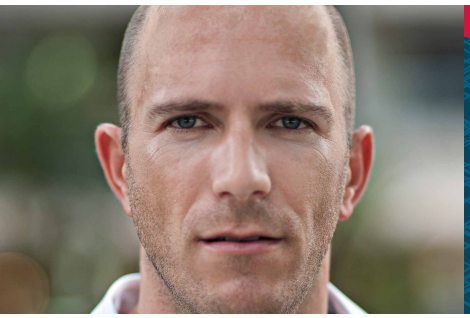

Пять основных аргументов в пользу развертывания специализированного решения для защиты баз данных

Создание критически важной последней линии обороны

Защита ценной и конфиденциальной информации, хранящейся в базах данных, является жизненно важным условием сохранения неприкосновенности и репутации организаций в любой стране мира, не говоря уже о выполнении требований нормативно-правового соответствия. Однако многие организации до сих пор используют средства защиты, возможности которых изначально ограничены. Учитывая высокую степень сложности современных баз данных и изощренность действий современных киберпреступников, развертывание комплексного специализированного решения для защиты баз данных является насущной необходимостью. Приведем пять аргументов в поддержку этого утверждения.

Преимущества McAfee Vulnerability Manager for Databases

- Обеспечивает полный сбор информации о состоянии безопасности базы данных
- Проверяет многочисленные базы данных всего предприятия с централизованной консоли
- Сокращает время на обеспечение соответствия нормам и ограничивает до минимума циклы аудита, позволяя экономить значительные средства
- Может быть быстро развернут, для чего требуются минимальные знания СУБД
- Быстро генерирует специализированные отчеты для разных пользовательских ролей в простых для понимания форматах

Преимущества McAfee Database Activity Monitoring

- Максимально повышает уровень визуального контроля и защиты от всех источников атак
- Отслеживает внешние угрозы, угрозы от привилегированных пользователей информационных систем и изощренные атаки, организуемые изнутри баз данных
- Снижает риск и ответственность путем предотвращения атак до причинения ими ущерба
- Экономит время и деньги благодаря более быстрому развертыванию и более эффективной архитектуре
- Обеспечивает гибкость, позволяющую вам легко развернуть выбранную ИТ-инфраструктуру

1. Нельзя защитить актив, о существовании которого вы не знаете

Даже в ИТ-средах корпораций с чрезвычайно жесткими внутренними правилами нередко можно встретить сотни, а иногда и тысячи экземпляров баз данных с очень конфиденциальной информацией, точное количество, местоположение, степень конфиденциальности и уровень защищенности которых не известны даже сотрудникам ИТ-подразделений. И хуже всего то, что киберпреступники знают об этом и постоянно ищут слабые места. У них есть время и технические ресурсы, необходимые для взлома тех баз данных, в безопасности которых вы были уверены или о существовании которых вы даже не знали. Ваша неинформированность играет им на руку.

Информация об имеющихся у вас базах данных может быть полной только в том случае, если у вас есть возможность обнаружить все имеющиеся в вашей среде базы данных и проверить их содержимое на наличие информации о платежных картах, персональных данных сотрудников, статистики продаж и иной конфиденциальной информации. Помимо этого, для точного определения характера ваших рисков необходимо иметь автоматизированные средства глубокого тестирования баз данных на наличие уязвимостей. Только специализированное решение для защиты баз данных может дать вам возможность получать детальную информацию, позволяющую приоритезировать и устранять бреши в защите, что также избавит вас от необходимости пользоваться дорогостоящими услугами стороннего консультанта по безопасности.

McAfee® Vulnerability Manager for Databases автоматически обнаруживает все базы данных, имеющиеся в вашей сети, определяет, установлены ли новейшие пакеты исправлений, и проводит проверку на наличие уязвимостей. McAfee Vulnerability Manager проводит более 4 200 тестов на наличие уязвимостей в основных разновидностях баз данных, классифицирует угрозы по отдельным уровням приоритета, а затем предлагает сценарии устранения уязвимостей и необходимые рекомендации. Решение требует минимальных знаний в области систем управления базами данных, позволяет настраивать и генерировать отчеты для разных пользовательских ролей в простых для понимания форматах и имеет централизованную консоль для управления всеми указанными функциями.

2. Средства защиты на периметре не защищают от внутренних угроз

Вы затратили много времени, усилий и капитала для выбора и развертывания межсетевых экранов и других средств обеспечения сетевой безопасности. Однако, как вам известно, не все случаи взлома баз данных берут начало за пределами периметра. Согласно результатам исследований, ежегодно проводимых группой CERT (Computer Emergency Response Team), число случаев взлома баз данных, причиной которых являются действия внутренних пользователей, может составлять до половины всех прецедентов. Т. е. вам нужно обеспечить защиту своих критически важных данных еще и от внутреннего, более коварного врага в лице сотрудников вашей компании, имеющих права доступа и знающих, как обойти встроенные функции безопасности систем управления базами данных (СУБД), как подделать журналы доступа и как скрыть свои следы.

Правильно выбранное решение для защиты баз данных обеспечит обнаружение и предотвращение угроз по всем возможным векторам, берущим начало не только за пределами, но и прежде всего внутри компании. Кроме того, оно предоставит вам платформу для создания и применения политик доступа к базам данных в соответствии с конкретными нормативно-правовыми требованиями, что позволит обеспечить подлинное и непрерывное разграничение обязанностей.

McAfee Database Activity Monitoring автоматически обнаруживает базы данных в вашей сети, обеспечивает их безопасность с помощью набора заранее сконфигурированных средств защиты и помогает создать индивидуальную политику безопасности для вашей среды, что упрощает декларирование нормативного соответствия при аудитах и повышает уровень защиты критически важных данных. Решение McAfee Database Activity Monitoring дает возможность получать информацию обо всех действиях, связанных с базами данных, включая локальный привилегированный доступ и изощренные атаки, исходящие изнутри базы данных. Оно обеспечивает защиту ваших данных от любых угроз с помощью локального мониторинга активности на каждом сервере баз данных независимо от его местоположения, что позволяет рассылать предупреждения или автоматически завершать сеансы, имеющие подозрительный характер или каким-либо образом нарушающие политику безопасности. McAfee Database Activity Monitoring обеспечивает безопасность ваших баз данных и применение ваших политик даже в виртуальных и облачных вычислительных средах.

3. Злоумышленники атакуют быстрее, чем вы устанавливаете исправления

«Вторник исправлений» (Patch Tuesday) следует сделать официальным праздником — Днем хакеров. Каждый месяц в этот день поставщики баз данных раскрывают самые привлекательные цели для атак. Более того, «вторник исправлений» дает злоумышленникам преимущество, потому что они знают, что ваши сотрудники, отвечающие за управление базами данных, должны будут потратить немало времени на отключение баз данных, установку пакетов исправлений и их тестирование. Собственно, злоумышленники и рассчитывают на то, что процесс установки исправлений покажется вам такой значительной помехой в работе, что вы решите отложить его на столько, на сколько возможно, и в результате злоумышленники получат достаточно времени, чтобы найти возможность для проникновения в ваши базы данных.

Единственной альтернативой традиционному процессу установки исправлений, дающему преступникам вышеуказанные преимущества, является использование специализированного решения для защиты баз данных. Такое решение должно давать вам возможность устанавливать критические обновления ваших баз данных в режиме реального времени, без стресса для сотрудников и без помех в работе вашей компании.

Решение McAfee Virtual Patching for Databases ограждает базы данных от риска, связанного с наличием неустраненных уязвимостей, в режиме реального времени обнаруживая и блокируя попытки атак и вторжений без необходимости временно отключать базы данных и тестировать приложения. Оно избавляет вас от тревог, поскольку вы знаете, что защищены от угроз даже в периоды наибольшей уязвимости, то есть в периоды между выпуском пакетов исправлений и их установкой.

Еще одним неинтрузивным решением, дающим дополнительный слой защиты не только во «вторник исправлений», но и в остальное время, является McAfee Database Activity Monitoring. Используя расположенные в памяти датчики, оно перехватывает атаки на базы данных, исходящие из любой точки сети, от вошедших на сам сервер локальных пользователей и даже изнутри баз данных (в результате активации хранимых в них процедур или триггеров).

4. Нельзя постоянно жертвовать нормативно-правовым соответствием ради непрерывности работы

Нормативно-правовые требования, действующие в здравоохранении, финансовом секторе и розничной торговле постоянно изменяются, становясь все более и более жесткими. Поэтому не удивляет тот факт, что к базам данных, имеющим критически важное значение для коммерческой деятельности, применяются методы обеспечения нормативно-правового соответствия, требующие обязательной установки новейших пакетов исправлений, выпускаемых поставщиками СУБД. Но поскольку временное отключение, обновление и последующее тестирование нескольких баз данных различных типов — процесс трудоемкий, большинство организаций жертвуют нормативно-правовым соответствием ради обеспечения бесперебойности работы. Более того, на фирмах и предприятиях могут до сих пор использоваться устаревшие базы данных, пакеты исправлений для которых уже даже не выпускаются.

Решение McAfee Virtual Patching for Databases дает вам возможность поддерживать бесперебойный ход работы, не принося в жертву нормативно-правовое соответствие. Благодаря ему вы можете как и прежде устанавливать пакеты исправлений по заранее намеченному вами расписанию, зная, что ваши базы данных защищены и соответствуют нормативно-правовым требованиям. Решение McAfee Virtual Patching for Databases позволяет значительно экономить время и является признанным компенсирующим средством защиты с точки зрения аудиторов, контролирующих нормативно-правовое соответствие. К тому же оно может обеспечить надежную защиту устаревших баз данных, которые больше не поддерживаются поставщиками СУБД.

Преимущества McAfee Virtual Patching

- Защита от угроз обеспечивается еще до установки пакетов исправлений от производителя
- Специалистам по ИТ и безопасности не требуется хорошо разбираться в конкретной СУБД
- Неинтрузивный характер программного обеспечения позволяет не переводить рабочие базы данных в автономный режим
- Автоматическая установка обновлений позволяет обеспечить непрерывную защиту баз данных
- Облегчает обеспечение соответствия требованиям таких стандартов, как PCI DSS, HIPAA и др.

Преимущества McAfee ePolicy Orchestrator

- Сбор полной информации о степени защищенности и нормативно-правовом соответствии баз данных при помощи централизованной консоли управления
- Наличие единого окна для представления информации позволяет легко объединить различные базы данных в рамках одной программы управления вне зависимости от того, где они расположены: локально, на удаленных ресурсах или даже в «облаке»
- Открытая и расширяемая архитектура позволяет объединить средства управления решениями McAfee и сторонних поставщиков с вашим LDAP-приложениями, ИТ-процессами и средствами управления конфигурацией

5. Если данные находятся в «облаке», то контроль за ними очень ограничен

«Облако» дает огромные преимущества с точки зрения расходов на ИТ и эксплуатационной эффективности, но здесь, как вы знаете, есть и своя ловушка: ваши сотрудники могут потерять контроль над конфиденциальными данными и почти полностью лишиться возможности отслеживать, кто получает к ним доступ. Однако использование правильного решения для защиты баз данных позволяет обеспечить защиту данных как в физических, так и виртуальных средах. Правильное решение может предотвращать несанкционированные действия в базах данных и посылать отчеты на вашу консоль управления даже в том случае, если используемая вами база данных является виртуальной и находится в «облаке».

McAfee Database Activity Monitoring, с его уникальной реализацией расположенного в памяти датчика, можно настроить таким образом, чтобы его установка производилась автоматически вместе с каждой новой виртуальной машиной. При установке оно может запросить политики безопасности, касающиеся расположенных на виртуальной машине данных, а затем начать рассылку уведомлений на сервер управления. Более того, его датчики могут функционировать автономно даже будучи отключенными от сервера, обеспечивая тем самым защиту и сохранность конфиденциальных данных независимо от того, в каком режиме (сетевом или автономном) работает база данных и где она расположена в данный момент времени. Даже в случае прерывания сетевого соединения данные все равно находятся под защитой, так как датчик внедряет политику безопасности локально, и оповещения попадают в очередь для доставки после того, как сервер снова станет доступен.

Кроме того, мониторинг доступа к вашим «облачным» базам данных можно осуществлять с помощью программного обеспечения McAfee® ePolicy Orchestrator® (McAfee ePO™), которое предоставляет в ваше распоряжение консоль управления корпоративной системой безопасности, дающую возможность полного сбора информации о степени защищенности баз данных, об уровне корпоративной безопасности и о нормативно-правовом соответствии.

Другими словами, вы получаете максимальную возможность сбора информации о происходящем независимо от того, используете вы «облачные» решения или нет. Мы видим, что McAfee предлагает правильное решение для защиты баз данных в вашей ИТ-среде независимо от масштаба ваших операций и степени конфиденциальности ваших данных.

Дополнительная информация о том, как поддерживать безопасность и работоспособность баз данных

Мы, сотрудники McAfee, понимаем, что в ваших базах данных хранятся самые важные бизнес-активы вашей компании. Чтобы ваша компания могла работать бесперебойно, они должны быть доступны круглосуточно. И поскольку ваши базы данных не берут выходных, не берем выходных и мы. Вот почему мы говорим, что безопасность всегда начеку. Вы можете быть уверены в том, что наши специалисты по защите баз данных беспрерывно занимаются задачей обеспечения безопасности и доступности ваших конфиденциальных данных и при этом помогают вашей компании обеспечивать соответствие внутренним политикам и отраслевым нормативным требованиям.

За дополнительной, более подробной информацией о том, какую помощь средства McAfee для защиты баз данных могут оказать в деле обеспечения безопасности ваших критически важных баз данных, посетите наш веб-сайт www.mcafee.com/ru/products/database-security/index.aspx или же обратитесь либо к своему региональному представителю McAfee, либо к реселлеру McAfee.

Подпишитесь на нас в Twitter: @McAfee_DBSecure.

О решениях McAfee для обеспечения безопасности конечных точек

McAfee — стопроцентная дочерняя компания Intel Corporation (NASDAQ: INTC), является крупнейшим в мире предприятием, специализирующейся на технологиях информационной безопасности. Наши решения следующего поколения для обеспечения безопасности конечных точек гарантируют безопасность всех ваших устройств, данных проходящих через эти устройства и приложений, установленных на устройствах. Наши комплексные и индивидуально настраиваемые решения понижают уровень сложности, позволяя создать многоуровневую систему защиты конечных точек и при этом избежать падения производительности. Они представляют собой совершенное сочетание традиционных интеллектуальных средств поиска вредоносных программ, динамических белых списков, бихевиористических средств предотвращения вторжений «нулевого дня», единых механизмов управления и интегрированных средств сбора информации об угрозах. Для получения подробной информации посетите страницу www.mcafee.com/ru/products/endpoint-protection/index.aspx.

Преимущества решения McAfee для защиты баз данных

- Легкость в развертывании и управлении
- Обеспечение полного сбора информации о степени защищенности баз данных
- Согласование практики администрирования политик безопасности между сотрудниками, занимающимися управлением средствами защиты и базами данных
- Эффективное обеспечение нормативно-правового соответствия
- Снижение риска и ответственности путем предотвращения атак до причинения ими ущерба
- Управление безопасностью баз данных с централизованной консоли

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
Бизнес центр «Башни на набережной»
4ый этаж, офис 405 – 409
Телефон: +7 (495) 967 76 20
Факс: +7 (495) 967 76 00
www.McAfee.ru

41903brf_top5-db-sec_0212_fnl_ASD