IMPERVA®

File Security

DATASHEET

Audit and Protect Unstructured Data

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 allows organizations to put a repeatable workflow in place for performing access rights reviews, and enables data owners to make access control decisions. 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.

Products

- SecureSphere File Activity Monitor
- SecureSphere File Firewall
- SecureSphere for SharePoint
- SecureSphere Directory Services Monitor
- User Rights Management for Files

Imperva SecureSphere File Security Products

- Audit all access to files for security, compliance, and IT operations efficiency
- Map files to data owners
- Streamline access rights reviews by allowing business owners, such as the VP of Finance or HR, to decide who should have access to corporate files
- Alert on or block file access requests that violate corporate policies
- Demonstrate compliance and respond to security incidents with advanced analytics and reporting

Increase IT Operations Efficiency

SecureSphere automates the most challenging aspects of managing user rights, auditing data access, and finding data owners.

- Aggregates user rights across the organization
- Illustrates how rights were derived
- Provides a comprehensive record of access activity
- Identifies data owners and allows them to manage file access rights
- Shows user and group changes in Active Directory
- Finds unused data
- Helps with data migration and domain consolidation

Imperva File Security Capabilities

Audit File Access and Integrity 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 directory, the access time, the access operation, and more. SecureSphere's ability to detect and alert on file changes helps organizations address compliance- and security-related File Integrity Monitoring requirements. 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.

Manage 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 and permissions management 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
- Tracking and alerting on Active Directory changes in real-time

Allow Data Owners to Control File Access

SecureSphere identifies data owners by analyzing data usage. Once the data owner is determined, organizations can reduce risk and keep files secure by directly involving data owners in access rights reviews.

SecureSphere features an intuitive Data Owner Portal that allows business owners to log in, make file access decisions, and submit the results directly to IT to take action. By putting file access control decisions in the hands of those who know corporate data the best, such as the VP of Finance or HR, access rights reviews are more accurate and can be performed more quickly. With an end-to-end workflow in place, rights reviews can be repeated on an ongoing basis to ensure your critical data is secure and compliance requirements are met.

Alert on or Block Abnormal Activity in Real Time

SecureSphere augments native permissions by blocking or alerting on access activity that deviates from corporate policy. Policy-based blocking enables organizations to guard against mistakes introduced in directory and file level permissions. 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.

Investigate and Respond to Security Incidents

SecureSphere provides interactive, on-screen audit analytics for visualizing data access activity, Active Directory changes, 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.

Monitor and Protect Microsoft SharePoint

SecureSphere for SharePoint helps organizations protect sensitive files in SharePoint. SecureSphere addresses the unique security requirements of SharePoint's file, web, and database elements ensuring that users with legitimate business needs can access data and others cannot. It provides visibility and analysis of access rights and data usage, and delivers protection against web-based threats.

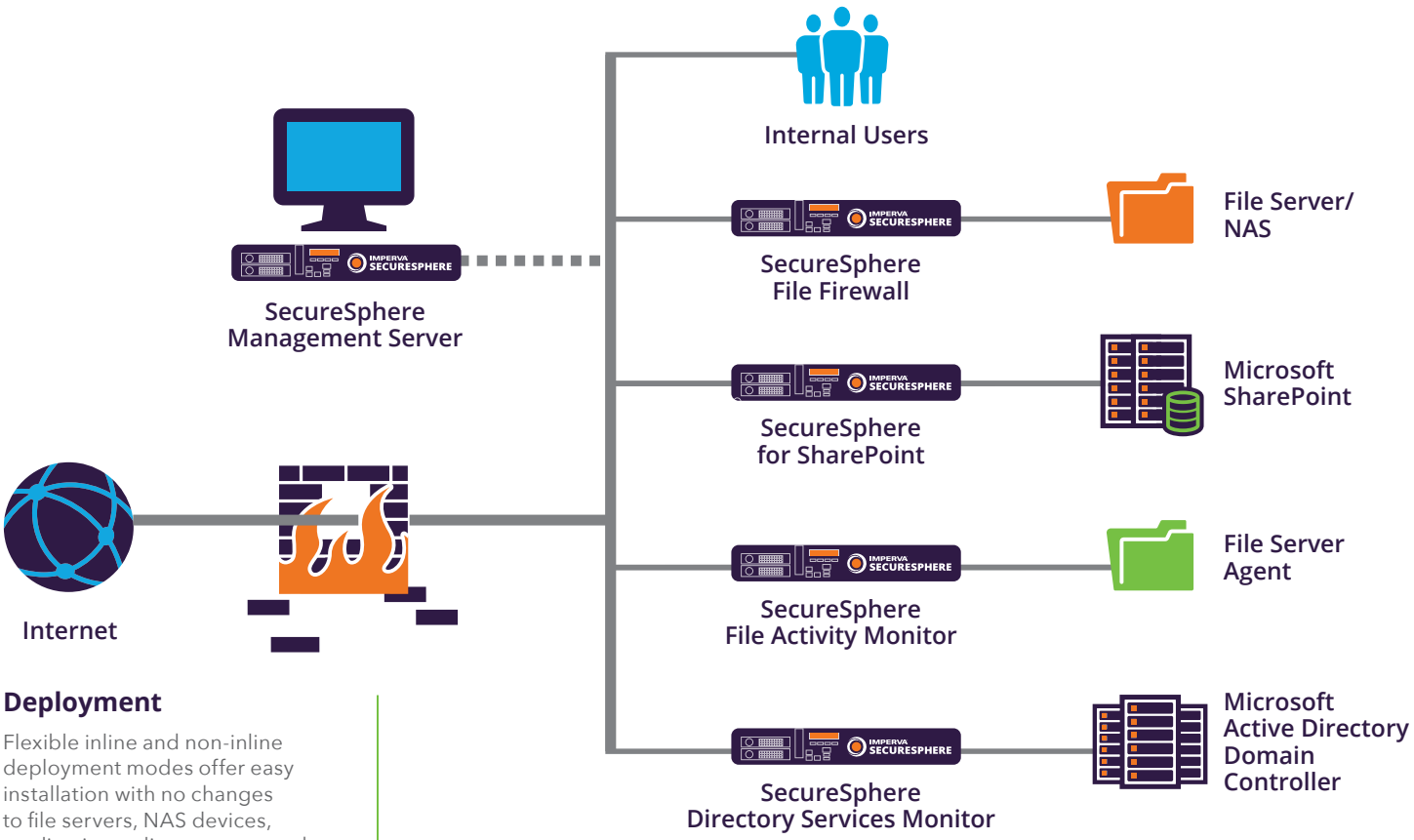
- Enforce business rules by generating alerts or blocking access to files in SharePoint Grant access rights with a current and accurate view of data owners and permissions
- Identify files that have not been accessed recently
- Expedite data migrations and directory services domain consolidations based on information about data owners, dormant accounts, and unused data
- Simplify user rights reviews during migration and consolidation projects

Monitor Changes in Active Directory

Active Directory plays a central role in defining data access rights for SharePoint, file servers, and NAS devices. Therefore, changes within Active Directory can have broad implications for sensitive business data. SecureSphere Directory Services Monitor (DSM) helps organizations achieve security and compliance goals for Microsoft Active Directory. It ensures that critical concerns such as separation of duty, privileged user monitoring, escalation of privileges, and high impact changes are addressed and controlled. SecureSphere Directory Services Monitor provides continuous visibility into directory services activity that enables security, compliance, and IT professionals to audit, alert, analyze, report, and respond to changes in real time.

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 or SharePoint site to large enterprises with geographically distributed data centers. SecureSphere provides unparalleled data security with protection for web applications, databases, and files.



Deployment

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

- **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 Center Security

Imperva SecureSphere is a comprehensive, integrated security platform that includes SecureSphere Web, Database and File Security. It scales to meet the data center security demands of even the largest organizations and is backed by the Imperva Application Defense Center, a world-class security research organization that maintains the product's cutting-edge protection against evolving threats.

Imperva SecureSphere Cyber Security

Imperva SecureSphere is a comprehensive, integrated security platform that includes SecureSphere Web, Database and File Security. It scales to meet the data center security demands of even the largest organizations, and is backed by Imperva Application Defense Center, a world-class security research organization that maintains the product's cutting-edge protection against evolving threats.

IMPERVA SECURESPHERE

WEB APPLICATION SECURITY PRODUCTS	
Web Application Firewall	Accurate, automated protection against online threats
ThreatRadar Reputation Services	Leverage reputation data to stop malicious users and automated attacks
ThreatRadar Community Defense	SecureSphere deployments around the world provide crowd-sourced threat intelligence to subscribers
ThreatRadar Fraud Prevention	Stop fraud malware and account takeover quickly and easily
Incapsula SaaS WAF and DDoS Protection	Best-of-breed web application security and content delivery as a service
DATABASE SECURITY PRODUCTS	
Database Activity Monitor	Full auditing and visibility into database data usage
Database Firewall	Activity monitoring and real-time protection for critical databases
Database Assessment	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 SECURITY PRODUCTS	
File Activity Monitor	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
Directory Services Monitor	Audit, alert, and report on changes made in Microsoft Active Directory
SHAREPOINT SECURITY PRODUCTS	
SecureSphere for SharePoint	Visibility and analysis of SharePoint access rights and data usage, and protection against Web based threats