Андрей Тимошенков, Консультант по решениям безопасности, IBM Russia/CIS
13 февраля 2013г.

Обеспечение безопасности в “облаках”

Решения компании IBM

Содержание

- Что волнует бизнес
- Проблемы безопасности в «облаках»
- Какие решения мы готовы предложить
- Контакты

Какие проблемы безопасности в этой области?

- Сегодня организации сталкиваются с задачей внедрения новых сервисов для бизнеса при этом с сильно ограниченными бюджетами. Многие организации выбирают облачную модель, чтобы получить преимущества, включая уменьшение затрат и перевод расходов из капитальных в операционые. Другие преимущества , такие как масштабируемость, гибкость и эффективное использование человеческих и технологических ресурсов так же кажутся привлекательными.
- Однако, облака могут представлять потенциальные риски для безопасности и конфиденциальности бизнеса. Эти проблемы являются основной причиной замедления темпов внедрения облачных технологий в организациях.
- Защита высоко виртуализированных сред от целевых атак и угроз, обеспечение безопасной совместной работы пользователей и защиты данных (изоляция, совместное исользование), быстрый провижнинг и де-провижнинг (пользовательских и технических компонентов) и недостача прямого контроля параметров безопасности и конфиденциальности являются основными растущими проблемами безопасности облаков.

Какие проблемы безопасности в этой области?

- Кроме того, в IBM проанализировали множество клиентских облачных проектов и определили следующие основные требования безопасности:
  - Governance, Risk and Compliance (GRC)
  - Identity Management
  - Data Security
  - Intrusion Prevention
  - Virtualization Security
  - Patch Management

Как IBM может помочь?

IBM предлагает обширный и проверенный портфель решений, чтобы помочь клиентам с обеспечением безопасности облака, включая следующие продукты для решения наиболее частых задач клиентов.

Customer requirement (Entry point)	Getting started	Next Steps
Governance (GRC)	Q1 Labs QRadar	IBM Managed Security Information Event Management
Identity	Tivoli Federated Identity Manager Business Gateway	Tivoli Identity & Access Bundle
Data	Guardium	Tivoli Security Policy Manager
Intrusion	Network IPS	Host IPS (Server Protection)
Virtualization	Virtual server protection for VMware	Network virtual IPS
Patch Management	Tivoli Endpoint Manager for Security and Compliance	Tivoli Endpoint Manager for Core Protection

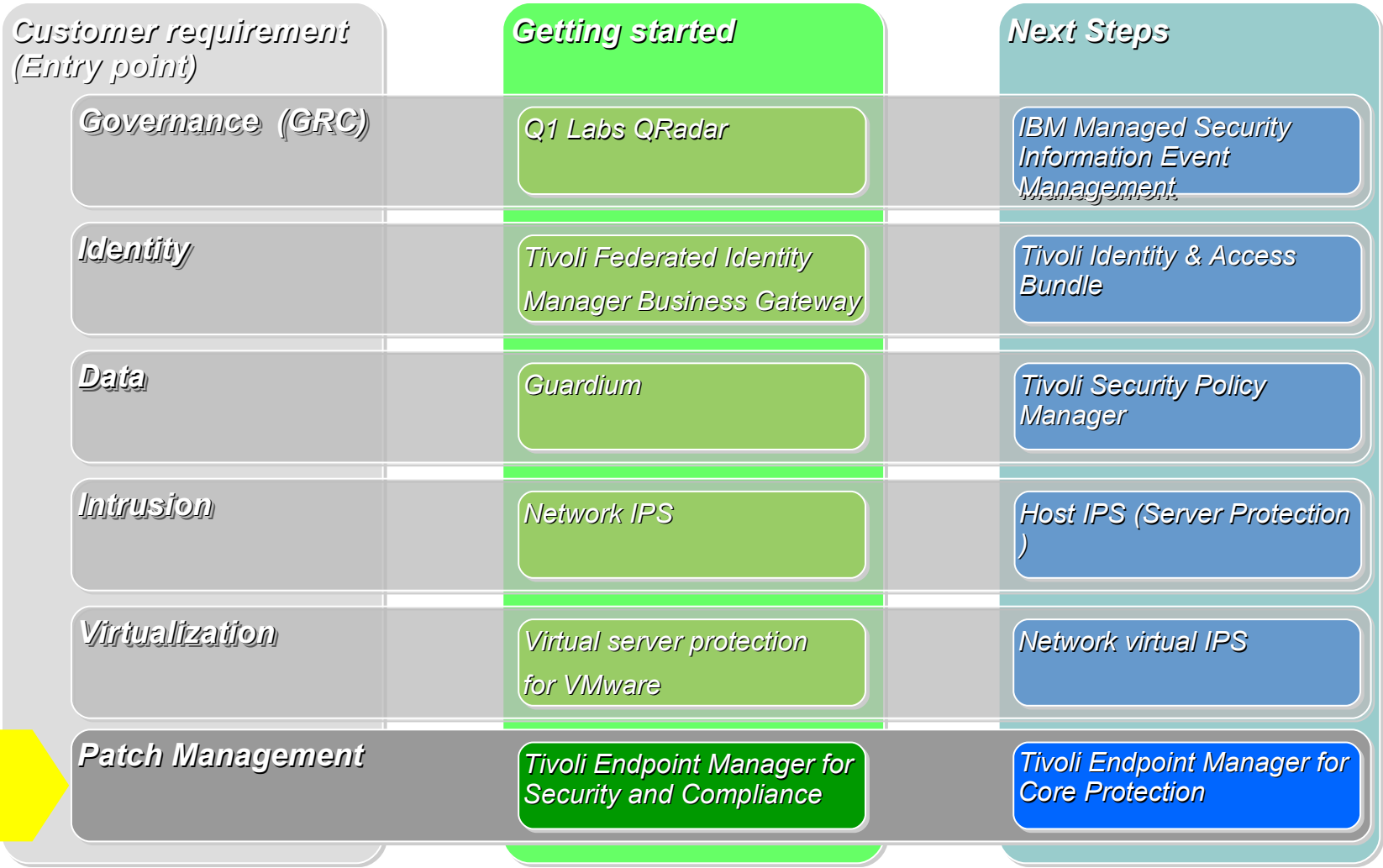
Требования обеспечения безопасности

Управление обновлениями

Какие проблемы безопасности в этой области?

- Критичные патчи выходят ежедневно, требуя бдительности и осведомленности для защиты от последних угроз и уязвимостей. Определение какие патчи необходимы для каких машин, физических или виртуальных – это большая проблема для всех клиентов, неважно, управляющих своим частным облаком или публичным.
- Большое и быстро меняющееся количество виртуальных серверов создает значительные расходы на управление. Изменения, сделанные во время планового обслуживания, могут вызвать непредвиденные проблемы с конфигурациями безопасности, и даже повлиять на предыдущие патчи.
- Облако требует стандартизации. Клиенты должны иметь возможность эффективно управлять серверами и конечными точками, чтобы быть уверенными, что стандарты конфигурации соблюдаются.

Как IBM может помочь?



Как IBM может помочь?

- IBM предоставляет решение для управления патчами и конфигурациями безопасности, которое обеспечивает:
  - Единый агент для патчинга и настройки безопасности, поддерживающий Microsoft, Mac и различные UNIX-системы, так же как и сторонние приложения (Adobe, Mozilla, Java, и т.д.).
  - Значительное уменьшение затрат на инфраструктуру и управление: один сервер может управлять до 250,000 конечными точками.
  - Непрерывное соответствие: постоянно оценивает изменения конфигураций и отчитывается о найденный несоответствиях, предлагая способ устранения.
  - Инвентаризация активов: обнаруживает устройства, которые не находятся под управлением, уменьшая риск.
  - Управление конфигурациями безопасности: непрерывно оценивает безопасность конечной точки на соответствие, тем самым реализуя требования аудита.
- И этот продукт?

Tivoli Endpoint Manager for Security and Compliance

(built on BigFix technology)

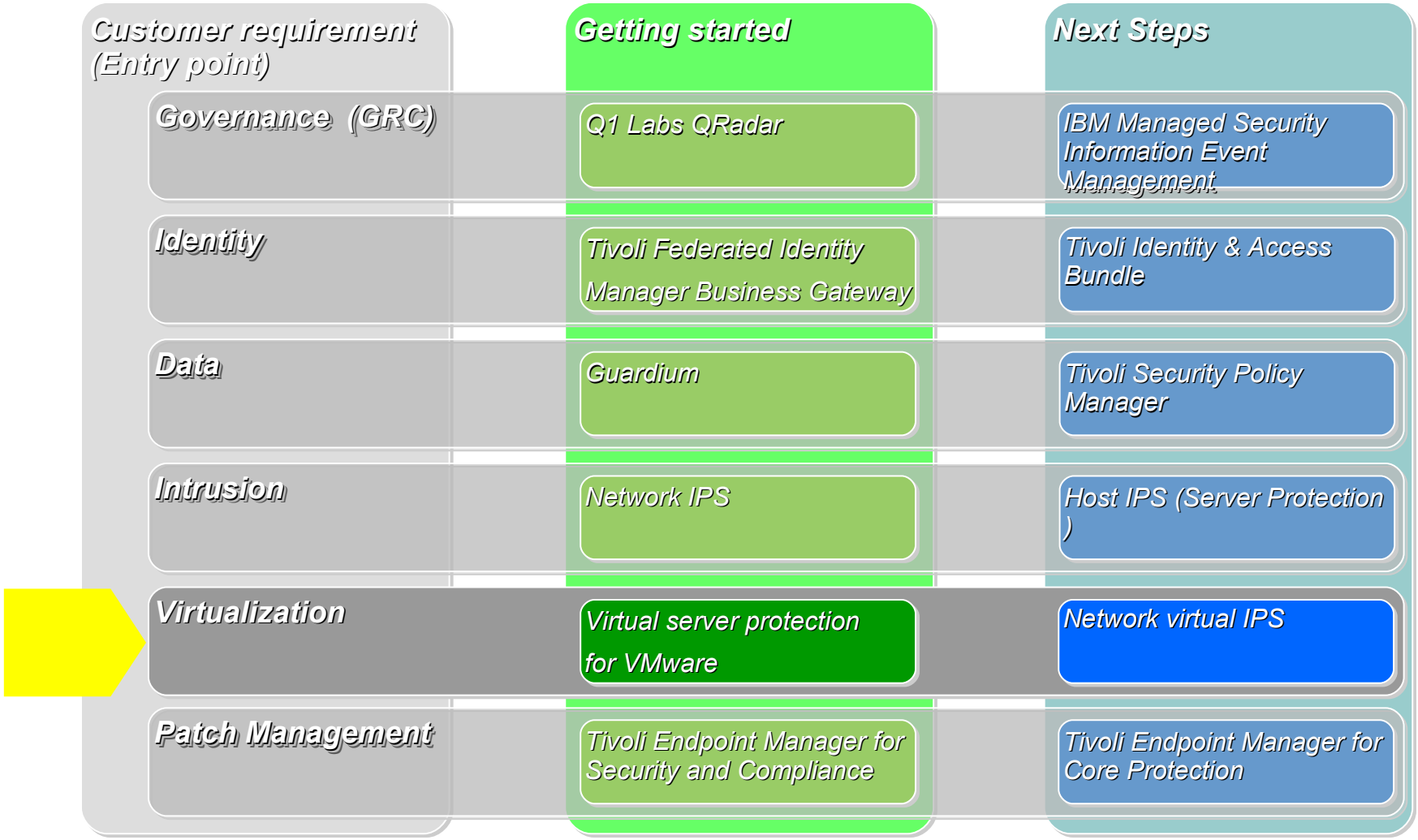
Требования обеспечения безопасности

Защита виртуальной среды

Какие проблемы безопасности в этой области?

- Облака могут предоставлять единую точку входа для потенциальных атак на множество виртуальных серверов. Перемещая рабочую нагрузку в виртуальную среду, заказчики должны быть уверены, что эти виртуальные сервера защищены.
- Клиентам необходимо обеспечить функции безопасности и отчетности, кастомизированные для виртуальной инфраструктуры
  - Виртуальная сегментация сети для отдельных виртуальных серверов.
  - Автоматизированная защита обеспечивает контроль безопасности, которая работает даже в самых динамичных средах.
- Клиентам необходимо защитить облачные приложения и данные от скрытых рут-китов, воровства ВМ и поддельных ВМ – так называемых атак изнутри облака.

Как IBM может помочь?



Как IBM может помочь?

- IBM может:
  - Интегрировать решения безопасности с гипервизором Vmware, обеспечивая контроль этого “облачного” слоя, помогая защитить заказчиков от угроз и обеспечить мониторинг активности администраторов.
  - Реализует автоматическую защиту, используя наши признаные возможности защиты от атак, адаптированные специально для облачного виртуального гипервизора. Мы также обеспечиваем технологии файервола для контроля критичного доступа на сетевом уровне.
  - Помогает защитить облачные виртуальные рабочие данные от известных рут-кит атак, оповещая пользователей о неполадке в системе.
  - Помогает соответствовать требованиям регуляторов, предлагая функционал безопасности и отчетности, кастомизированный для виртуальной среды.
- И этот продукт?

IBM Virtual Server Protection for VMware

Как IBM может помочь? (продолжение)

- IBM предлагает:
  - Наш проверенный функционал защиты от вторжений в виде виртуального аплаенса. Он обеспечивает первоклассную защиту от угроз, основанную на изучении уязвимостей (от X-Force), сфокусированную на облачных виртуальных процессах и внедрениях.
  - Мы можем защищать VMware ESX & ESXi виртуальные среды, обеспечивая предотвращение вторжений и сетевую защиту трафика между vSwitches. Это защищает облачные виртуальные машины на сервере.
  - Мы реализуем централизованное решение, которое может управлять облачной виртуальной безопасностью, наравне с традиционной сетевой безопасностью, с помощью единой консоли управления, используя общие политики безопасности.

- И этот продукт?

IBM Security Network Virtual IPS

(GV1000 and GV200)

Требования обеспечения безопасности

Защита данных

Какие проблемы безопасности в этой области?

- Мониторинг и управление доступом к данным в облачной среде может быть достаточно непростым. Множество облаков являются многопользовательскими средами, что увеличивает риск случайных или злонамеренных действий, которые приводят к взлому. Администраторы баз данных и систем могут иметь доступ к клиентским данным, и могут запутаться среди различных политик безопасности и конфиденциальности. Действительное размещение данных может быть непостоянным и может привести к более быстрому провижнингу и де-провижнингу пользователей и баз данных.
- Эти и другие вопросы заставляют клиентов предъявлять специфические требования к изоляции и разделению данных, обеспечению целостности файлов и возможностям мониторинга и управления привелигерованных пользователей.
- Кроме того, эти и другие факторы, связанные с облачными средами, могут значительно усложнить соответствие в области безопасности и управления. Клиенты, которые связаны с PCI, SOX и другими подобными стандартами, сталкиваются с непростой задачей соответствия им.

Как IBM может помочь?

Как IBM может помочь?

- IBM может:
  - Обеспечить инструменты для защиты клиентской информации и интеллектуальной собственности в облаке от кибер-преступников и внутренних злоумышленников.
  - Помочь обеспечить безопасность данных с помощью управления доступом облачных пользователей, систем, администраторов к базам данных, и предотвратить попытки доступа хакеров и злонамеренных пользователей.
  - Помочь предотвратить неавторизованные изменения критичных облачных данных привилегированными пользователями. При работе с облаком, дополнительные администраторы, включая системных администраторов, администраторов баз данных и администраторов приложений, могут иметь доступ к множеству баз даных. IBM предлагает инструменты для контроля и аудита их доступа к базам даных.
  - Помочь сократить расходы на аудит с помощью согласованного подхода к облачным и обычным базам данных.
  - Обеспечить гибкое и масштабируемое администрирование безопасности баз данных, чтобы адаптироваться к динамичной и эластичной облачной среде.
  - Обеспечить централизованную консоль безопасности для гетерогенных платформ баз данных, как облачных, так и физических.
- И этот продукт?

IBM InfoSphere Guardium

Требования обеспечения безопасности

Управление учетными данными

Какие проблемы безопасности в этой области?

- Поскольку пользователи имеют доступ к облачным приложениям, необходимы инструменты для контроля учетных записей и прав доступа к этим приложениям и даным. Клиенты должны быть уверены в том, что:
  - Конкретные пользователи имеют доступ к необходимым системам, приложениям и данным.
  - Они имеют возможность оперативно управлять учетными записями при изменении прав или смене работы пользователей.
  - Пользователи могут получать доступ к приложениям через SSO.
  - Доступ пользователей ограничен только к необходимым приложениям и возможностям.
- Клиенты озабочены возможным увеличением сложности управления внедрением облака. Клиенты бы хотели управлять своей ИТ инфраструктурой с помощью единого набора инструментов безопасности как для традиционной, так и для облачной среды.

Как IBM может помочь?

Как IBM может помочь?

- IBM может обеспечить:
  - Возможность пользователям получать доступ к множеству Web и облачных приложений через единую точку входа, с помощью одного ID и пароля.
  - Самообслуживание пользователей в части создания и управления учетными записями, например, сброс пароля.
  - Проверенное, простое для внедрения решение в виде виртуального аплаенса, для обеспечения облачной безопасности и поддержки миллионов пользователей.
  - Последовательный подход к управлению безопасностью учетных записей и прав доступа для обычных и облачных пользователей и приложений.
  - Модульный подход, когда дополнительная безопасность для учетных записей и прав доступа может быть добавлена в последствии, обеспечивает быстрое внедрение и окупаемость.
- И этот продукт?

IBM Tivoli Federated Identity Manager

Business Gateway

Требования обеспечения безопасности

Защита от вторжений

Какие проблемы безопасности в этой области?

- Клиентам необходимо:
  - Защита от случайно привнесенных пользователями в облако вредоносных программ.
  - Защита своего облачного рабочего процесса от злонамеренных угроз
  - Защита как сети, так и серверов от атак
  - Внедрение решения, которое масштабируется вместе с размером облачного трафика и не вносит значительные задержки.

Как IBM может помочь?

Как IBM может помочь?

- IBM может:
  - Обеспечить защиту на сетевом уровне (входящем/исходящем) против угроз и уязвимостей для облачной инфраструктуры.
  - Защитить пользователей от новых угроз. Получив доступ в облако, пользователи могут “подцепить” ненужный контент, включая вредоносное ПО. Решения безопасности IBM могут помочь защитить корпоративную сеть от такого пользовательского контента, распознав и заблокировав его.
  - Предотвратить несанкционированное использование пользователями облака, такого как системы мгновенных сообщений и peer to peer file sharing.
- И этот продукт?

IBM Security Network Intrusion Prevention System

Как IBM может помочь? (продолжение)

- IBM может:
  - Предложить выдающуюся защиту для облака, благодаря комбинации множества инспекционных технологий.
  - Уменьшить риск вредоносной активности с помощью файервола, который блокирует сетевой трафик от попадания в сеть из облака.
  - Помочь обеспечить конфиденциальность данных и упростить соответствие, используя расширенный функционал мониторинга; совмещая облачные активы с корпоративными активами в одном отчете.
  - Производить мониторинг целостности системы, файлов и регистров в облачных серверах.
- И этот продукт?

IBM Security Server Protection

Требования обеспечения безопасности

Governance, risk and compliance

Какие проблемы безопасности в этой области?

- Клиенты не уверенны, достаточно ли хороши их существующие политики безопасности и отказоустойчивости, так же как и системы управления безопасностью, рисками и соответствия для внедрения облака.
- В облачных средах должны быть эффективно расставлены приоритеты безопасности, чтобы снизить риск и обеспечить конфиденциальность, целостность и доступность бизнес информации.
- Некоторые облачные системы требуют более строгих требований к безопасности и доверию.
- Существующие решения и инструменты обеспечения соответствия могут быть недостаточно адекватны для динамических и гибких облачных сред.

Как IBM может помочь?

Как IBM может помочь?

- IBM может:
  - Предоставить клиентам идеальную возможность начать собирать данные и доказательства о том, что происходит на сетевом, пользовательском и уровне приложений в их облачных средах.
  - Это решение может быть быстро расширено для обеспечения детальной сетевой аналитики в облачной инфраструктуре, так же как и поведенческого анализа, и обнаружения аномалий.
  - Наконец, полная картина может быть построена с помощью анализа событий и профилирования активов, а завершит картину анализ потоков (разных Flow).
  - Это решение позволяет моделировать угрозы, чтобы в дальнейшем помочь организации проактивно реагировать на них.
- И этот продукт?

Q1 Labs QRadar

Спасибо!

andrey.timoshenkov@ru.ibm.com