IMPERVA®

Решение по безопасности данных Imperva SecureSphere

DATASHEET

Защищать и проводить аудит критичных данных

Постоянное подключение к сети и легкость доступа в интернет породили совершенно новые формы киберпреступности. В результате этого изменились взгляды потребителей, представителей бизнеса и правительственных структур на ответственность по защите критичных данных. В дополнение к расходам на расследования, штрафам за несоответствие регулирующим требованиям и потенциальному репутационному ущербу появился еще один повод для беспокойства. Недавнее постановление суда[1] изменило определение «ущерба клиента», расширив возможности инициирования судебных действий со стороны клиентов, чьи персональные данные были похищены в результате взлома. Ответственность компаний, потерявших данные в результате инцидентов безопасности, экспоненциально выросла за счет расширения понятия ущерба, увеличения судебных издержек и компенсационных выплат.

Ответственность компаний, потерявших данные в результате инцидентов безопасности, экспоненциально выросла за счет расширения понятия ущерба, увеличения судебных издержек и компенсационных выплат.

Лучшее в своем классе решение по защите данных и аудиту

Imperva – это выбор премиум-класса для защиты критичных для бизнеса данных и приложений в облачных средах и на собственных площадках клиентов. Решения по защите данных SecureSphere покрывает все аспекты безопасности баз данных и соответствия регулирующим требованиям, используя лучшие в индустрии механизмы аудита баз данных, защиты в реальном времени, не приводящие к потере производительности или доступности. С помощью многозвенной архитектуры SecureSphere может масштабироваться для поддержки самых больших баз данных и систем больших объемов данных. Учитывая автоматизацию защиты данных и соблюдения соответствия регулирующим требованиям, неудивительно, что тысячи компаний выбирают Imperva SecureSphere для обеспечения безопасности своих наиболее ценных активов.

[1] 7ой Окружной Апелляционный суд, судья Дайана Вуд (Diane Wood), истцы выиграли дело о взломе данных в Neiman Marcus.

Решение по защите данных Imperva SecureSphere

- Анализирует и помогает в классификации критичных баз данных;
- Идентифицирует пользователей с избыточными правами и «спящих» пользователей, что позволяет проводить регулярные циклы пересмотра прав;
- Защищает РСУБД, хранилища данных, платформы большого объема информации (Big Data) и базы данных мейнфреймов;
- Выявляет, изолирует и блокирует атаки на базы данных и неавторизованные действия в реальном времени;
- Автоматизирует и производит на регулярной основе действия по проверке соответствия регулирующим требованиям и выпуск отчетов.

Защищать данные в их источнике

SecureSphere обеспечивает мониторинг защиты данных и независимое журналирование аудита на соответствие регулирующим требованиям.

- Запись в журнал только необходимой информации об активности при проведении мониторинга всех действий на предмет нарушения безопасности;
- Мониторинг и защита баз данных с высоким уровнем транзакций;
- Блокировка подозрительных действий в момент, когда они происходят, – проведение контекстного расследования;
- Выполнение многовекторных сигналов безопасности, устраняя узкие места и задержки;
- Взаимосвязь защиты базы данных межсетевым экраном веб-приложений SecureSphere Web Application Firewall, системой защиты Account Take-over Protection и решением по защите от вредоносного программного обеспечения для обеспечения многофакторной безопасности.

Соответствие регулирующим требованиям

SecureSphere помогает организациям выполнить регулирующие требования, в том числе такие как PCI DSS, SOX, My Number и HIPAA.

- С помощью предопределенных политик и отчетов покрывает практически все регулирующие требования для баз данных;
- Быстрая конфигурация и развертывание новых и модифицированных политик: не требуется вмешательство администратора баз данных;
- Обеспечивает разделение ролей с использованием защищенных от подделки данных аудита;
- Обновления в режиме «на ходу» и «звонок домой» минимизируют необходимость перезапуска системы и вызванных ими пробелов в данных аудита;
- Гибкость и адаптивность для соответствия изменяющимся ИТ-средам и регулирующим требованиям.

Защита данных и аудит необходимы всей компании

Хакерам и лицам, совершающим кражу информации, нет дела до того, кто отвечает за информационную безопасность или за соблюдение регулирующих требований в компании. Их намерение – украсть данные в личных целях. Использование многовекторных атак показывает как злоумышленники обходят системы защиты, используя барьеры, существующие между командами и системами. Атака «распределенный отказ в обслуживании» отвлекает внимание, в то время как другой вектор атаки использует для получения тысяч записей данных слабости в идентификационной информации пользователей, выявленные с помощью направленного фишинга электронной почты и вредоносного ПО. Остановить кражу данных только лишь с помощью ручного мониторинга и изолированных решений не представляется возможным. Корреляционные панели могут помочь в этой задаче, но когда тревожные сообщения переполняют систему, реальная атака может продолжаться незамеченной неделями и более. Проактивный мониторинг безопасности, развернутый на уровне данных, – это последняя возможность остановить атаку на данные во время ее проведения. Когда такая система интегрирована с МСЭ веб-приложений, решениями по защите от вредоносного ПО и другими механизмами защиты, шансы на сохранение безопасности данных смещаются в пользу компании. Планы похитителей данных сорваны; команды ИТ, безопасности и соответствия регулирующим требованиям могут констатировать, что совместно они достигли своих целей по поддержанию безопасности данных и продемонстрировали, что они могут делать это в соответствии с определенными полномочиями и требованиями регуляторов.

Решение SecureSphere Database Assessment находит места размещения критичных данных и предоставляет систему приоретизации связанных с ней рисков, что помогает компаниям планировать мероприятия, системы и политики, направленные на снижение рисков.

Возможности Imperva по защите данных

Защита данных начинается с их обнаружения

Для того чтобы защищать и мониторить данные, необходимо обнаружить и классифицировать. В компаниях малого размера это может буть сделано путем ручного просмотра и опросов, однако при росте компании количество баз данных растет практически экспоненциально. Автоматизированное обнаружение данных и их классификация в этом случае становится единственным надежным способом на постоянной основе с высокой степенью надежности обнаруживать и классифицировать новые или модифицированные базы данных, содержащие до этого неизвестную критичную информацию. Решение SecureSphere Database Assessment находит места размещения критичных данных и предоставляет систему приоретизации связанных с ней рисков, что помогает компаниям планировать мероприятия, системы и политики, направленные на снижение рисков.

Постоянный мониторинг использования критичных данных

Даже при большом потоке информации баз данных SecureSphere одновременно мониторит весь трафик на предмет нарушений политик безопасности и в целях соответствия регулирующим требованиям. Такой высокоэффективный мониторинг в различных целях позволяет компаниям удовлетворять различные требования как безопасности, так и соответствия регулирующим стандартам, используя единое унифицированное решение.

SecureSphere анализирует всю активность баз данных в реальном времени, предоставляя организациям проактивный слой контроля исполнения требований безопасности и механизм детального аудита, показывающий информацию о том «кто, что, когда, где и как» для каждой транзакции. SecureSphere позволяет проводить аудит привилегированных пользователей, которые имеют доступ непосредственно к серверу баз данных, так же как и пользователей, получающих доступ через браузеры, мобильные приложения или приложения, работающие на рабочих станциях.

Мониторьте Big Data, SharePoint и файловые хранилища

В то время как базы данных остаются главной целью компьютерных краж, критичные данные существуют также и в других типах информационных систем предприятия. SecureSphere автоматизирует наиболее трудные аспекты развертывания унифицированных политик и мониторинга всех баз данных, систем больших объемов информации (Big Data), систем SharePoint и файловых хранилищ.

- SecureSphere Agent for Big Data расширяет применение SecureSphere Data Activity Monitor на ведущие платформы Big Data, включая MongoDB, Cloudera, IBM BigInsights и продукты Hortonworks.
- Продукты SecureSphere File Security позволяют в реальном времени проводить мониторинг, аудит, управление безопасностью и правами пользователей для файлов, расположенных в системах SharePoint, файловых серверах и сетевых системах хранения (NAS).

В отличие от решений, которые требуют участия администратора баз данных и опираются на дорогостоящие профессиональные сервисы, SecureSphere предоставляет необходимые возможности централизации и управления тысячами баз данных, узлами хранения больших объемов информации, репозиториями файлов.

Обнаружение неавторизованного доступа и мошеннической деятельности

SecureSphere идентифицирует профили типичного доступа пользователей к данным, применяя патентованный Метод Динамического Обучения (Dynamic Learning Method, DLM) и технологию Адаптивного Профилирования Нормального Поведения (Adaptive Normal Behavior Profile, NBP). Это позволяет установить базовый уровень для всей пользовательской активности, включая действия DML, DDL, DCL, действия «только чтения» (SELECT) и использование хранимых процедур. SecureSphere обнаруживает отличия в действиях пользователей, совершающих необычные запросы, и сигнализирует о них системе для принятия дальнейших мер по расследованию или блокировке таких действий.

Многовекторные сигналы безопасности, временные карантины и, если это необходимо, блокировка неавторизованных действий – все это может использоваться для защиты данных без деактивации учетной записи пользователя во избежание потенциальных перебоев в критичных бизнес-процессах. Автоматизированные процессы реагирования передают многовекторные сигналы безопасности, которые отсылают информацию в такие системы, как SPLUNK, систему управления событиями информационной безопасности (SIEM), систему тикетов или в другие системы третьих производителей для организации процессов более широкого расследования инцидента.

Унифицированная система развертывания и обеспечения соблюдения политик

Другим преимуществом SecureSphere является встроенная экспертная система. Многие компании пытаются поддерживать на достаточном уровне собственные ресурсы, имеющие навыки, необходимые для развертывания и эксплуатации сложных систем безопасности и аудита данных. Удачная реализация контроля доступа и процессов аудита требует их воспроизводимости. Централизованное управление аудитом и оценка гетерогенных систем упрощает управление такими процессами, в то же время автоматизация уменьшает объем ресурсов, необходимых для поддержания соответствия регулирующим требованиям и увеличивает возврат инвестиций.

В отличие от решений, которые требуют участия администратора баз данных и опираются на дорогостоящие профессиональные сервисы, SecureSphere предоставляет необходимые возможности централизации и управления тысячами баз данных, узлами хранения больших объемов информации, репозиториями файлов. Предустановленные политики, процессы реагирования на инциденты и сотни отчетов существенно снижают необходимость в написании сценариев SQL и наличии экспертизы по регулирующим требованиям. Отсутствие необходимости постоянного участия администратора баз данных позволяет соответствовать требованиям по разделению полномочий. Используя готовые процессы с интерфейсом прикладного уровня (API), консоль управления, рабочие процессы, отчеты и инструменты анализа существующий персонал может осуществить развертывание системы и успешно ее эксплуатировать.

Упрощение отчетности по соответствию требованиям

Imperva SecureSphere содержит сотни предустановленных форм отчетов наиболее востребованных нашими клиентами. Кроме того, решение содержит кастомизированный инструмент написания отчетов для создания документов, специфических для данного предприятия. Встроенные рабочие процессы и средства автоматизации позволяют быть уверенным в том, что задачи по контролю соответствия регулирующим требованиям и отчетности будут выполнены в срок по всему объему данных.

Остановка атак в реальном времени является единственным эффективным методом предотвращения кражи ваших данных хакерами. SecureSphere производит мониторинг всего трафика относительно нарушений политик безопасности для обнаружения атак на протоколы и операционную систему, а также неавторизованных SQL действий.

Эффективное управление правами пользователей по всем базам данных

Практически любой регулирующий документ содержит требование по управлению правами доступа пользователя к критичным данным. Соответствие этому требованию является одной из наиболее сложных задач для современного предприятия, если она выполняется в ручном режиме на больших объемах данных. SecureSphere автоматически агрегирует права пользователей на различных гетерогенных хранилищах данных и помогает установить автоматизированный процесс пересмотра прав пользователей для предотвращения их избыточности. Это помогает выполнить рутинную задачу в рамках соответствия таким стандартам, как SOX и PCI DSS. Автоматизация этих приземленных, но очень важных задач, снижает затраты на персонал и уменьшает риск возникновения ошибок или пробелов в отчетности.

Блокировка в реальном времени SQL инъекций, «отказов в обслуживании» и других атак

Остановка атак в реальном времени является единственным эффективным методом предотвращения кражи ваших данных хакерами. SecureSphere производит мониторинг всего трафика относительно нарушений политик безопасности для обнаружения атак на протоколы и операционную систему, а также неавторизованных SQL действий. Высокоэффективный механизм мониторинга позволяет подвергать карантину (путем временной задержки действий пользователя до подтверждения его прав) или блокировать такие действия без прерывания бизнес-процесса из-за полной блокировки учетной записи пользователя.

Блокировка возможна как на уровне агента базы данных, так и на сетевом уровне, что позволяет производить тонкую настройку профиля безопасности для баланса требований по обеспечению полной защиты данных и необходимости поддержания производительности критичных баз данных с высоким объемом транзакций.

Для того чтобы реально увеличить уровень проактивной безопасности, установите МСЭ веб-приложений Imperva SecureSphere, использующий ту же архитектуру и платформу управления, что и решение по защите данных SecureSphere. Дополнительная интеграция с решениями по защите от вредоносного ПО, системой управления событиями информационной безопасности (SIEM) и другими специализированными системами безопасности поможет организациям упорядочить процессы и закрыть пробелы в защите.

Анализ данных аудита для расследования инцидентов и криминалистики

Imperva SecureSphere предлагает унифицированное решение, позволяющее проводить независимые функциональные операции и одновременно объединять результаты, полученные при проведении расследований инцидентов для команды безопасности, группы соответствия регулирующим требованиям и юридической службы. Imperva предоставляет доступ как к историческим данным, так и данным в реальном масштабе времени, что позволяет командам реагирования на инциденты видеть действия в их контексте в момент их совершения. Возможность работы в реальном времени, сопровождение пользователей, рабочие процессы по реагированию на инциденты, корреляция с МСЭ веб-приложений SecureSphere WAF и большой объем предустановленных отчетов по соответствию регулирующим требованиям и криминалистике – все это является ключевыми отличительными чертами Imperva.

Развертывание и автоматизация конфигураций является главным фактором для достижения быстрой эффективности.

Один из заказчиков компании Imperva, используя средства автоматизации, смог развернуть систему на более чем 69 000 базах данных всего лишь за несколько месяцев.

Imperva – готовое решение класса предприятия

Предсказуемая производительность при масштабировании

Imperva достигает беспрецедентной масштабируемости путем высокоэффективной технологии аудита журналирования. В отличие от конкурирующих решений, полагающихся на SQL базы данных как хранилища информации мониторинга, Imperva использует технологии, которые применяются в наиболее совершенных решениях по анализу больших объемов данных. Способность быстрой записи и еще более быстрого чтения дает решениям Imperva возможность масштабировать свою производительность, далеко опережая своих конкурентов и предоставляя им уникальное преимущество на рынке.

Система может быть сконфигурирована для мониторинга всей активности на предмет нарушения политик безопасности и одновременного мониторинга и журналирования другого набора действий для целей аудита. Такое разделение может способствовать существенному улучшению защиты данных, производительности, размера файлов аудита и релевантности его данных по сравнению с другими подобными решениями.

SecureSphere поддерживает высокую доступность путем устранения единой точки отказа и использования встроенной в решение избыточности. SecureSphere реализует наиболее совершенные и интеллектуальные технологии обеспечения высокой доступности, включая такие, как самобалансирующиеся агенты, которые при необходимости можно перемещать, обеспечивая таким образом бесперебойную работу программы защиты данных и непрерывный журнал аудита.

Быстрое развертывание

Imperva предлагает целостный подход к предприятию, предлагая централизованную консоль менеджмента, способную предоставить управление и контроль на глобальном уровне. Консоль управления верхнего уровня позволяет производить быстрое развертывание глобальных политик и автоматизацию таких задач, как классификация данных, сокращая таким образом время внедрения решения.

Imperva также осознает значения ИТ-провижининга, предоставляя наборы интерфейсов API для бесшовного распространения ПО, обновлений конфигураций, распространения политик и обнаружения данных. Развертывание и автоматизация конфигураций является главным фактором для достижения быстрой эффективности. В качестве примера можно привести одного из заказчиков компании Imperva, который, используя средства автоматизации, смог развернуть систему на более чем 69 000 базах данных всего лишь за несколько месяцев.

Гибридный мониторинг

Imperva идет далее типового сценария развертывания, при котором агенты требуется размещать на всех серверах баз данных; SecureSphere поддерживает многочисленные способы развертывания, включая локальных агентов, режим прозрачного сетевого моста и режим сниффера, размещенного «не в линии». Используя комбинации этих способов развертывания предприятие может покрыть широкий спектр своих нужд, не будучи стесненной единой моделью «один размер подходит всем».

Решение Imperva включает в себя возможность просмотра среды и обнаружения в ней известных уязвимостей, предоставляя ясную картину того, какие данные находятся под угрозой.

Готовность для облачных сред

Решение Imperva SecureSphere for AWS распространяет возможности по обеспечению безопасности и соблюдения регулирующих требований наиболее доверенного и масштабируемого решения по безопасности данных и аудита на среду Amazon Web Services. SecureSphere является единственным решением по защите данных и соответствия регулирующим требованям класса предприятия, которое доступно для AWS. Исполняемая нативно в среде AWS, BYOL версия решения SecureSphere обладает такими же возможностями, как и версия, работающая на собственной площадке заказчика. Размещая любое из решений SecureSphere (DBF, DAM, или WAF) в среде AWS, клиенты могут по желанию активировать функционал Imperva SkyFence для защиты своих облачных приложений, таких как Office 365 и AWS Management Console.

Оценка уязвимостей баз данных и виртуальные «заплатки» для них

Внутри предприятия данные могут храниться в различных местах земного шара в различных базах данных, каждая из которых может потенциально иметь свою версию ПО и уровень обновлений. Таким образом обязательным является наличие доступного способа поиска в них известных уязвимостей. Решение Imperva включает в себя возможность просмотра среды и обнаружения в ней известных уязвимостей, предоставляя ясную картину того, какие данные находятся под угрозой. Система виртуальной постановки «заплаток» SecureSphere virtual patching блокирует попытки эксплуатации известных, но незакрытых обновлениями уязвимостей. Виртуальная постановка «заплаток» помогает минимизировать окно уязвимости и существенно снижает риск взлома данных в процессе тестирования и установки обновлений ПО баз данных.

Быстрое достижение эффективности

Гибкая архитектура SecureSphere предоставляет возможность роста без прерывания работы существующей среды и позволяет бизнесу достичь большего с меньшими затратами. Imperva предлагает эффективную, предсказуемую масштабируемость решений масштаба предприятий. Недавно одна компания из списка Fortune 500 перешла на решение Imperva из-за невозможности планировать свой будущий бюджет в рамках существующего решения. С решением Imperva компания не только смогла существенно уменьшить расходы на мониторинг и операционные издержки, но и более точно планировать бюджет на свое будущее развитие.

Киберзащита Imperva SecureSphere

Imperva SecureSphere – это целостная интегрированная платформа безопасности, включающая в себя решения SecureSphere по безопасности веб, баз данных и файлов, масштабируемая для соответствия требованиям центров обработки данных даже крупнейших организаций. Ее развитие обеспечивается исследовательской организацией по безопасности мирового класса - Центром Защиты Приложений (Imperva Application Defense Center), которая поддерживает продукт на передовом крае защиты от постоянно эволюционирующих угроз.

IMPERVA SECURESPHERE

	SECURESPHERE DATABASE FIREWALL (DBF)	SECURESPHERE DATABASE ACTIVITY MONITORING (DAM)	SECURESPHERE DATABASE ASSESSMENT (DAS)
Обнаружение и классификация	Да	Да	Да
Журнал мониторинга и аудита	Да	Да	-
Блокировка в реальном времени	Да	Нет	-
Оценка уязвимостей[1]	Да	Да	Да
Агенты для БД[1]	Да	Да	-
Кластеризация шлюза	Опционально	Опционально	-
Мониторинг Big Data	Опционально	Опционально	-
Управление правами пользователей[2]	Опционально	Опционально	Опционально[3]
Расширеный сервис для специфических приложений (Oracle, EBS, SAP, Peoplesoft)	Опционально	Опционально	-
Высокая доступность для сервера управления (MX)	Опционально	Опционально	-
Доступность для Amazon Web Services (AWS) BYOL[4]	Да	Да	-

[1] Количество, включенное в поставку, зависит от приобретаемого устройства, подробную информацию можно найти в брошюре SecureSphere Appliances data sheet

[2] Мониторинг прав пользователей не доступен для узлов Big Data

[3] Функционал, требующий детализации журнала аудита, не будет доступен при развертывании DAS в одиночном (stand-alone) режиме

[4] Для среды AWS доступны не все опции

© 2015, Imperva, Inc. All rights reserved. Imperva, the Imperva logo, SecureSphere, Incapsula and Skyfence are trademarks of Imperva, Inc. and its subsidiaries. All other brand or product names are trademarks or registered trademarks of their respective holders. DS-Company-Overview-rev#1