Cloud Advisor

Решение проблем безопасности в публичном облаке с помощью Cloud Advisor

Автор: Cloud Advisor

Тип документа: Whitepaper

Содержание

Проблема

Использование публичных облаков требует изменения политики безопасности данных и новых подходов к ее реализации. Основные вызовы, с которыми сталкиваются пользователи публичных облаков, – это контроль за конфигурацией, управление уязвимостями и соответствие требованиям. Рассмотрим их подробнее.

Ошибки конфигурации (23%) занимают первое место среди инцидентов в области облачной безопасности, опережая взлом учетных записей (15%), эксплуатацию уязвимостей (14%) и заражение вредоносным ПО (9%).

Отчет Cloud Security Report 2022, Cybersecurity Insiders

Контроль за конфигурацией

Публичный доступ

Публичный доступ - одно из самых важных отличий облака от традиционной on-prem инфраструктуры - заключается в том, что данные и серверы находятся вне периметра безопасности организации в публичном облаке и любая ошибка в конфигурировании может привести к утечке конфиденциальных данных.

Выключение ИБ из процесса создания ресурсов

Облако используется как система «самообслуживания» для сотрудников, создающих вычислительные ресурсы, без длительных этапов планирования и согласования. Рост скорости запуска проектов приводит к появлению брешей в защите, так как разработчики, взаимодействующие с облачными сервисами и ресурсами, зачастую не обладают достаточной квалификацией для принятия верных решений в области безопасности и создают ресурсы без участия служб ИБ.

Динамическая природа облака

Легкость развертывания новых ресурсов в облаке стимулирует рост числа облачных активов. Ресурсы постоянно добавляются в облако при запуске новых проектов. Кроме того, меняется конфигурация существующих ресурсов. Ситуацию осложняют обширные возможности автоматизации, предоставляемые облачным провайдером, с помощью которых сотни виртуальных машин могут быть запущены, остановлены или изменены за считанные секунды.

Вывод

Облако представляет собой десятки и сотни тысяч различных объектов, количество и конфигурация которых динамически меняются, при этом изменения происходят без согласования со службой ИБ и могут привести к раскрытию конфиденциальных данных.

Управление уязвимостями

Традиционные средства поиска уязвимостей, созданные для on-prem, испытывают сложности с защитой облачных инфраструктур.

> 59% респондентов назвали адаптацию мер обеспечения информационной безопасности самой сложной задачей при переходе на облачные технологии.
>
> Исследование «Страх облаков», PwC

Отсутствие контекста

Традиционные средства поиска уязвимостей не имеют данных о конфигурации облака. Для решений, разработанных для on-prem, приоритет уязвимости Log4Shell на ВМ, которая является публичным веб-сервером, имеющим доступ к важной БД, и Log4Shell на тестовой машине без каких-либо прав будет одинаковым.

В итоге организация получает сотни, иногда тысячи алертов о найденных на ВМ уязвимостях без возможности автоматически определить, какие из них являются действительно важными. Это приводит к ряду серьезных негативных последствий: увеличению времени реагирования на критический инцидент, пропуску важных алертов, повышению расходов, связанных с разбором алертов, и другим.

Общая стоимость владения и покрытие

Подходы, используемые традиционными решениями для получения данных об уязвимостях на ВМ (такие как сканирование с помощью агентов или аутентифицированное сканирование), имеют недостатки, которые особо ярко проявляются в динамично меняющейся облачной среде.

Основными проблемами являются:

- Увеличение стоимости владения ПО для поиска уязвимостей, связанное с необходимостью внедрения и поддержки агентов или специализированных учетных записей на ВМ.
- Снижение покрытия (% инфраструктуры, которую контролирует решение по выявлению уязвимостей) в связи с тем, что агенты или учетные записи не могут быть развернуты на всех ВМ из-за ограничений по причинам производительности, сетевой связности и трудоемкости самого процесса.

Соответствие требованиям

Зачастую ресурсы, развернутые в облаке, обязаны удовлетворять определенным требованиям. Это могут быть требования регулятора (например, ФЗ-152 или PCI-DSS) или требования самой организации (например, требования по безопасности, отказоустойчивости, производительности и инвентаризации).

На данный момент единственный способ проверить выполнение требований - это осуществить проверку вручную. Ручная проверка является трудоемкой процедурой и фиксирует выполнение требований на момент ее выполнения.

Облако имеет динамическую природу и уже через несколько дней или даже часов состояние облачной инфраструктуры может поменяться - некоторые ресурсы могут быть удалены, другие изменят свои свойства, будут созданы новые ресурсы. Данные о соответствии требованиям будут более неактуальны и необходимо будет снова провести трудоемкую и долгую ручную проверку.

Решение

Контроль за конфигурацией

Cloud Advisor включает в себя специализированное средство управления состоянием безопасности облака CSPM (Cloud Security Posture Management). Этот модуль позволяет получать данные о конфигурации облачных сервисов с помощью API облачного провайдера и в автоматическом режиме проверять их на соответствие политике безопасности, сигнализируя пользователю о ее возможных нарушениях и потенциальных угрозах. Cloud Advisor содержит более 1200 политик безопасности и в случае обнаружения ошибок в конфигурации предлагает рекомендации по их исправлению.

> Практически все успешные атаки на облачные сервисы являются результатом их неверной настройки пользователем, неграмотного управления и допущенных ошибок. Менеджеры по безопасности и управлению рисками обязаны инвестировать в процессы и инструменты, обеспечивающие меры безопасности облака, чтобы иметь возможность проактивно и реактивно обнаруживать и устранять эти риски.
>
> Отчет Innovation Insight for Cloud Security Posture Management

Управление уязвимостями

Контекст

Cloud Advisor обладает полной информацией о сетевой связности облачных ресурсов благодаря данным из модуля CSPM. Этот анализ помогает понять какие уязвимости находятся на ресурсах с неограниченным публичным доступом и поэтому должны быть исправлены в первую очередь.

Кроме того, основываясь на данных о правах ресурсов в облаке, Cloud Advisor способен оценивать возможные последствия от их компрометации и поднимать приоритет уязвимостям, обнаруженным на ВМ, имеющих широкие права в облаке (например, доступ к объектному хранилищу или права на запуск других ВМ).

Развертывание и эксплуатация

Cloud Advisor использует уникальную технологию доступа к жестким дискам ВМ, работающих в облаке. В данный момент Cloud Advisor готовит заявку на изобретение, относящееся к этой технологии, для подачи в Роспатент.

Технология, реализуемая решением Cloud Advisor для сбора данных об уязвимостях, является специфичной для облачной среды и основана на создании снимков дисков. Этот подход:

- Обеспечивает 100% покрытие всех виртуальных машин сразу после их развертывания.
- Позволяет развернуть Cloud Advisor за минуты и получить полную информацию обо всех уязвимостях в инфраструктуре в течение нескольких часов.
- Не требует работ по установке и обновлению агентов, снижая общую стоимость владения. Не оказывает влияния на производительность виртуальных машин.
- Не требует сетевой связности между машиной и сканирующим модулем.

В будущем эта технология будет применена для сканирования ВМ и контейнеров на вирусы, поиска секретов, хранящихся в открытом виде и проверки выполнения требований безопасности на уровне ВМ и контейнеров (например, Linux CIS).

Соответствие требованиям

Cloud Advisor позволяет автоматизированно проводить проверку облачной инфраструктуры на соответствие требованиям ФЗ-152, PCI DSS и GDPR и предоставляет отчет о том, какие требования регулятора выполняются, а какие - нет и какие ресурсы нарушают требования.

Cloud Advisor предоставляет возможность формулировать и приводить в исполнение собственные политики в области безопасности, отказоустойчивости, производительности и инвентаризации. Оповещения о нарушении этих политик направляются ответственному по выбранному каналу доставки.

Вывод

Cloud Advisor представляет собой комплексное средство обеспечения безопасности инфраструктуры, расположенной в публичном облаке. Решение обеспечивает контроль за конфигурацией, управление уязвимостями и соответствие требованиям. Cloud Advisor осуществляет контроль инфраструктуры на уровне конфигурации облака, уровне виртуальных машин и уровне кластеров Kubernetes. Благодаря технологии безагентного анализа данных с учетом контекста решение обеспечивает быстрое развертывание, широкое покрытие и корректную приоритизацию алертов.