File

Protecting the Data That Drives Business®

File Security

Audit and Protect Critical Files

Cutting edge Imperva SecureSphere File Security products:

- Audit all access to files for security, compliance, and IT operations efficiency
- Identify excessive user rights and enable a complete file rights audit and review cycle
- Alert on or block file access requests that violate corporate policies
- Map files to data owners
- Demonstrate compliance and respond to security incidents with advanced analytics and reporting

Products

SecureSphere File Activity Monitoring

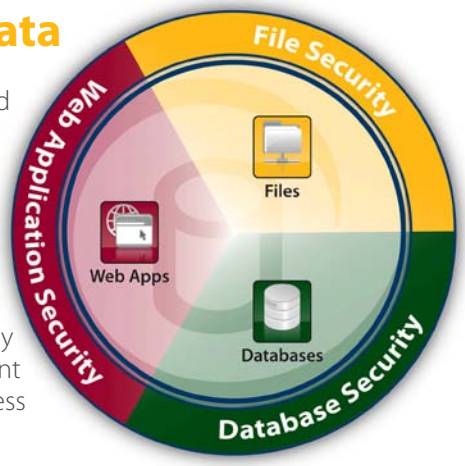
SecureSphere File Firewall

User Rights Management for Files

Unmatched Auditing and Protection for File Data

Conventional approaches for auditing file activity and managing permissions simply don't work for most organizations. Third-party administrative tools and other widely used solutions, such as directory services groups and the file auditing built into operating systems, do not keep pace with organizational changes or the volume and growth of unstructured data.

Imperva SecureSphere File Security products deliver real-time file monitoring, auditing, security, and user rights management for files stored on file servers and network attached storage (NAS) devices. SecureSphere audits all file access to ascertain who owns and who is using file data. It secures sensitive file data by alerting on and optionally blocking unauthorized access. It accelerates forensic investigations through clear, relevant reports and analytics. And, unlike native auditing solutions, SecureSphere audits file access without degrading file server performance.



Audit All File Data Access without Impacting Critical Systems

SecureSphere continuously monitors and audits all file operations in real time without impacting file server performance or availability. SecureSphere creates a detailed audit trail that includes the name of the user, file accessed, parent folder, the access time, the access operation, and more. To enforce separation of duties, the audit trail is maintained in an external, secured, and hardened repository which can be accessed exclusively through read-only views via a role based access mechanism.

Control User Access Rights to Sensitive File Data

SecureSphere identifies existing user access rights and facilitates a complete rights review cycle to ensure sensitive file data is accessible only by those with a business need-to-know. It streamlines audits by consolidating and reporting on user access rights across all file servers and NAS devices. SecureSphere accelerates review cycles by:

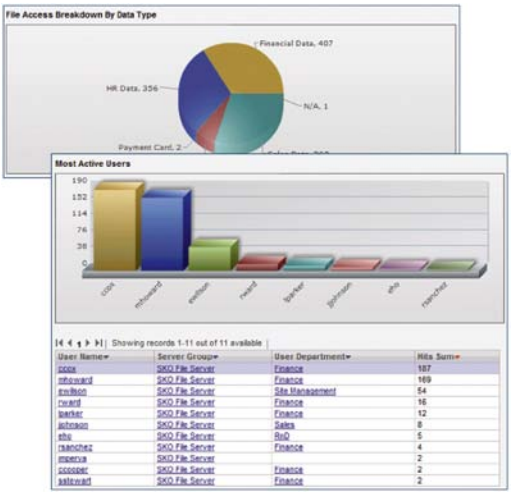
- Identifying users with access to sensitive, high-risk file data
- Highlighting users with excessive access rights
- Discovering dormant users and un-used access rights
- Providing rights review workflow capabilities

Alert on or Block Abnormal Activity in Real Time

SecureSphere File Firewall provides file protection by blocking or alerting on access activity that deviates from corporate policy. Policy-based blocking enables administrators to guard against mistakes introduced at the ACL level. A flexible policy framework enables the creation of policies that consider a variety of criteria, such as file meta-data, organizational context, access activity, and data classification, and then take action when undesirable behaviors are observed.

Identify Data Owners for Policy Management

SecureSphere identifies data owners by analyzing file and folder usage. Owner identification is critical for compliance, security and IT operations because owners understand the business relevance of their data and provide critical input on how data should be managed and protected.



PCI, SOX, and HIPAA Compliance

SecureSphere helps organizations address multiple compliance regulations including PCI, SOX, and HIPAA.

- Addresses 8 of 12 high-level PCI requirements, including sections 10, 7, and 8.5
- Meets auditing requirements for financial data in SOX sections 302 and 404
- Satisfies HIPAA sections 160.103 and164.312(b)
- Enforces separation of duties
- Ensures audit data integrity
- Detects unauthorized access to sensitive data
- Offers graphical reports that streamline compliance

Investigate and Respond to Security Incidents

SecureSphere provides interactive, on-screen audit analytics for visualizing file data activity and user rights with just a few clicks. Security, compliance, and audit staff can leverage these analytics to identify trends, patterns, and risks associated with file activity and user rights. With near real-time, multidimensional views of audit data, interactive audit analytics streamline forensics investigations and pinpoint security incidents.

Quickly and Efficiently Document Compliance with Graphical Reports

SecureSphere offers rich graphical reporting capabilities, enabling businesses to measure risk and document compliance with regulations such as SOX, PCI, HIPAA, and other data privacy laws. Reports can be viewed on demand or scheduled and distributed on a regular basis. A real-time dashboard provides a high-level view of security events and system status. The SecureSphere reporting platform instantly visualizes security, compliance, and user rights management concerns.

Increase IT Operations Efficiency

SecureSphere helps IT operations staff, such as Windows, storage, help desk, and directory services administrators, work more efficiently. File activity monitoring enables IT operations to:

- Grant access rights with a current and accurate view of data owners and permissions
- Identify files that have not been accessed recently
- Expedite data migrations and directory services domain consolidations based on information about data owners, dormant accounts, and unused data
- Simplify user rights reviews during migration and consolidation projects

Zero Impact Deployment and Ultra High Performance

- **Hardware Appliances:** Offer multi-Gigabit throughput and support for thousands of users
- **Virtual Appliances:** Provide adaptable, reliable, and manageable security that grows with your business

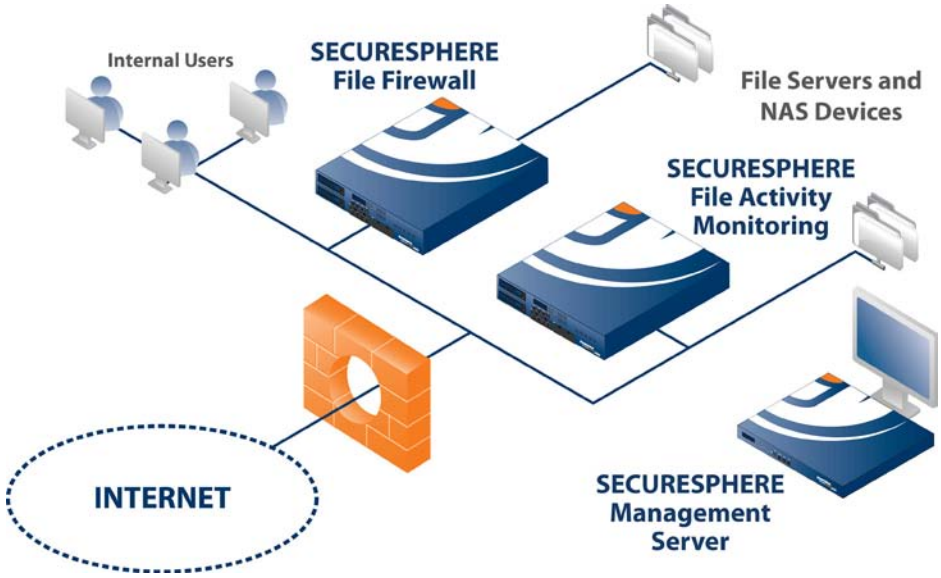
Rely on the Leader in Data Security

SecureSphere offers best-of-breed file auditing and user rights management that accelerate compliance, bolster security, and streamline IT operations processes. Leveraging a powerful centralized management and reporting platform, SecureSphere meets the needs of any environment – from small organizations with a single file server to large enterprises with geographically distributed data centers. SecureSphere provides unparalleled data security with protection for Web applications, databases, and files.

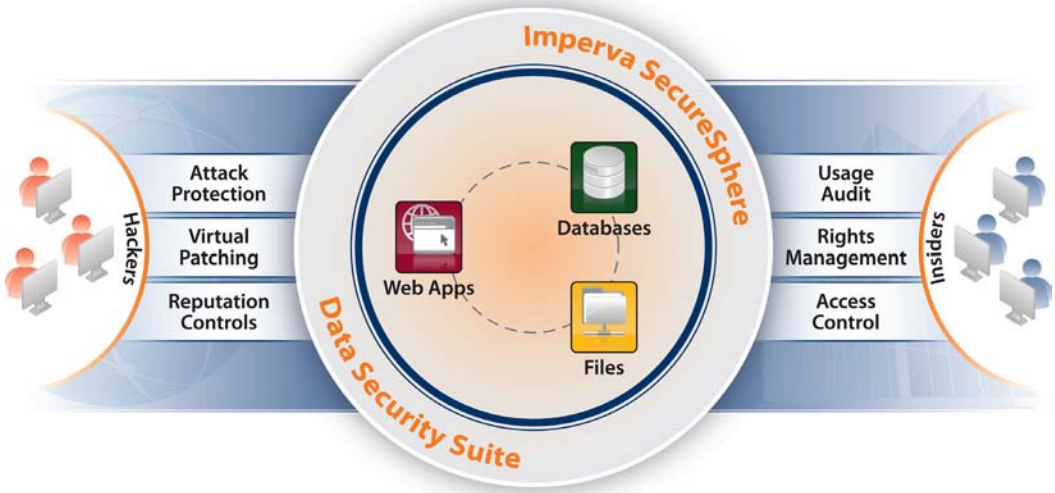
Flexible inline and non-inline deployment modes offer easy installation with no changes to file servers, NAS devices, applications, clients, or network

Deployment

- **Non-inline Network Monitoring**: Activity monitoring with zero impact on performance or availability
- **Transparent Inline Protection**: Drop-in deployment and industry-leading performance for proactive security



Imperva SecureSphere Data Security Suite



SecureSphere Data Security Suite is the market-leading data security and compliance solution. SecureSphere protects web applications and sensitive file and database data from hackers and malicious insiders, provides a fast and cost-effective route to regulatory compliance, and establishes a repeatable process for data risk management.

Family	SecureSphere Product
Database	**Database Activity Monitoring** Full auditing and visibility into database data usage **Database Firewall** Activity monitoring and real-time protection for critical databases **Discovery and Assessment Server** Vulnerability assessment, configuration management, and data classification for databases **User Rights Management for Databases** Review and manage user access rights to sensitive databases **ADC Insights** Pre-packaged reports and rules for SAP, Oracle EBS, and PeopleSoft compliance and security
File	**File Activity Monitoring** Full auditing and visibility into file data usage **File Firewall** Activity monitoring and protection for critical file data **User Rights Management for Files** Review and manage user access rights to sensitive files
Web	**Web Application Firewall** Accurate, automated protection against online threats **ThreatRadar** Industry-first reputation-based Web application security

Imperva is the global leader in data security

Thousands of the world's leading businesses, government organizations, and service providers rely on Imperva solutions to prevent data breaches, meet compliance mandates, and manage data risk.

Imperva
Headquarters
3400 Bridge Parkway, Suite 200
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

Toll Free (U.S. only): +1-866-926-4678
www.imperva.com