Руководство по обеспечению безопасности облачных платформ

Оглавление

Основные моменты

1. В идеале поставщик облачных услуг должен иметь возможность интегрировать систему управления идентификационными данными вашей компании в свою платформу или при необходимости предоставить вам надежное решение для этой задачи.

2. В ходе проверки убедитесь, что облачная платформа предоставляет хорошо интегрируемые брандмауэры, группы безопасности и возможности микросегментирования с учетом задач и доверенных вычислительных хостов.

3. Поставщики облачных услуг должны предоставить решения BYOK, позволяющие вашей организации монопольно управлять ключами во всех системах хранения данных и услугах.

4. Лучшая методика защиты контейнеров – сканирование их на наличие уязвимостей и перед развертыванием, и во время работы.

5. Система безопасности облачной платформы предполагает эффективное управление доступом на уровне задач, подробное отслеживание деятельности и интеграцию в локальные системы.

Переосмысление безопасности облачных приложений

По мере того как все больше организаций переходят на облачную модель разработки приложений и управления задачами, эффективность традиционных моделей безопасности, основанных на защите периметра, в платформах облачных вычислений быстро теряется. Хотя необходимость в защите периметра еще не отпала, одной ее уже недостаточно. Так как данные и приложения в облаке находятся вне границ организации в привычном понимании, их необходимо защищать по-новому.

Организации, переходящие на облачную модель или планирующие внедрение гибридных облачных приложений, должны дополнить традиционную систему защиты периметра сети технологиями защиты облачных задач. Предприятия должны быть уверены в том, что поставщик облачных услуг надежно защищает их парк приложений, начиная с уровня инфраструктуры. Поэтому основной критерий выбора поставщика – это доверие в вопросе обеспечения безопасности платформы.

Определяющие факторы безопасности облака

В числе определяющих факторов облачной безопасности находится защита данных и соблюдение требований законодательства, что в то же время является и главным препятствием для внедрения облака. Решение этих вопросов затрагивает все аспекты разработки и операций. В облачных приложениях данные могут быть рассредоточены по разным объектным хранилищам, службам обработки данных и облакам, что создает многочисленные мишени для возможной атаки. Причем атаки могут исходить отнюдь не только от изощренных кибермошенников и из внешних источников: по данным недавнего опроса, 53 % респондентов сообщили, что за прошедшие 12 месяцев им приходилось сталкиваться с инсайдерскими атаками.[1]

Пять основополагающих принципов облачной безопасности

Так как у каждой организации свои, уникальные потребности в отношении безопасности облачных платформ, им требуется (и они вправе этого ожидать), чтобы их провайдеры стали для них надежными технологическими партнерами. По сути, организациям следует оценивать соответствие облачных провайдеров особым требованиям организации по следующим пяти критериям:

1. **Идентификация и управление доступом:** идентификация, проверка подлинности и контроль доступа
2. **Безопасность сети:** защита, изоляция и сегментация
3. **Защита данных:** шифрование данных и управление ключами
4. **Обеспечение безопасности приложений и DevSecOps:** в том числе тестирование безопасности и защита контейнеров
5. **Прозрачность и аналитика:** мониторинг и анализ протоколов, потоков данных и событий для шаблонов

Проверка идентификационных данных и управление доступом в облачной платформе

Любое взаимодействие с облачной платформой начинается с проверки идентификационных данных, установления личности или инструмента, осуществляющего взаимодействие: администратор ли это, пользователь или служба. В экономике API службам присваиваются отдельные ИД, поэтому для успешной работы облачных приложений крайне важна возможность точно и безопасно вызвать службу из API по этим данным.

Ищите провайдеров, обеспечивающих унифицированный способ идентификации и проверки подлинности для доступа к API или вызова служб. Также вам необходим способ идентификации и проверки подлинности конечных пользователей, получающих доступ к размещенным в облаке приложениям. К примеру, в IBM Cloud используется ИД приложения, который разработчики могут использовать для встраивания функции идентификации в свои мобильные или веб-приложения.

При строгой идентификации запрещается доступ незарегистрированных пользователей в облачные системы. Так как система идентификации и управления доступом (IAM) для платформы является основой основ, организации, у которых уже есть подобная система, вправе ожидать, что облачные провайдеры интегрируют в нее свои решения. Чаще всего для этого используется технология объединения идентификационных данных, которая связывает ИД и атрибуты пользователей в разных системах.

Зачем идентифицировать вызовы служб?

В архитектуре на основе микросервисов обмен данными и взаимодействие приложений осуществляется посредством API. Когда приложение работает, оно использует API для вызова служб, необходимых для выполнения разнообразных операций. К примеру, ваше приложение может вызвать службу объектного хранилища для данных. В ходе выполнения запроса уже сама служба объектного хранилища может вызвать службу управления ключами, чтобы получить ключи шифрования, необходимые для расшифровки данных. В процессе взаимодействия с пользователем приложение может применять API для доступа к идентификационным данным пользователя, публикации информации из приложений (например, публикация контента из приложения в Twitter), а также для определения местоположения пользователя и предоставления информации, связанной с регионом. **При обеспечении безопасности все эти аспекты интеграции представляют определенные сложности.**

У облачных провайдеров должен быть налажен унифицированный способ проверки идентификационных данных пользователя или службы, запрашивающих доступ к API или службе. Разумеется, в ходе идентификации все запросы на доступ и все транзакции должны регистрироваться для целей аудита. **Скорее всего, ваши API и службы содержат ценную информацию, являющуюся вашей интеллектуальной собственностью, и вам вряд ли захочется делить ее с кем-то другим.**

Попросите у потенциальных поставщиков доказательства, что их архитектура и системы IAM предоставляют такие возможности. К примеру, в основе управления идентификационными данными и доступом, реализованного в IBM Cloud, лежат несколько ключевых компонентов (рис. 1):

Идентификационные данные

- Каждому пользователю присваивается уникальный идентификатор
- Службы и приложения идентифицируются по своим служебным ИД
- Ресурсы идентифицируются и обрабатываются по имени облачного ресурса (CRN)
- После идентификации пользователи и службы получают токены со своими идентификационными данными

Управление доступом

- Когда пользователи и службы пытаются получить доступ к ресурсам, система IAM определяет, следует ли разрешить или запретить доступ и действия
- Службы определяют действия, ресурсы и роли
- Администраторы определяют политики присвоения пользователям ролей и разрешений на различных ресурсах
- Защита распространяется на API, облачные функции и серверные ресурсы, размещенные в облаке

Оценивая систему безопасности, предлагаемую облачным провайдером, смотрите на наличие списков управления доступом вместе с именами общих ресурсов: это позволяет ограничивать доступ пользователей не только к определенным ресурсам, но и даже к определенным операциям на этих ресурсах. Эти функции помогут гарантировать защиту данных от несанкционированного доступа как извне, так и изнутри.

Если ваш поставщик корпоративных идентификационных данных (Enterprise IdP) поддерживает облако, то это пригодится вам, если вы решите создавать облачные приложения на основе имеющихся корпоративных приложений, использующих Enterprise IdP. Ваши пользователи смогут без труда входить и в облачное, и в изначальное приложения, не используя для этого несколько систем или идентификаторов. Снижение сложности – это всегда хорошо.

Ключевой момент

В идеале поставщик облачных услуг должен иметь возможность интегрировать систему управления идентификационными данными вашей компании в свою платформу или при необходимости предоставить вам надежное решение для этой задачи.

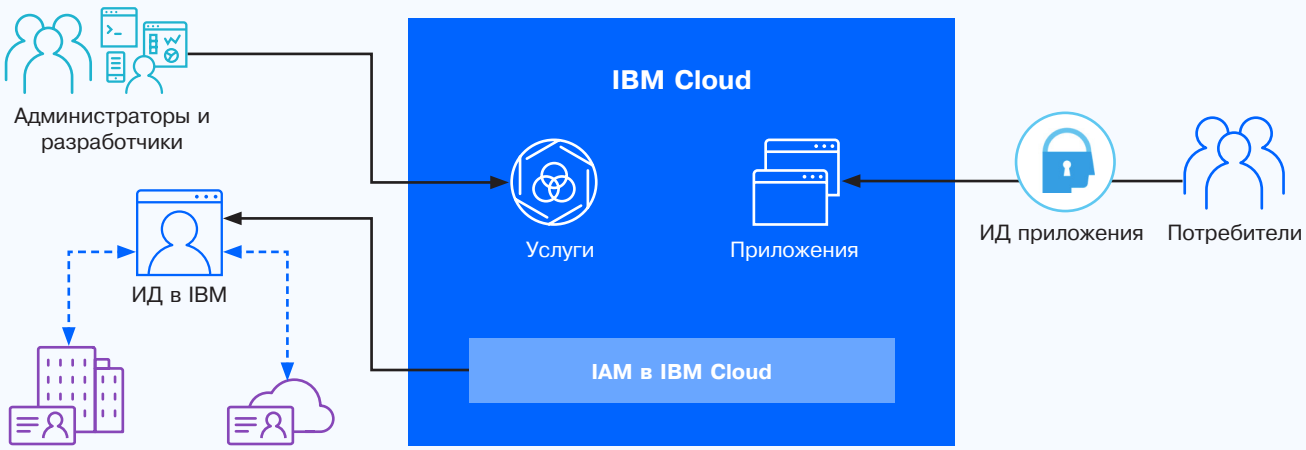


Рис. 1. Разделение элементов кластера, управляемых провайдером и клиентом.

Перестройка изоляции и защиты сети

Для ограничения доступа к устройствам и серверам в одной сети многие провайдеры применяют сегментацию. В дополнение к этому поверх физической инфраструктуры провайдеры создают виртуальные изолированные сети, автоматически ограничивающие доступ пользователей и служб. Эти и другие базовые технологии обеспечения безопасности являются минимально необходимым условием для доверия облачной платформе.

Часто облачные провайдеры предлагают технологии защиты (от брандмауэров для веб-приложений до виртуальных частных сетей и средств противодействия DoS-атакам) как услуги для защиты программно-определяемых сетей с платой за фактическое использование. В эпоху цифровых технологий обязательно стоит применять следующие важнейшие для сетевой безопасности технологии:

Группы безопасности и брандмауэры

Пользователи облаков часто встраивают сетевые брандмауэры для защиты сети (доступ к сети на уровне виртуального частного облака или подсети) и создают сетевые группы безопасности для доступа на уровне экземпляров. При управлении доступом к облачным ресурсам группы безопасности эффективно служат первой линией обороны. Они позволяют легко добавлять средства безопасности на уровне экземпляров, чтобы управлять входящим и исходящим трафиком как в публичных, так и в частных сетях.

Многим клиентам нужна возможность управления периметром для защиты сети и подсетей периметра. Самым простым способом решения этой задачи являются виртуальные брандмауэры. Они предотвращают попадание нежелательного трафика на серверы и уменьшают площадь атаки. Облачные провайдеры должны предоставлять как виртуальные, так и аппаратные брандмауэры, позволяющие настраивать правила на основе разрешений для всей сети или для отдельных подсетей.

Безусловно, для обеспечения защищенного соединения от облака к вашим локальным ресурсам нужны VPN. Если вы работаете в гибридной облачной среде, то без сетей VPN вам не обойтись.

Микросегментирование

Разработка приложений в облаке в виде набора небольших сервисов дает преимущество в плане безопасности за счет возможности изоляции этих приложений с помощью сегментов сети. Поэтому следует искать облачную платформу с поддержкой микросегментирования посредством автоматизации настройки сети и выделения сетевых ресурсов. **Что касается изоляции задач с возможностями масштабирования, то сейчас быстро набирают популярность контейнеризованные приложения с микросервисной архитектурой.**

Ключевой момент

В ходе проверки убедитесь, что облачная платформа предоставляет хорошо интегрируемые брандмауэры, группы безопасности и возможности микросегментирования с учетом задач и доверенных вычислительных хостов.

Защита данных с помощью шифрования и управления ключами

Надежная защита данных – это основа всей системы безопасности для любого цифрового предприятия, особенно в отраслях со строгим регулированием: например, в финансовом секторе и здравоохранении.

Данные, связанные с облачными приложениями, могут быть рассредоточены по разным объектным хранилищам, службам обработки данных и облакам. Традиционные приложения могут работать только со своей базой данных, с собственной ВМ и могут содержать конфиденциальные данные, хранящиеся в файлах. В таких ситуациях жизненно важно, чтобы конфиденциальные данные шифровались как во время хранения, так и в процессе передачи.

Предприятия вправе беспокоиться о том, что облачные провайдеры или другие неавторизованные пользователи без их ведома получат доступ к их данным, и требовать от провайдеров полной прозрачности в отношении доступа к данным. **Поэтому клиенты ожидают, что провайдер обеспечит контроль доступа к данным с помощью шифрования, а также контроль ключей шифрования.** Это привело к тому, что сейчас для облачной безопасности обязательно нужна поддержка модели создания собственных ключей (BYOK). Она позволяет централизованно управлять ключами шифрования, гарантирует, что корневые ключи никогда не выйдут за пределы системы управления ключами, а также позволяет контролировать все операции жизненного цикла управления ключами (рис. 2).

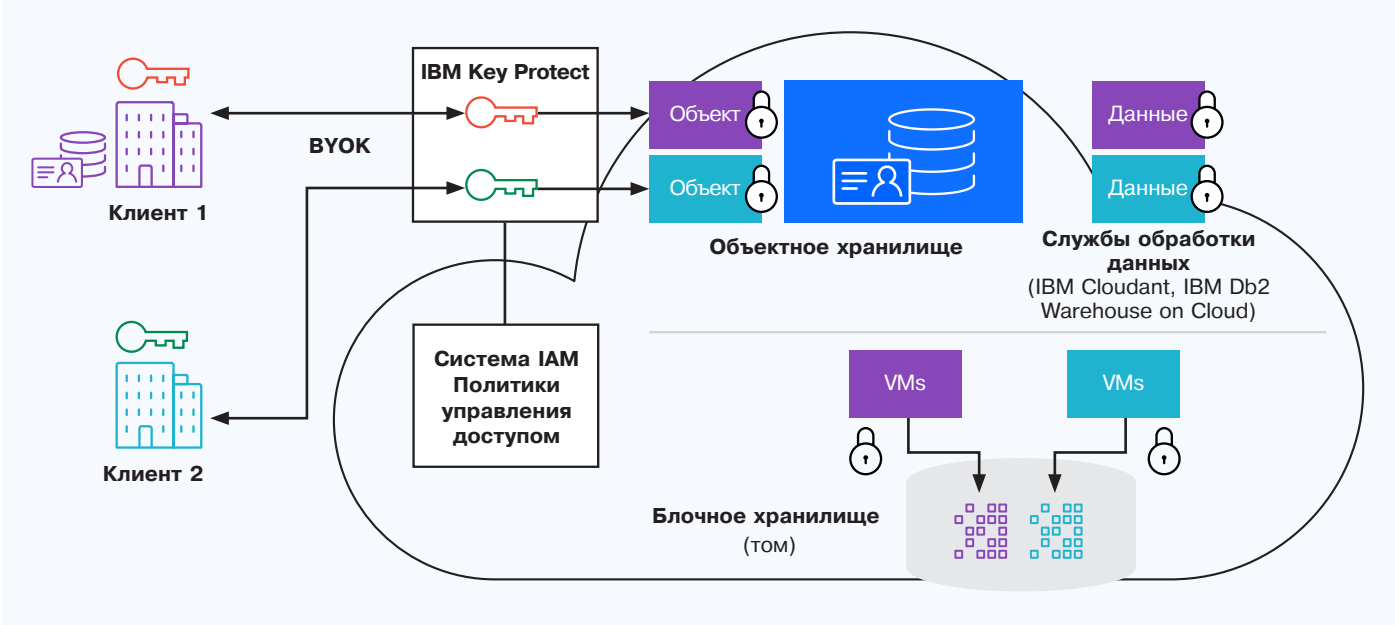
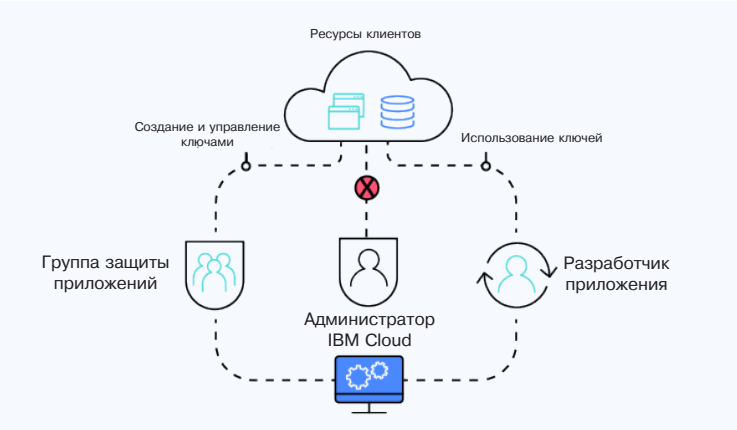


Рис. 2. Архитектура решения BYOK.

Хранение собственных ключей (KYOK)

Для того чтобы сохранить полную конфиденциальность ваших данных в общедоступном облаке, IBM разработала уникальное решение, позволяющее вам оставаться единственным хранителем своего ключа шифрования. Будучи единственной в отрасли услугой, построенной на оборудовании, сертифицированном по стандарту FIPS 140-2, уровень 4, IBM Cloud Hyper Protect Crypto Services предоставляет аппаратный модуль управления ключами и облачной защиты (HSM).



Доверенные вычислительные узлы

В конечном счете, все сводится к оборудованию: никто не захочет развертывать серьезные приложения и данные на хосте, которому нет доверия. Облачные провайдеры, предлагающие оборудование, работающее по принципу “измерение-проверка-запуск”, предоставят надежно защищенные хосты для приложений, развертываемых в системах координации контейнеров.

В качестве примеров таких технологий, реализованных на уровне хоста и укрепляющих доверие к облачной платформе, можно назвать Intel Trusted Execution Technology (Intel TXT) и Trusted Platform Module (TPM). Intel TXT защищает от программных атак, рассчитанных на кражу конфиденциальной информации путем повреждения кода системы или BIOS либо изменения конфигурации платформы. Intel TPM – это аппаратное устройство безопасности, помогающее защитить процесс начальной загрузки системы путем проверки его подлинности до того, как управление системой будет передано ОС.

Защита данных во время хранения и в процессе передачи

Где бы ни находились ваши данные – на локальных ресурсах или в облаке – встроенные функции шифрования и модель BYOK помогут вам ни на минуту не выпустить их из-под контроля. Это отличный способ управления доступа к данным в случае облачного развертывания приложений. При таком подходе клиентская система управления ключами создает ключ на локальных ресурсах и передает его в службу управления ключами, работающую у провайдера. К тому же, этот сценарий включает в себя шифрование данных в хранилищах любого типа: в блочных, объектных или в службах обработки данных.

Для передаваемых данных защита соединения и передачи обеспечивается с помощью протокола TLS/SSL. Шифрование TLS/SSL позволяет также обеспечивать нормативное соответствие, безопасность и управляемость без контроля криптосистемы или инфраструктуры со стороны администратора. Поэтому функция управления сертификатами SSL является обязательным условием доверия к облачной платформе.

Решение задач аудита и обеспечения нормативного соответствия

Предоставление собственных ключей шифрования и хранение их в облаке без доступа поставщика услуг обеспечивает прозрачность и контроль информации, необходимой директору по ИТ-безопасности для проверки нормативного соответствия.

Ключевой момент

Поставщики облачных услуг должны предоставить решения BYOK, позволяющие вашей организации управлять ключами во всех системах хранения данных и услугах.

Автоматизация обеспечения безопасности для DevOps

Так как группы DevOps создают облачные услуги и работают с контейнерными технологиями, им нужен способ интеграции проверок безопасности в конвейере, который все больше автоматизируется. Поскольку такие площадки, как Docker Hub, продвигают открытый обмен, разработчики могут запросто сэкономить время на подготовку, просто загрузив необходимые ресурсы. Но такая гибкость требует регулярной проверки всех образов контейнеров в реестре до их развертывания.

Автоматизированная система сканирования помогает обеспечить доверие за счет поиска потенциальных уязвимостей в образах еще до того, как они будут запущены. Задайте поставщику платформы вопрос, сможет ли ваша организация самостоятельно создавать политики (к примеру, “не развертывать образы, в которых обнаружены уязвимости” или “предупреждать меня перед развертыванием таких образов в производственной среде”) в рамках обеспечения безопасности конвейера DevOps?

Например, служба контейнеров IBM Cloud предоставляет систему Vulnerability Advisor (VA), которая сканирует и пассивные, и активные контейнеры. VA проверяет каждый уровень каждого образа в частном реестре клиента в облаке и ищет уязвимости или вредоносный код еще до того, как образ будет развернут. Так как при обычном сканировании образов в реестрах можно пропустить такие ситуации, как перемещение пассивного образа в развернутые контейнеры, VA также сканирует запущенные контейнеры на наличие отклонений. Инструмент выдает рекомендации в форме многоуровневых предупреждений.

Ключевой момент

Лучшая методика защиты контейнеров – сканирование их на наличие уязвимостей и перед развертыванием, и во время работы.

Также в VA есть и другие функции, помогающие автоматизировать обеспечение безопасности в конвейере DevOps:

- **Параметры на случай нарушения политик:** VA позволяет администраторам настроить политики развертывания образов на основе трех типов нарушений: установлены пакеты с известными уязвимостями; выполнен удаленный вход в систему; выполнен удаленный вход в систему пользователей с простыми паролями.
- **Практические советы:** На данный момент VA проверяет 26 правил, основанных на стандарте ISO 27000, включая такие параметры, как минимальный возраст и минимальная длина пароля.
- **Обнаружение повреждения конфигурации системы безопасности:** VA отмечает все найденные изменения конфигурации, предоставляет их описания и рекомендует комплекс мер по исправлению.
- **Интеграция с IBM X-Force:** VA получает аналитическую информацию о безопасности из пяти внешних источников и оценивает каждую уязвимость по таким критериям, как вектор атаки, сложность и наличие известного исправления. Удобная система рейтингов (критический уровень, высокий, средний, низкий) помогает администраторам быстро оценить серьезность уязвимостей и упорядочить исправительные меры.

Также следует отметить, что VA не прерывает работу образов для исправления. Вместо этого IBM исправляет “золотой” образ в реестре и развертывает этот новый образ в контейнере. Такой подход позволяет гарантировать, что все последующие экземпляры этого образа будут уже исправленными. С виртуальными машинами можно работать традиционно: с помощью службы обеспечения безопасности конечных точек, которая будет исправлять их и устранять нарушения безопасности Linux.

Слово о Kubernetes

Если ваши группы DevOps работают с популярным ПО для координации контейнеров Kubernetes, убедитесь, что они смогут и дальше работать с привычными инструментами. Также оцените, насколько легко платформа способна выделять новые кластеры и управлять уже развернутыми кластерами Kubernetes.

Спросите, поддерживает ли система Kubernetes облачного провайдера технологии Calico и Istio. Calico и Istio – это два важнейших компонента Kubernetes, помогающих обеспечить безопасность приложений и задач. Calico помогает обеспечить соблюдение политик безопасности, упрощая управление IP-адресами, присвоенными задачам на вычислительном узле, и списками контроля доступа к программам на каждом узле. Настройка определений политик и применение их посредством меток конфигурации в Istio обеспечивает контроль соединений на основе сертификатов в микросервисах в поде или кластере Kubernetes.

Создание “иммунной системы безопасности” с помощью интеллектуального мониторинга

В процессе перехода в облако директора по ИТ-безопасности часто беспокоятся о недостаточной прозрачности и потере контроля. К примеру, если облако может отключиться в результате удаления какого-то ключа или случайного разрыва соединения с локальными ресурсами или центром управления безопасностью предприятия (SOC) из-за изменения конфигурации, почему бы операторам не потребовать полной прозрачности всех его компонентов: облачных задач, API, микросервисов?

Журналы доступа и контрольные журналы

Весь доступ пользователей и администраторов как со стороны облачного провайдера, так и со стороны вашей организации должен автоматически заноситься в протоколы. Встроенная функция отслеживания облачных операций может сформировать журнал, в котором будут зарегистрированы все попытки получения доступа к платформе и услугам, включая API, доступ из мобильных и веб-приложений. Вашей организации должна быть предоставлена возможность получения этих протоколов и интеграции их в ваш корпоративный SOC.

Аналитика безопасности предприятия

Убедитесь, что у вас есть возможность интегрировать все протоколы и события в свою локальную систему управления событиями и информационной безопасностью (SIEM) (рис. 3). Некоторые поставщики облачных услуг также предлагают средства мониторинга безопасности с функциями управления инцидентами и отчетности, анализом предупреждений безопасности в реальном времени и объединенным представлением обо всех гибридных решениях.

К примеру, IBM QRadar представляет собой комплексную SIEM-платформу, вобравшую в себя ряд решений для аналитики безопасности, которые можно масштабировать по мере роста требований организации. Его функции машинного обучения учатся на шаблонах угроз, в результате чего формируется прогнозная, “иммунная” система безопасности.

Управляемая безопасность, подкрепленная опытом

Если вашей организации недостает опыта в сфере обеспечения безопасности, то ищите провайдеров, способных взять управление безопасностью на себя. Некоторые провайдеры могут отслеживать инциденты безопасности, анализировать угрозы в различных отраслях и сопоставлять эти данные для выработки оптимальных мер. Спросите, сможет ли провайдер, помимо прочего, обеспечить единую сводную панель, на которой можно было бы отслеживать и внутренние, и управляемые службы безопасности.

Ключевой момент

Система безопасности облачной платформы предполагает эффективное управление доступом на уровне задач, подробное отслеживание деятельности и интеграцию в локальные системы.

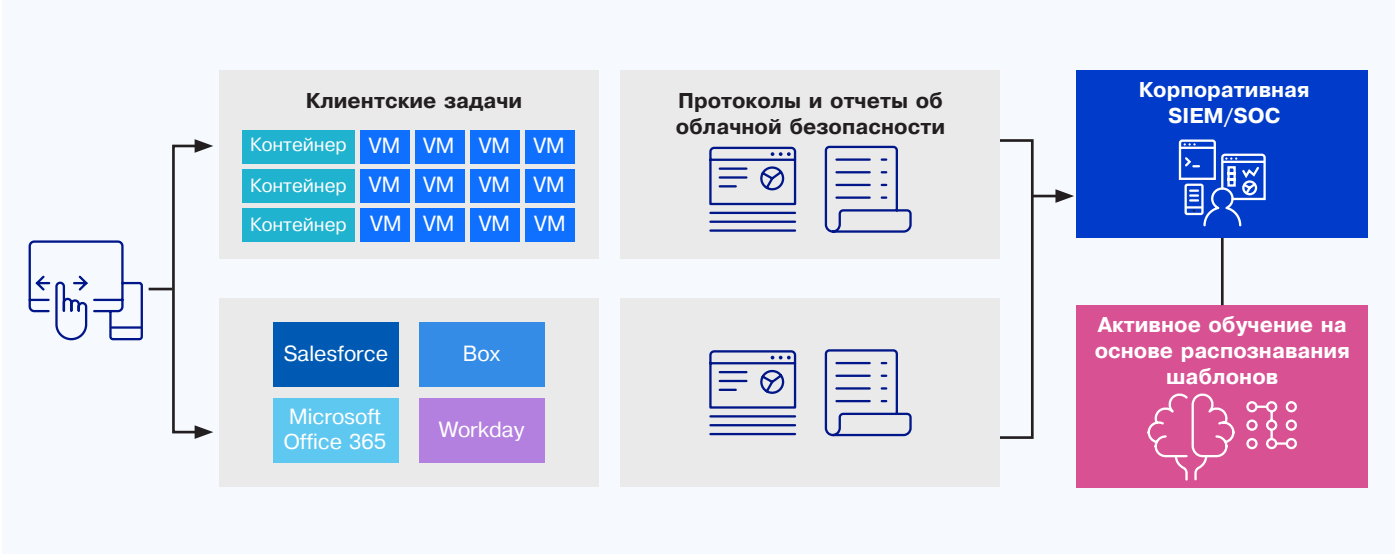


Рис. 3. Интеграция прозрачности облака в корпоративную платформу SIEM/SOC.

Безопасность, ориентированная на успех бизнеса

По мере того, как облачные технологии все шире и глубже вплетаются в работу цифрового бизнеса, выбор оптимального облачного провайдера, способного предоставить нужный набор функций и средств управления для защиты ваших данных, приложений и облачной инфраструктуры, от которой зависят клиентские приложения, становится в прямом смысле делом первостепенной важности. Требуйте, чтобы решение для обеспечения безопасности платформы охватывало пять главных направлений облачной защиты: идентификация и доступ, сетевая безопасность, защита данных, защита приложений, а также прозрачность и аналитика. В приоритете должна быть возможность целиком сосредоточиться на своей профильной деятельности, как можно меньше отвлекаясь на управление технологиями.

Облачный провайдер с надежной и эффективной системой безопасности дает следующие преимущества:

- **Ускорение окупаемости:** так как система безопасности уже реализована и настроена, группы могут легко получить ресурсы и быстро разработать прототипы пользовательских интерфейсов, оценить результаты и при необходимости повторить процесс.
- **Меньшие капитальные расходы:** применение облачных услуг по обеспечению безопасности может избавить вас от многих начальных расходов, например на серверы, лицензии на ПО и устройства.
- **Снижение нагрузки на администраторов:** благодаря успешному установлению и поддержанию доверия к облачной платформе провайдер с оптимальным набором решений для безопасности берет основные административные задачи на себя, что позволяет меньше платить за отчетность и обслуживание ресурсов.

Ознакомьтесь с отчетом Gartner Peer Insights и узнайте, почему стоит выбрать IBM Cloud.

Самые высокие оценки за корпоративную интеграцию (4,6 из 5 звезд)

Также эта платформа имеет самый высокий рейтинг среди ведущих облачных провайдеров (4,7 из 5 звезд)

...по результатам **90 отзывов за последние 12 месяцев на 1 июня 2020 г.**

https://www.gartner.com/reviews/market/public-cloud-iaas/vendor/ibm/product/ibm-cloud

Обзоры Gartner Peer Insights представляют собой субъективные мнения конечных пользователей, основанные на их личном опыте, и не отражают точку зрения Gartner или его дочерних компаний.

Дополнительная информация

Дополнительная информация о пяти главных направлениях облачной безопасности, а также о сопутствующих технологиях и услугах IBM опубликована на странице **ibm.com**/cloud/security

Оставайтесь на связи

Блог об IBM Cloud

Следите за нами

@IBMcloud
Facebook

Свяжитесь с нами

LinkedIn
YouTube

© Copyright IBM Corporation 2020

IBM Восточная Европа/Азия
123112 Москва
Пресненская наб., 10

Веб-сайт IBM:
ibm.com

IBM, логотип IBM, ibm.com, Cloudant, Db2, QRadar и X-Force – товарные знаки International Business Machines Corp., зарегистрированные во многих странах. Названия других продуктов и услуг могут быть товарными знаками IBM или других компаний. Действительный в настоящее время список товарных знаков IBM можно найти на веб-странице по адресу **ibm.com**/legal/copytrade.shtml

Intel и Intel TXT – товарные знаки или зарегистрированные товарные знаки Intel Corporation или ее дочерних компаний в США и других странах.

Linux – зарегистрированный товарный знак Линуса Торвальдса (Linus Torvalds) в США и/или других странах.

Microsoft и Office 365 – зарегистрированные товарные знаки Microsoft Corporation в США и/или других странах.

Настоящий документ актуален по состоянию на момент публикации и может быть изменен IBM в любое время. Не все предложения могут быть доступны во всех странах, в которых IBM ведет свою деятельность.

[1] Прогноз Insider Threat на 2018 г., опубликованный в ноябре 2017 г. http://crowdresearchpartners.com/portfolio/insider-threat-report