Обеспечение безопасности баз данных

Аудит и защита баз данных

Продукты

SecureSphere Database Activity Monitoring

SecureSphere Database Firewall

SecureSphere Discovery and Assessment Server

User Rights Management for Databases

ADC Insights

Лучшие в своем классе средства аудита и защиты баз данных

Базы данных предназначены для хранения чрезвычайно ценной и секретной информации. В соответствии с требованиями стандартов безопасности заказчики должны проводить анализ прав доступа к своим данным и принимать эффективные меры для их защиты.

Признанные продукты линейки Imperva SecureSphere Database Security позволяют выполнять аудит в автоматическом режиме, мгновенно обнаруживать атаки, вредоносные действия и попытки мошенничества. В сочетании с продуктами Web Application Security и File Security они обеспечивают надежную защиту служебных данных.

Продукты Imperva SecureSphere Database Security

- Аудит прав доступа пользователей к конфиденциальным данным.
- Оповещение об атаках на базы данных и предотвращение несанкционированных действий в реальном времени.
- Оценка уязвимостей баз данных и внесение исправлений.
- Обнаружение чрезмерных прав доступа к данным и неактивных пользователей, а также анализ полного цикла прав доступа.
- Оперативное реагирование и расследование инцидентов безопасности с помощью передовых инструментов аналитики.

Возможности Imperva по обеспечению безопасности данных

Непрерывный аудит доступа к конфиденциальным данным

Решения SecureSphere выполняют непрерывный мониторинг и аудит всех действий с базами данных в реальном времени, что позволяет с высокой точностью контролировать все аспекты операций. Они отслеживают действия пользователей, которые обращаются с запросами к базам данных с помощью различных приложений, а также действия администраторов, имеющих непосредственный доступ к этим базам данных. Система SecureSphere также выполняет мониторинг откликов баз данных, оповещая об утечках важной информации либо предотвращая их.

Аналитика аудита для расследования инцидентов безопасности

Устройства SecureSphere обеспечивают глубокий анализ данных аудита с помощью интерактивных средств аналитики. Они позволяют специалистам, ответственным за безопасность и аудит баз данных, оперативно фиксировать, изучать и обрабатывать любые действия пользователей с базами данных с помощью простого интерфейса, не задействуя скрипты SQL. Интерактивная аналитика данных аудита упрощает процесс расследования инцидентов и позволяет определить тенденции и механизмы, связанные с рисками для безопасности.

Обнаружение попыток несанкционированного доступа и мошенничества

Решения SecureSphere фиксируют поведение пользователей при работе с базами данных с помощью технологии динамического профилирования, которая скоро будет запатентована. Этот механизм позволяет создать профиль всех действий пользователей, включая запросы DML, DDL, DCL и SELECT, а также факты запуска встроенных процедур. SecureSphere обнаруживает отклонения от установленных правил, оповещает о действиях пользователей, нарушающих права доступа, или блокирует их. За выполнение несанкционированных запросов SQL пользователи могут помещаться в карантин до тех пор, пока система не проанализирует и не утвердит их права доступа.

Предотвращение атак (SQL Injection, DoS и других) в реальном времени

В процессе выборочного аудита доступа к конфиденциальным данным устройства SecureSphere отслеживают все действия с базами данных в реальном времени, предотвращая утечку информации и блокируя несанкционированные SQL-операции и атаки. Независимо от источника и места происхождения, будь то приложение или привилегированный пользователь, сеть или сервер базы данных, система SecureSphere может сообщать о вредоносных атаках и при необходимости блокировать их.

Применение политик безопасности и создание отчетов

Решения SecureSphere содержат полный набор стандартных, настраиваемых политик безопасности и аудита. Встроенная в систему база знаний бизнес-приложений, таких как SAP, Oracle EBS и PeopleSoft, а также учтенные в ней основные правила, включая SOX, PCI DSS и HIPAA, упрощают процедуру развертывания и соблюдение требований стандартов. Для оптимизации бизнес-процессов оповещения об инцидентах безопасности могут поступать в системы SIEM, системы учета заявок и другие решения сторонних поставщиков.

Классификация данных в соответствии с требованиями стандартов безопасности

Устройства SecureSphere могут автоматически обнаруживать базы данных в сети, проводить оценку их уязвимости и классифицировать сохраненную в них информацию в соответствии с требованиями стандартов безопасности. Такие функции позволяют организациям расставить приоритеты при выработке мер противодействия атакам.

Соблюдение требований стандартов безопасности

Устройства SecureSphere помогают организациям соблюдать требования регулирующих органов в части безопасности данных, включая стандарты PCI DSS, SOX и HIPAA:

- обеспечивают соблюдение 8 из 12 важнейших требований PCI, включая разделы 10, 7 и 8.5;
- соответствуют требованиям к аудиту финансовых данных в разделах SOX 302 и 404;
- реализуют принцип разделения полномочий;
- обеспечивают целостность данных аудита;
- обнаруживают несанкционированный доступ к финансовым сведениям и данным держателей карт;
- предоставляют готовые формы отчетов, обеспечивающие соблюдение требований.

Оценка уязвимостей баз данных и внесение исправлений

Решения SecureSphere позволяют обнаружить свыше 1 500 уязвимостей в конфигурациях, базах данных и платформе и своевременно принять корректирующие меры. Применение «виртуальных заплаток», или виртуальное внесение исправлений, помогает мгновенно заблокировать все попытки злоумышленников использовать уязвимости для нанесения атак. Это средство значительно снижает риск утечки данных на то время, пока на серверах баз данных не будут установлены программные обновления от производителей.

Эффективный контроль прав доступа пользователей к данным

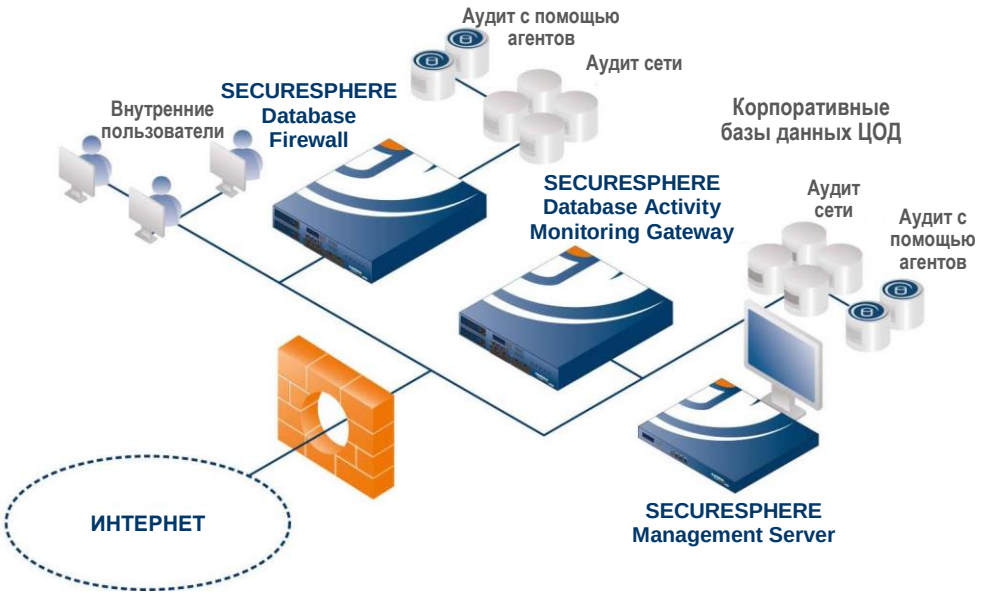
Устройства SecureSphere автоматически объединяют информацию о правах доступа пользователей к различным базам данных. С помощью модуля User Rights Management организации могут автоматизировать процесс анализа прав доступа, идентифицировать их превышение и соблюдать требования стандартов SOX, PCI 7 и PCI 8.5.

Аудит и защита локальных баз данных с помощью упрощенных агентов

В целях полноценного контроля действий пользователей устройства SecureSphere осуществляют операции аудита, мониторинга и обязательного применения правил с помощью агентов, устанавливаемых на серверах баз данных. Не требующие большого объема памяти агенты отслеживают действия пользователей и защищают конфиденциальную информацию, практически влияя на производительность сервера.

Надежная защита баз данных и соответствие стандартам безопасности

Устройства SecureSphere позволяют учесть все аспекты защиты баз данных и требования стандартов безопасности благодаря лучшим в отрасли механизмам аудита и защиты в реальном времени без снижения производительности и доступности используемых систем. Многоуровневая архитектура SecureSphere дает возможность масштабировать решение в соответствии с требованиями самых крупных баз данных. Благодаря автоматизированным механизмам защиты информации и соблюдения стандартов тысячи заказчиков доверяют свои самые ценные данные решениям Imperva SecureSphere.



Варианты развертывания

- **Non-inline Network Monitoring**. Мониторинг действий без влияния на производительность и доступность баз данных.
- **Transparent Inline Protection**. Блокирование вредоносного трафика и лучшая в отрасли производительность.
- **Agent-based Monitoring and Blocking**. Мониторинг и блокировка локальных привилегированных действий и сетевого трафика с помощью малоразмерных программных агентов.
- **Поддерживаемые платформы баз данных**. Oracle, Oracle Exadata, Microsoft SQL Server, IBM DB2 (на Linux, UNIX, Windows, z/OS и DB2/400), IBM IMS на z/OS, IBM Informix, IBM Netezza, SAP Sybase, Teradata, Oracle MySQL, PostgreSQL и Progress OpenEdge.

Пакет Imperva SecureSphere Business Security Suite

SecureSphere — передовые инструменты для обеспечения безопасности корпоративных данных. Решения SecureSphere — это комплексная, интегрированная защита приложений и данных, позволяющая предотвратить утечку и несанкционированное использование информации, выполнить требования стандартов безопасности и реализовать эффективные механизмы управления рисками.

РЕШЕНИЯ ДЛЯ ЗАЩИТЫ БАЗ ДАННЫХ

Database Activity Monitoring

Комплексный аудит и мониторинг работы пользователей с базами данных.

Database Firewall

Отслеживание действий и защита важнейших баз данных в реальном времени.

Discovery and Assessment Server

Оценка уязвимости, управление конфигурациями и классификация информации для баз данных.

User Rights Management for Databases

Анализ и контроль прав доступа пользователей к закрытым базам данных.

ADC Insights

Встроенные отчеты и правила для соблюдения требований стандартов безопасности и защиты бизнес-приложений SAP, Oracle EBS и PeopleSoft.

РЕШЕНИЯ ДЛЯ ЗАЩИТЫ ФАЙЛОВ

File Activity Monitoring

Комплексный аудит и мониторинг работы пользователей с файлами.

File Firewall

Отслеживание действий и защита важнейших файловых данных.

SecureSphere for SharePoint

Мониторинг и анализ прав доступа и использования данных в системе SharePoint, а также защита от интернет-угроз.

Directory Services Monitoring

Аудит изменений в Microsoft Active Directory, оповещение и составление отчетов по ним.

User Rights Management for Files

Анализ и контроль прав доступа пользователей к защищенным файлам.

РЕШЕНИЯ ДЛЯ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ

Web Application Firewall

Надежная автоматизированная защита от интернет-угроз.

ThreatRadar Reputation Services

Эффективный механизм репутационной защиты, обеспечивающий блокировку доступа для злоумышленников и предотвращающий автоматические атаки.

ThreatRadar Fraud Prevention

Быстрый и эффективный способ блокировки вредоносного ПО и предотвращения взломов учетных записей.

DS-DBS-0413.1