McAfee Public Cloud Server Security Suite

Комплексная защита облачных рабочих нагрузок в AWS и Azure

Ключевые преимущества

- Предназначен для рабочих нагрузок AWS и Azure
- Мгновенное обнаружение рабочих нагрузок
- Оценка уровня защищенности систем и устранение угроз
- Масштабируемость средств защиты
- Комплексная защита
- Использование консоли управления McAfee® ePolicy Orchestrator® (McAfee ePO™)
- Возможность развертывания с помощью Chef, Puppet и OpsWorks
- Подтверждение соответствия нормативно-правовым требованиям
- Интеграция с другими решениями Intel Security

Переходя на использование экземпляров облачных серверов, размещенных в публичном облаке, в качестве дополнительных, а нередко даже основных компонентов своих центров обработки данных, предприятия отдают себе отчет в том, что одним из ключевых факторов успеха такой стратегии является наличие модели разделения ответственности[1]. Поставщики публичных облачных сред, такие как Amazon Web Services (AWS) и Microsoft Azure, обеспечивают защиту периметра, а защиту содержимого должны обеспечивать пользователи. Поэтому перед дальновидными предприятиями встает вопрос о том, как обеспечить защиту нагрузок в облаке от угроз «нулевого дня» и постоянных угроз повышенной сложности, сохраняя при этом расходы на уровне, соответствующем их стратегии использования облачных технологий. Вот некоторые из основных проблем, с которыми сталкиваются предприятия, начинающие использовать облачные технологии:

- Предприятиям становится труднее справляться со сложными угрозами и угрозами «нулевого дня».
- Отсутствие централизованного управления и возможности собирать информацию о происходящем крайне осложняет работу с инфраструктурой, состоящей из большого числа разных облачных технологий.
- Для систем обеспечения безопасности рабочих нагрузок в облаке актуальна проблема снижения быстродействия.

McAfee® Public Cloud Server Security Suite позволяет мгновенно обнаруживать рабочие нагрузки и угрозы безопасности в AWS и Azure и брать их под контроль с целью обеспечения полной, единообразной и непрерывной защиты с минимальным снижением быстродействия. С помощью данного комплекта решений вы сможете обнаруживать разные облачные центры обработки данных, облачные учетные записи, виртуальные машины и новейшие угрозы безопасности.

Комплект McAfee Public Cloud Server Security Suite включает в себя обязательные средства антивирусной защиты и предотвращения вторжений, а также усовершенствованную технологию белых списков (для защиты от угроз «нулевого дня»), средства контроля за изменениями (для выполнения нормативно-правовых требований) и механизм управления шифрованием (для защиты данных). Наличие единой консоли управления дает возможность легко управлять большим количеством облачных технологий и применять политики. Возможность проводить развертывание в соответствии с методологией DevOps, используя Chef, Puppet и OpsWorks, позволяет автоматизировать процесс развертывания и свести к минимуму потери производительности.

intel Security

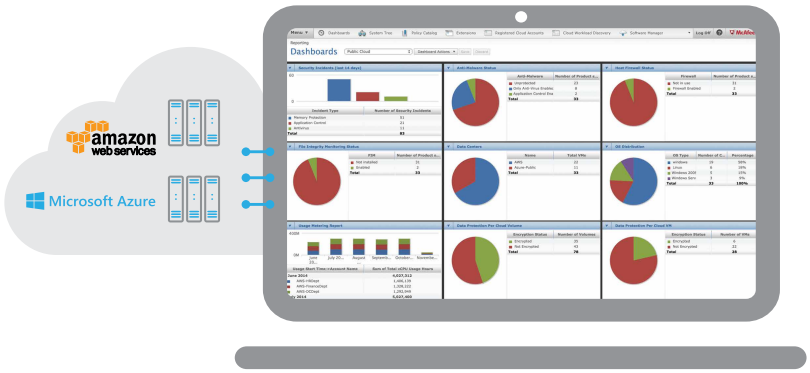

Рис. 1. Единая консоль для управления большим количеством разных облачных инфраструктур и разных технологий Intel Security

Поддерживаемые платформы

- Windows Server 2008, 2008 R2, 2012, 2012 R2
- Linux (Red Hat, CentOS, SUSE, Ubuntu, Amazon Linux)

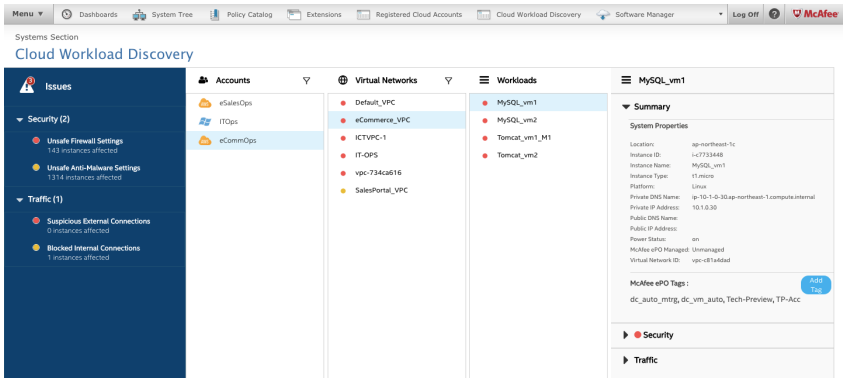

Рис. 2. Обнаружение и мониторинг большого количества разных облачных инфраструктур и новейших угроз

Дополнительная информация

Страница продукта: **www.mcafee.com/ru/products/public-cloud-server-security-suite.aspx**.

Данный продукт можно также приобрести в **AWS Marketplace**.

Обнаружение облачных инфраструктур и угроз

Для повышения эффективности контроля над облачными инфраструктурами и угрозами безопасности необходимо оптимизировать сбор информации о том, что происходит в этих инфраструктурах.

- Данный продукт позволяет за считанные минуты обнаруживать все виртуальные сети (виртуальные частные облака, VPC), шаблоны и рабочие нагрузки в облачных инфраструктурах AWS и Azure. Обеспечение адекватной защиты облачной инфраструктуры требует принятия следующих первоочередных мер: сбор подробной информации обо всех учетных записях в облачной инфраструктуре; сбор информации о том, какие пользователи имеют доступ к отдельным сегментам облачной инфраструктуры; анализ того, как происходит распределение рабочих нагрузок по шаблонам и VPC; и получение общего представления о дереве систем в облачной инфраструктуре.
- Сбор информации о происходящем в разных облаках осуществляется централизованно. Использование комплексной информации об угрозах (включая информацию об источниках атак) позволяет повысить уровень защиты.
- Возможность отслеживать трафик на всех рабочих нагрузках позволяет управлять потоками информации между ними и доступом к этой информации из-за пределов организации.

Мониторинг облака и быстрое реагирование на оповещения системы безопасности

В сегодняшних условиях все большее значение приобретает скорость восстановления систем и устранения уязвимостей. Данное решение позволяет быстро оценивать проблемы безопасности на более глубоком уровне и незамедлительно принимать меры реагирования.

- Цветовая кодировка обнаруженных угроз дает возможность выделять угрозы, требующие неотложного внимания, и принимать соответствующие меры.
- При необходимости администратор может создавать собственные теги и присваивать их рабочим нагрузкам.
- Администратор может принимать корректирующие меры, необходимые для устранения проблем безопасности, а также защищать инфраструктуру от будущих инцидентов с помощью таких инструментов, как политики и репутация угроз.
- Управление облачным брандмауэром осуществляется с помощью индивидуальных политик, создаваемых для отдельных рабочих нагрузок или групп рабочих нагрузок. Управление политиками групп безопасности AWS позволяет брать под контроль трафик одного или нескольких экземпляров.
- Возможность выявлять подозрительный трафик в VPC позволяет принимать меры реагирования, необходимые для защиты критически важной информации от несанкционированного доступа.

Комплексная защита от угроз

В McAfee Public Cloud Server Security Suite используется один-единственный агент, обеспечивающий несколько уровней защиты, управление которыми осуществляется с помощью единой консоли управления независимо от количества облачных платформ. Для оптимизации работы с данным решением его развертывание можно также проводить с помощью инструментов, позволяющих использовать методологию DevOps.

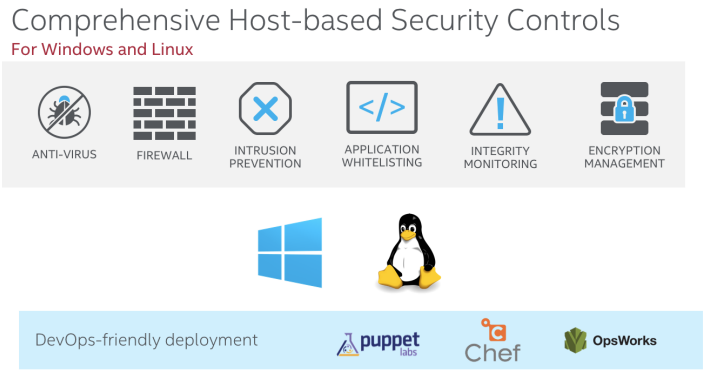

Рис. 3. Комплексная защита рабочих нагрузок в публичных облаках

Функция	Преимущества
Возможность развертывания с помощью Chef, Puppet и AWS OpsWorks	• Развертывание данного решения с помощью инструментов, позволяющих использовать методологию DevOps, не только облегчает процесс развертывания, но и дает возможность заранее учесть вопросы безопасности. • Обеспечение безопасности может быть встроено в процесс эксплуатации.
Обнаружение рабочих нагрузок в облаке	• Мгновенный сбор информации о происходящем в облачных инфраструктурах позволяет обнаруживать виртуальные центры обработки данных, облачные рабочие нагрузки и облачные брандмауэры. • Быстрая доставка предупреждений об угрозах и автоматическая оценка уровня защищенности. • Более оперативное устранение угроз благодаря наличию приоритизированных предупреждений, приоритет которых определяется исходя из степени серьезности угроз и наличия возможностей для быстрого принятия мер реагирования.
Единая консоль управления разными решениями для защиты облачных инфраструктур (программное обеспечение McAfee ePO)	• Огромное преимущество при использовании гибридной среды. • Управление физическими, виртуальными и облачными рабочими нагрузками и политиками осуществляется посредством одной-единственной панели. • Интеграция облачных и локальных защитных технологий Intel Security и компаний-партнеров. • Наличие встроенных процессов обеспечения безопасности и возможность быстро принимать меры реагирования ведут к снижению совокупной стоимости владения решением.
Защита от вредоносных программ	• Максимальная защита от вредоносных программ: защита систем и файлов от вирусов, шпионских программ, червей, троянов и других рисков; обнаружение и удаление вредоносных программ; возможность для пользователей легко настраивать политики для управления объектами, находящимися в карантине.
Брандмауэр на узле	• Защита рабочих нагрузок от несанкционированного доступа и атак.
Предотвращение вторжений на узел	• Блокирование нежелательного и вредоносного сетевого трафика и упреждающее блокирование атак «нулевого дня» и известных атак с помощью запатентованной технологии, удостоенной отраслевых наград. • Ограничение доступа к отдельным портам, файлам, общим папкам, ключам реестра и значениям реестра позволяет защитить рабочие нагрузки от внесения нежелательных изменений. • Средства защиты памяти не дают аномальным программам и угрозам выходить за границы буфера и перезаписывать соседние сегменты памяти при записи данных в буфер. Переполнение буфера представляет собой уязвимость, позволяющую злоумышленникам запускать на уязвимом компьютере какой угодно код.
Белые списки приложений	• Защита от угроз «нулевого дня» и постоянных угроз повышенной сложности, не требующая обновления сигнатур. • Повышение уровня защиты и сокращение стоимости владения благодаря использованию динамических белых списков, автоматически принимающих новое программное обеспечение, если оно установлено по доверенным каналам. • Сокращение количества циклов установки исправлений благодаря использованию белых списков приложений и передовой технологии защиты памяти.
Мониторинг целостности файлов	• Мониторинг целостности файлов позволяет непрерывно отслеживать изменения, вносимые на системном уровне в любой точке распределенной сети, включая удаленные объекты. • Предотвращение внесения несанкционированных изменений в критически важные системные файлы, каталоги и настройки. • Отслеживание и проверка в режиме реального времени всех попыток внесения изменений на вашей рабочей нагрузке, с соблюдением политики изменений по временному интервалу, источнику или уведомлению о разрешении изменений.
Управление шифрованием	• Шифрование данных, хранящихся в томах AWS EBS, осуществляется с помощью AWS Advanced Encryption Standard (AES). • Удобство шифрования томов, на которых уже есть данные. • Интеграция со службой управления ключами шифрования AWS Key Management Service (KMS).

1. **http://www.mcafee.com/ru/resources/white-papers/wp-cloud-security-primer-techtarget.pdf**

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