данных, используемых для взаимодействия с заказчиками и анализа коммерческой деятельности, становится все больше. Растет потребность в их сборе и хранении в центрах обработки данных поставщиков услуг.
  - **Быстрое изменение ИТ-потребностей.** В связи с потребностью в ИТ-поддержке краткосрочных мобильных кампаний и аналитических проектов компаниям приходится покупать, разворачивать или переориентировать ресурсы в срочном порядке и на непродолжительное время.

Такая реорганизация и изменение баланса ЦОД и ИТ-ресурсов также значительно влияет и на существующие глобальные сети организаций. Организациям приходится менять имеющиеся способы подключения, чтобы обеспечить связь внутренних ЦОД с ресурсами сторонних поставщиков. Кроме того, необходимо учитывать значительные изменения объема трафика и его разнообразие, так как предприятия будут менее предсказуемо перемещать большие объемы информации между большим числом местоположений.

Роль информационной безопасности в современном ЦОД

Основным фактором, лежащим в основе вышеупомянутых изменений и быстро растущих рабочих нагрузок ЦОД, становится потребность в большей адаптивности и гибкости в том, что касается обеспечения безопасности ЦОД. Для каждого сценария использования безопасность означает что-то свое – целостность, точность, мониторинг или управление контентом и данными. ИТ-отделам необходима общая платформа, которую они могли бы использовать для быстрой и надежной настройки, перенастройки и использования широкого спектра функций безопасности в ЦОД и во всей организации.

На уровне сети встраиваемая функциональность безопасности включает возможности мониторинга (обнаружение вторжений), сегментации с учетом политик (межсетевые экраны) и шифрование для защиты каналов связи (виртуальные корпоративные сети). Однако предприятия зачастую рассматривают ресурсы ЦОД как единое целое, не делая различий между уровнями использования или риска. При таком подходе все ресурсы предприятия сосредотачиваются в одной большой «зоне», а защита ориентирована на точки входа и выхода на периметре сети (иногда их также называют «северными» и «южными» точками доступа в ЦОД).

По мере своего роста ЦОД превращаются в наборы разноплановых ресурсов, предоставляющих функции для разных подразделений, пользователей и платформ. Однако при этом должна совершенствоваться и безопасность – защита этих ресурсов от новых угроз. Предприятиям необходимо задуматься о том, как обеспечить безопасные способы обмена ресурсами, а также мониторинг и шифрование каналов связи на еще более тонком уровне.

Для современного ЦОД необходимо определить, как развернуть системы обнаружения и предотвращения вторжений и как сегментировать межсетевые экраны. Без этого невозможно выбрать, куда переносить средства управления и требуются ли новые функции для защиты внутренних коммуникаций между серверами и другими ресурсами. В частности, нужно выбрать небольшой набор ресурсов (обычно на уровне приложений, но возможны и другие разграничения) и добавить новые средства мониторинга и управления политиками, чтобы лучше контролировать трафик между приложениями.

Чем больше средств управления разворачивается в ЦОД, тем настоятельнее становится потребность в их централизации. Так как местоположение и использование ресурсов, которые необходимо защищать, становятся все более динамичными, функции безопасности должны адаптироваться к новым архитектурам.

Этот обзор решения подготовлен компанией IDC по результатам опроса пользователей, связанных с продуктами безопасности для ЦОД в новых условиях. Здесь приводятся данные о том, каких преимуществ позволяют достичь эти решения, в частности: повысить производительность ИТ-персонала на 33,5 %, снизить время незапланированных простоев из-за угроз и нарушений безопасности на 80,7 % и ускорить развертывание средств безопасности для новых приложений и услуг на 63,5 %. В организации с 1000 пользователей повышение надежности за год может принести 48 700 долл. США, увеличение эффективности труда ИТ-персонала – 71 700 долл. США, а увеличение времени эффективной работы за счет оптимизации производственных операций – 92 600 долл. США.

Преимущества решений по безопасности центров обработки данных нового поколения для бизнеса

Решения по безопасности для ЦОД нового поколения должны максимально повышать эффективность инвестиций в ЦОД. Таким образом, эти решения по безопасности должны основываться на политиках, быть интегрированными, надежными, адаптивными и масштабируемыми. Разработанные и внедренные с учетом всех этих требований, решения по безопасности создают ценность, позволяя экономить время и усилия, затрачиваемые на управление и инициализацию решений по безопасности, уменьшать последствия угроз для производства и бизнеса и гарантировать, что обеспечение безопасности никак не повлияет на скорость поддержки и осуществления бизнес-операций со стороны ЦОД. Таким образом, эти решения по безопасности обеспечивают следующие возможности ЦОД.

- **Интеграция с целью повышения эффективности и снижения риска.** Продукты по обеспечению безопасности, которые интегрируются как с решениями, поддерживающими традиционные среды ЦОД организаций, так и с другими продуктами по безопасности, используемыми в среде ЦОД нового поколения, позволяют сэкономить время и снизить риски. Это обусловлено несколькими причинами. Во-первых, интеграция ускоряет изменение политик. Во-вторых, помогает отказаться от неэффективных разрозненных решений. В-третьих, она сокращает время, в течение которого угрозы безопасности могут затронуть услуги и приложения.

- **Упрощение для снижения затрат на управление.** Продукты по безопасности в ЦОД нового поколения развертываются в средах со значительными возможностями автоматизации и оркестрации. Чтобы адаптироваться в такой среде, продукты по безопасности также должны быть основаны на политиках и иметь возможность предоставлять выделение ресурсов как услугу. Это нужно не только для того, чтобы работала новая архитектура ЦОД, но и чтобы специалисты по ИТ-безопасности могли работать эффективнее и тратить меньше времени на развертывание, конфигурацию и настройку вручную.
- **Надежные возможности для минимизации последствий угроз безопасности.** Продукты по безопасности в ЦОД нового поколения должны защищать весь трафик – входящий, исходящий и внутренний. Это нужно, чтобы угрозы безопасности меньше затрагивали пользователей и бизнес – сотрудники смогут дольше работать с максимальной эффективностью, а компания сведет к минимуму свои простои.
- **Адаптивность и масштабируемость для поддержки бизнеса с использованием приложений.** ЦОД нового поколения сконфигурированы так, чтобы компании могли быстрее разрабатывать свои приложения и управлять ими с меньшими затратами. Для этого необходимо, чтобы продукты безопасности можно было развертывать быстро и по мере необходимости, максимально сокращая срок вывода приложений и услуг на рынок.

Ориентированная на приложения архитектура Cisco ACI

Программно-определяемые сети отделяют функции уровня управления от уровня передачи данных. Обычно их описывают узкоспециализированными терминами. В основе программно-определяемой безопасности лежит философия архитектуры программно-определяемых сетей, однако ее возможности шире благодаря интеграции с большим количеством сред. Звездообразная топология программно-определяемой сети объединяет вместе контроллер (здесь определяются и оцениваются политики безопасности) и узлы (то место, где политики применяются). Все это происходит динамически, в реальном времени. Политики абстрагированы до уровня приложений; благодаря этому их можно точно применять к нужному узлу – с нужной гибкостью и в зависимости от нужных компонентов. Такая архитектура безопасности проста и удобна в управлении и помогает достичь максимальной эффективности.

Ориентированная на приложения инфраструктура Cisco разработана с учетом двух важнейших потребностей ЦОД: безопасности и работы с данными. Всей этой инфраструктурой управляет контроллер APIC. Он следит за всеми устройствами обеспечения безопасности ЦОД, как физическими, так и виртуальными, и обеспечивает соответствие этих устройств ресурсам, которые они должны защищать. Он может выделять ресурсы и управлять сетью и устройствами безопасности Cisco, поддерживать экосистему сторонних поставщиков решений по безопасности и расширять возможности для дополнительной поддержки сторонними поставщиками.

Поскольку Cisco ACI совместима с той архитектурой безопасности, которая уже есть в организации, она позволяет сохранить все установленные физические средства безопасности. При этом в ней есть более функциональные средства управления для физических и виртуальных машин, которые защищают важнейшие внутренние коммуникации. Для работы с динамическими ресурсами можно создавать политики. Они сопоставляются с профилями приложений, а затем развертываются по всей среде. Таким образом, если потребуется перенести ресурс в другое место, вместе с ним будет перенесена и политика.

Многие организации уже вложили значительные средства в решения Cisco по безопасности и имеют утвержденный набор действующих политик безопасности. Таким компаниям ACI позволяет надежно и безопасно расширить архитектуру ЦОД вместо того, чтобы полностью ее изменять. В то же время ACI может удовлетворить современные требования виртуализированных и распределенных архитектур и одновременно обеспечить безопасность предприятия на должном уровне.

Преимущества решений по безопасности центров обработки данных нового поколения для бизнеса в количественном выражении

В таблице 1 представлены количественные оценки преимуществ, которые организации смогут достичь за счет использования решений по безопасности в ЦОД нового поколения, по данным настоящего исследования IDC.

На рисунке 1 показано, какую прибыль от повышения производительности труда может получить организация с 1000 пользователей от развертывания решения для безопасности в ЦОД нового поколения.

ТАБЛИЦА 1

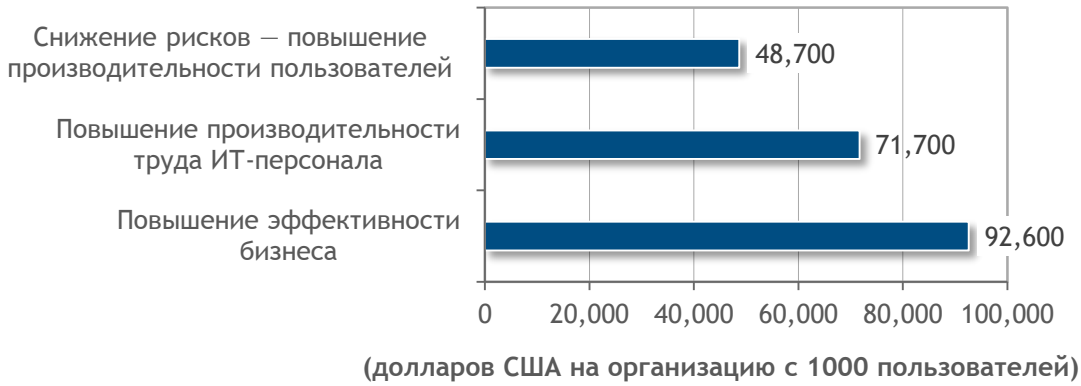
Преимущества, связанные с использованием продуктов по обеспечению безопасности в центрах обработки данных нового поколения

	(%)
Повышение производительности труда ИТ-персонала	
Сокращение времени на управление системой безопасности	33,5
Увеличение числа предварительно обнаруживаемых угроз	50,9
Уменьшение времени реагирования на угрозы	82,1
Снижение рисков — повышение производительности пользователей	
Сокращение незапланированных простоев	80,7
Повышение эффективности бизнеса	
Сокращение времени на развертывание систем безопасности	63,8

Источник: IDC, 2015 г.

РИСУНОК 1.

Типовое ежегодное улучшение показателей для организации с 1000 пользователей, применяющей решения по безопасности в ЦОД нового поколения



Источник: IDC, 2015 г.

Приложение. Методология

Данные, представленные в настоящем документе, обобщены компанией IDC по результатам опроса организаций, использующих решения по безопасности для ЦОД. В целях упорядочения результатов они выражены в долларовом эквиваленте для средней организации, имеющей 1000 пользователей. Для количественной оценки преимуществ, связанных с работой ИТ-персонала, показатели сэкономленного времени и эффективности были умножены на среднюю годовую зарплату, равную 100 000 долл. США. Для вычисления показателей по сэкономленному времени и производительности труда других сотрудников в расчет бралась годовая зарплата в 70 000 долл. США.

О компании IDC

International Data Corporation (IDC) — крупнейшая компания в сфере исследований рынка, консультационных услуг и организации мероприятий для рынков информационных технологий, телекоммуникаций и потребительских технологий. Она помогает ИТ-специалистам, руководящему персоналу и инвесторам принимать обоснованные решения о приобретении технологий и бизнес-стратегии. Свыше 1100 экспертов IDC анализируют возможности отраслей и технологий более чем в 110 странах по всему миру. В течение 50 лет IDC публикует результаты своих стратегических исследований, чтобы помочь своим клиентам достичь их ключевых бизнес-целей. IDC является дочерней компанией IDG — лидера рынка в области информации, исследований и событий, связанных с высокими технологиями.

Международная штаб-квартира

5 Speen Street
Framingham, MA 01701
USA
+1 508 872-8200
Twitter: @IDC
idc-insights-community.com
www.idc.com