Обеспечение безопасности файлов

Аудит и защита неструктурированных данных

Продукты

SecureSphere File Activity Monitor

SecureSphere File Firewall

SecureSphere for SharePoint

SecureSphere Directory Services Monitor

User Rights Management for Files

Передовые инструменты аудита и защиты файлов

Традиционные подходы к аудиту операций с файлами и управлению правами доступа зачастую не отвечают потребностям заказчиков. Инструменты администрирования и другие широко распространенные решения от сторонних поставщиков, такие как группы в службах каталогов и встроенные в операционную систему механизмы аудита файлов, не соответствуют высоким темпам роста информационных систем и неструктурированных данных.

Продукты линейки Imperva SecureSphere File Security обеспечивают мониторинг, аудит и защиту файлов на файловых серверах и в сетевых хранилищах (NAS), а также контроль прав доступа пользователей в реальном времени. Они дают возможность организациям наладить стандартную процедуру для анализа прав доступа, позволяя владельцам данных принимать решения на основе полученной информации. Эти решения обеспечивают безопасность конфиденциальных файловых данных путем оповещения и при необходимости блокировки попыток несанкционированного доступа. Благодаря возможности создания четких, достоверных отчетов и инструментам аналитики можно оперативно расследовать инциденты безопасности. В отличие от встроенных механизмов, решения SecureSphere выполняют аудит доступа к файлам, не влияя на производительность файловых серверов.

Продукты Imperva SecureSphere File Security

- Аудит доступа всех пользователей к файлам для обеспечения безопасности и соответствия стандартам, а также эффективности ИТ-операций.
- Сопоставление файлов с владельцами данных.
- Оптимизация анализа прав доступа за счет предоставления руководству финансовых или кадровых отделов возможности определять пользователей, которые будут иметь доступ к служебным файлам.
- Оповещение о запросах доступа к файлам, нарушающих корпоративные политики, или их блокировка.
- Соблюдение требований стандартов и реагирование на инциденты безопасности с помощью расширенных инструментов аналитики и отчетности.

Повышение эффективности ИТ-операций

Устройства SecureSphere позволяют автоматизировать выполнение наиболее сложных задач по управлению правами пользователей, аудиту доступа к данным и поиску их владельцев:

- объединение прав пользователей внутри организации;
- определение способа получения прав;
- комплексный учет операций доступа;
- определение владельцев данных и предоставление им возможности управлять правами доступа к файлам;
- отражение изменений пользователей и групп в службе Active Directory;
- поиск неиспользуемых данных;
- упрощенный перенос данных и консолидация доменов.

Возможности Imperva по обеспечению безопасности файлов

Аудит доступа к файлам и целостность данных без снижения производительности ключевых систем

Решения SecureSphere осуществляют непрерывный мониторинг и аудит всех операций с файлами в реальном времени без снижения производительности и доступности файловых серверов. Они создают подробный журнал аудита, который содержит имена пользователей, файлов, папок, время доступа, наименования операций и другие параметры. Возможность обнаружения изменений файлов и оповещения об этих изменениях помогает организациям соблюдать стандарты, а также выполнять требования модуля File Integrity Monitoring в части безопасности. Журнал аудита хранится во внешнем, защищенном хранилище, доступном только для чтения и только на основе ролей. Это позволяет реализовать принцип разделения обязанностей.

Контроль прав доступа пользователей к файлам

Устройства SecureSphere определяют текущие права доступа пользователей к файлам и с помощью комплексного цикла анализа реализуют принцип доступа к важной информации только при наличии служебной необходимости. Этот механизм позволяет оптимизировать аудит и контроль разрешений путем консолидации прав доступа к файлам на файловых серверах и в сетевых хранилищах NAS, а также создания соответствующих отчетов. Циклическая перепроверка прав пользователей подразумевает:

- определение пользователей, имеющих доступ к файлам с конфиденциальными данными;
- оповещение о пользователях с чрезмерными правами доступа;
- выявление неактивных пользователей и неиспользуемых прав доступа;
- обеспечение последовательных операций анализа прав доступа;
- отслеживание изменений в службе Active Directory и оповещения о них в реальном времени.

Контроль доступа к файлам, осуществляемый владельцами данных

Устройства SecureSphere определяют владельца данных путем анализа его работы с данными. Организации могут снижать риск и обеспечивать защиту файлов, непосредственно вовлекая владельцев данных в анализ прав доступа.

Система SecureSphere обеспечивает доступ к удобному порталу для владельцев данных, на котором руководители предприятия могут регистрироваться, принимать решения о доступе к файлам и отправлять результаты напрямую в ИТ-отдел для принятия мер. Предоставляя возможность принятия решений о контроле прав доступа к файлам именно тем лицам, которые располагают самой полной информацией (т. е. руководителям финансовых или кадровых отделов), решения SecureSphere позволяют выполнять анализ прав доступа регулярнее и точнее. Благодаря прозрачной процедуре операцию анализа можно проводить достаточно часто, обеспечивая защиту важных данных и соответствие стандартам.

Оповещение о несанкционированных действиях и их блокировка в реальном времени

Устройства SecureSphere расширяют стандартные полномочия, блокируя доступ к файлам или оповещая о нарушении корпоративной политики. Блокировка доступа на основе политики позволяет организациям обеспечить защиту от ошибок, связанных с правами доступа и возникающих на уровне каталогов и файлов. Гибкая система дает возможность учитывать при создании политик самые разные критерии, например метаданные файлов, контекст организации, операции доступа и классификацию данных, а затем принимать необходимые меры при обнаружении нежелательных действий.

Расследование инцидентов безопасности и принятие мер

Решения SecureSphere предоставляют интерактивные средства аналитики аудита, позволяющие выводить на экран сведения о доступе к данным, изменениях в Active Directory и правах пользователей с помощью нескольких щелчков мыши. Используя эти данные, специалисты служб безопасности, нормативного соответствия и аудита могут определять тенденции, механизмы и риски, связанные с операциями с файлами и правами пользователей. Возможность оперативно просматривать данные аудита в многомерном режиме, а также интерактивные инструменты аналитики упрощают выявление инцидентов безопасности и их расследование.

Быстрая и эффективная регистрация соблюдения стандартов с помощью графических отчетов

Устройства SecureSphere предлагают широкие возможности для создания графических отчетов, позволяющие предприятиям оценивать риски и регистрировать соблюдение требований стандартов безопасности, таких как SOX, PCI, HIPAA, и других законов о конфиденциальности данных. Можно просматривать отчеты в любой момент, а также настроить для них график создания и рассылки. Панель мониторинга в реальном времени дает общую картину о событиях в системе безопасности и состоянии системы. Система отчетности SecureSphere мгновенно выводит на экран сведения о текущих проблемах, связанных с безопасностью, соблюдением стандартов и правами пользователей.

Мониторинг и защита Microsoft SharePoint

Решение SecureSphere for SharePoint гарантирует защиту конфиденциальных файлов организаций в системе SharePoint. Оно учитывает уникальные требования к безопасности файлов, веб-приложений и баз данных SharePoint, предоставляя пользователям доступ только при наличии обоснованной служебной необходимости. Решение обеспечивает мониторинг и анализ прав доступа и использования данных, а также защиту от интернет-угроз.

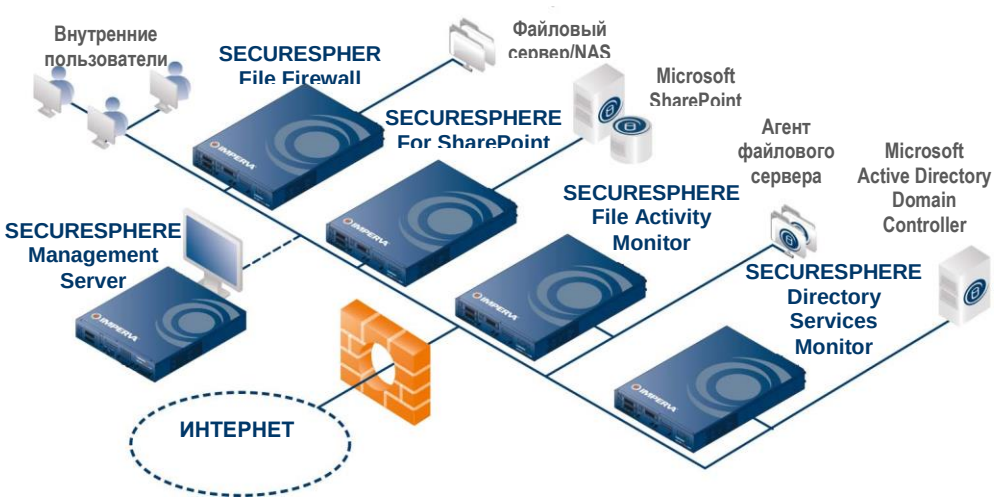
- Применение бизнес-правил за счет оповещения или блокировки доступа к файлам в системе SharePoint. Предоставление прав доступа с возможностью просмотра актуальных и точных сведений о владельцах данных и полномочиях.
- Выявление файлов, запросы доступа к которым давно не подавались.
- Ускорение переноса данных и консолидация доменов в службах каталогов на основе информации о владельцах данных, неактивных учетных записей и неиспользуемых данных.
- Оптимизация анализа прав пользователей в процессе переноса и консолидации данных.

Мониторинг изменений в Active Directory

Служба Active Directory играет ключевую роль при определении прав доступа к SharePoint, файловым серверам и устройствам NAS. По этой причине любые изменения в Active Directory могут значительно повлиять на конфиденциальные бизнес-данные. Решение SecureSphere Directory Services Monitor (DSM) помогает организациям обеспечить безопасность и соблюдение стандартов при работе со службой Microsoft Active Directory. Оно позволяет эффективно контролировать выполнение важнейших задач, таких как разделение обязанностей, отслеживание действий привилегированных пользователей, повышение привилегий и внесение существенных изменений. SecureSphere Directory Services Monitor дает возможность непрерывно отслеживать действия в службах каталогов, гарантируя безопасность и соответствие требованиям стандартов, а также предоставляет ИТ-специалистам функции аудита, оповещения, анализа изменений, составления отчетов и реагирования в реальном времени.

Лидер в области безопасности данных

Устройства SecureSphere обладают лучшими среди аналогов возможностями для аудита доступа к файлам и управления правами доступа пользователей, помогают соблюдать требования стандартов безопасности, обеспечивая высокий уровень защиты и оптимизируя ИТ-операции. Эффективно используя функции централизованного управления и отчетности, решения SecureSphere отвечают требованиям заказчиков любого масштаба — от небольших организаций с одним файловым сервером или системой SharePoint до крупных предприятий с распределенной сетью ЦОД. Эти решения обеспечивают непревзойденную безопасность данных за счет эффективных механизмов защиты веб-приложений, баз данных и файлов.



Варианты развертывания

Гибкие механизмы развертывания — как в качестве встроенного, так и в качестве внешнего компонента — обеспечивают удобство установки без необходимости изменения параметров файловых серверов, устройств NAS, приложений, клиентов и пр.

- **Non-inline Network Monitoring.** Мониторинг действий без влияния на производительность и доступность.
- **Transparent Inline Protection.** Блокировка вредоносного трафика и лучшая в отрасли производительность для принятия превентивных мер защиты.

Решения Imperva SecureSphere для защиты центров обработки данных

Imperva SecureSphere — это комплексная, интегрированная платформа безопасности, в состав которой входят решения SecureSphere для защиты веб-приложений, баз данных и файлов. Благодаря возможности масштабирования в соответствии с требованиями безопасности центров обработки данных она подходит для использования в самых крупных средах, а резервирование, осуществляемое специалистами международного исследовательского центра Imperva Application Defense Center, обеспечивает защиту решений от угроз с помощью самых передовых средств.

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 Community Defense

Ценная информация для защиты от угроз, полученная от пользователей, работающих с продуктами SecureSphere по всему миру.

ThreatRadar Fraud Prevention

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

Incapsula SaaS WAF и DDoS Protection

Передовые средства защиты веб-приложений и доставки контента-услуги.

РЕШЕНИЯ ДЛЯ ЗАЩИТЫ БАЗ ДАННЫХ

Database Activity Monitor

Комплексный аудит и мониторинг работы пользователей с базами данных.

Database Firewall

Отслеживание действий и защита важнейших баз данных в реальном времени.

Database Assessment

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 Monitor

Комплексный аудит и мониторинг работы пользователей с файлами.

File Firewall

Отслеживание действий и защита важнейших файловых данных.

User Rights Management for Files

Анализ и контроль прав доступа пользователей к защищенным файлам.

Directory Services Monitor

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

РЕШЕНИЯ ДЛЯ ЗАЩИТЫ ИНФРАСТРУКТУРЫ SHAREPOINT

SecureSphere for SharePoint

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

IMPERVA

www.imperva.com