ORACLE DATA SHEET

Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall обеспечивает первый рубеж обороны для баз данных и консолидируют данные аудита баз данных, операционных систем и каталогов. Очень точный, основанный на грамматике SQL, механизм контролирует и блокирует несанкционированный трафик SQL, прежде чем он достигнет базы данных. Данные аудита сетевого трафика объединены с подробными данными аудита от других источников для подготовки отчетности о выполнении нормативных требований, формирования предупреждений при нарушениях. С использованием Oracle Audit Vault and Database Firewall задачи аудита и контроля могут быть легко адаптированы для обеспечения соответствия требованиям корпоративной безопасности.

МАСШТАБИРУЕМЫЙ КОНТРОЛЬ АКТИВНОСТИ БАЗ ДАННЫХ И АУДИТ

ГЛАВНЫЕ ОСОБЕННОСТИ

- Контроль активности и блокирование в сети объединены с консолидацией данных аудита для различных баз данных: Oracle, MySQL, Microsoft SQL Server, SAP Sybase и IBM DB2
- «Белый список», «черный список» и список исключений обеспечивают гибкость настроек политик безопасности
- Расширяемая платформа с возможностью получения данных аудита из XML файлов и из таблиц с данными аудита контролируемых приложений
- Десятки встроенных настраиваемых отчетов о выполнении политик безопасности объединены с возможностями превентивного контроля
- Интерактивные отчеты, PDF и Excel форматы
- Детальная модель авторизации доступа к данным аудита
- Хорошо масштабируемая архитектура для поддержки большого количества баз данных большого объема и интенсивным трафиком

Детективный и превентивный контроль

Брандмауэры периметра играют важную роль в защите центров обработки данных от несанкционированного внешнего доступа, но средства и способы нападения на базы данных становятся все более и более сложными. Злоумышленники обходят безопасность периметра, используют в своих интересах уязвимости серверов приложений, и даже привлекают привилегированных инсайдеров. В результате задача обеспечения эффективной защиты баз данных стала критически важной. Эффективный контроль и аудит могут предупредить и блокировать нарушения политик информационной безопасности, а также предоставить всесторонние отчеты для оценки уровня защищенности баз данных от несанкционированного доступа.

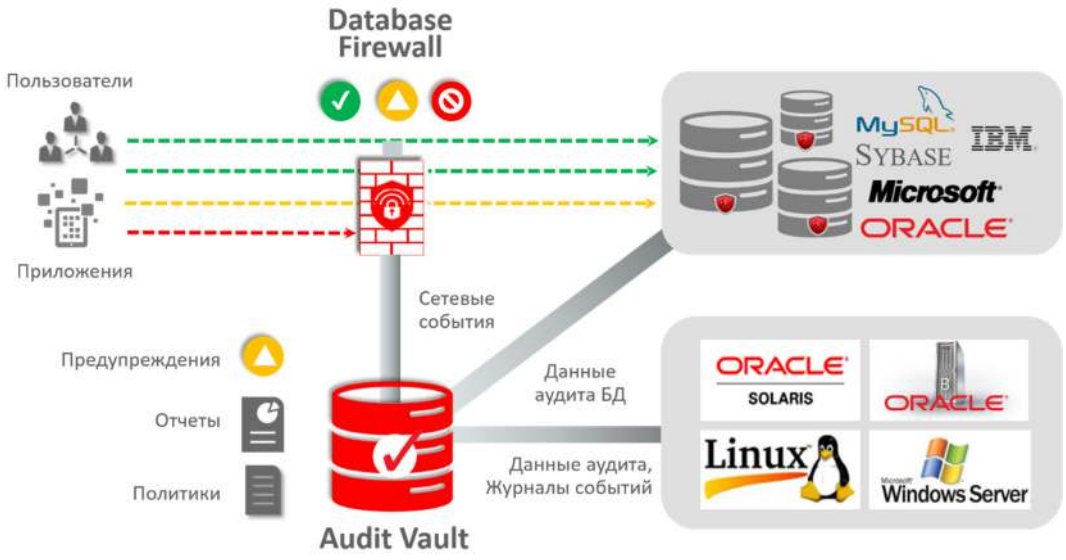

Рис. 1. Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall консолидируют события контроля сетевых запросов к базам данных и журналы аудита. Устанавливаемые политики безопасности приводят в исполнение ожидаемое поведение приложения, помогают предотвратить SQL-инъекции, обход приложения и другие злонамеренные операции. Также проводится аудит за действиями привилегированных пользователей и другими операциями в базе данных. Oracle Audit Vault and Database Firewall могут также консолидировать данные аудита от Microsoft Active Directory, Microsoft Windows, Oracle Solaris, Oracle Linux и Oracle ASM Cluster File System. Использование плугинов позволяет обеспечивать консолидацию пользовательских данных аудита из таблиц приложения и других источников.

- Предварительно сконфигурированное Soft Appliance для удобства и надежности
- Режим высокой доступности

КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

- Первый рубеж обороны, который прозрачно блокирует несанкционированный трафик, обеспечивает полное представление об текущей активности баз данных и консолидирует данные аудита из различных источников
- Контроль выполнения нормативных требований на основе использования встроенных отчетов

Брандмауэр баз данных для контроля активности и блокирования

Oracle Database Firewall обеспечивает сложный аналитический механизм грамматического анализа SQL-выражений, который проверяет SQL-операторы, поступающие в базу данных и определяет с высокой точностью какое из предписанных политикой безопасности действие нужно произвести: разрешить выполнение; разрешить, но зарегистрировать; сформировать предупреждение; заменить или блокировать SQL. Oracle Database Firewall поддерживает технологии «белый список», «черный список», и списки исключений в политиках безопасности. «Белый список» является простым набором утвержденных SQL-операторов, которые брандмауэр базы данных будет пропускать. Они могут изучаться в течение долгого времени или разрабатываться в тестовой среде. «Черный список» включает SQL-операторы от определенных пользователей, IP-адресов или определенные типы SQL-выражений, которые не разрешены для защищаемой базы данных. Списки исключений обеспечивают дополнительную гибкость развертывания для уточнения политик «белого» и «черного» списков. Политики могут быть приведены в исполнение с учетом атрибутов, включая категорию SQL, название программы, имя пользователя и IP-адрес. Эта гибкость, объединенная с очень точным анализом грамматики SQL, позволяет минимизировать уровень ложных срабатываний системы защиты, и собирать только те данные, которые действительно важны. События Oracle Database Firewall поступают в Audit Vault Server, где они обрабатываются сместно с данными аудита от других источников.

Консолидация данных аудита и управление жизненным циклом

Собственные (native) данные аудита обеспечивают полное представление о деятельности базы данных вместе с полным контекстом выполнения независимо от того, выполнялся ли отчет непосредственно через динамический SQL или через хранимые процедуры. В дополнение к консолидации данных аудита от баз данных, операционных систем и каталогов Audit Collection Plugin может использоваться, чтобы собрать данные аудита из таблиц приложения или XML-файлов, и передать их в Audit Vault Server. Данные аудита в базах данных-источниках автоматически очищаются после их перемещения в Audit Vault Server. Хранилище данных Audit Vault Server зашифровано и защищено от несанкционированных изменений с использованием опции Database Vault. Audit Vault Server поддерживает политики хранения данных, охватывающие месяцы или годы – в точном соответствии с установленной политикой безопасности или другими нормативными требованиями.

Детальная, настраиваемая отчетность и предупреждения

Десятки встроенных отчетов предоставляют простую, адаптированную отчетность о выполнении положений нормативных документов, таких как SOX, DSS PCI и HIPAA. Отчеты формируются на основе консолидированных данных аудита баз данных, сетевых событий и данные аудита от других контролируемых систем. Для подробного анализа трендов определенные системы или события могут быть объединены или отфильтрованы, представлены в интерактивном режиме или в форматах Excel и PDF. Менеджеры безопасности могут произвести настройки системы оповещения о критичных событиях безопасности. Детальный механизм настройки прав доступа позволяют Менеджеру безопасности ограничить аудиторов информацией из определенных источников, позволяя собирать данные в едином хранилище для предприятия или группы организаций.

Гибкость развертывания и масштабируемость

Средства обеспечения безопасности могут использоваться в режиме контроля и блокирования для некоторых баз данных и только в режиме контроля для остальных. Database Firewall может быть развернут различными способами (in-line, out-of-band, proxy) в зависимости от конкретной конфигурации сети. Кроме того, имеется использовать Host Monitor, который устанавливается на сервер базы данных и передает сетевой трафик к удаленному Database Firewall. Установленный как Soft Appliance (программное обеспечение устанавливается на выбранную аппаратную платформу), один Audit Vault Server может консолидировать данные аудита и события брандмауэров для тысяч баз данных. И Audit Vault Server, и Database Firewall могут быть сконфигурированы в режиме высокой доступности (High Availability, HA) для повышения отказоустойчивости.