IMPERVA®

Imperva SecureSphere File Security

DATASHEET

Protect Unstructured Data from Ransomware and Insider Threats

Unmatched Protection for File Data

Imperva SecureSphere File Firewall monitors access to your critical files in real-time and stops unwanted access, providing the highest level of security for your unstructured data. With an audit trail of all file access activity, security teams can quickly perform forensic investigations and generate reports. In addition, interactive audit analytics allow administrators to drill down into the details to identify suspicious behavior and document problems. With SecureSphere File Firewall, you can take security to the next level by generating alerts or blocking unauthorized file access based on the industry's leading security policy framework.

Nearly 40 percent of businesses got hit by ransomware in 2015

SOURCE: OSTERMAN RESEARCH

Imperva SecureSphere File Security Products

- Secure critical files to prevent costly data breaches
- Immediately detect and block ransomware attacks
- Allow IT organizations to quickly respond to security incidents
- Restrict access to sensitive files based on flexible, granular security policies

Stop Ransomware in its Tracks

Essential capabilities for a real-time file access monitoring solution:

- Real-time monitoring and analysis of user file access behavior
- Granular visibility into who, what, when, where, and how files were accessed
- Alerting when suspicious behavior is detected
- Detection and blocking of unauthorized/ransomware access
- Analytics to accelerate investigation of security incidents
- Backed by ongoing research dedicated to understanding how ransomware behaves

Imperva File Security Capabilities

Real-time Monitoring and Auditing

Imperva SecureSphere File Firewall 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. By keeping a complete record of every file access across the company, including the actions of privileged users, organizations accelerate security incident response and simplify the compliance process. To enforce separation of duties, the audit trail is maintained in a secured and hardened repository which can be accessed exclusively through read-only views via a role-based access mechanism.

Real-time Ransomware Detection and Mitigation

When it comes to ransomware, time is of the essence. The good news is that there is a more effective way to defend your organization. Real-time file access monitoring detects and blocks ransomware before it does widespread damage. It automates identification of ransomware based on file-access activity patterns and applies policies to block that behavior and protect your files.

SecureSphere File Firewall identifies distinctive behavior patterns associated with ransomware, such as rapid file overwriting and repeated use of the rename operation. The solution features deception-based detection capabilities, which leverage strategically planted, hidden files on file storage systems to detect ransomware at the earliest stage of the attack. Any write or rename actions on these hidden files trigger automatic blocking of the infected user or endpoint.

Alert on or Block Abnormal Activity in Real Time

Imperva SecureSphere File Security solutions notify you immediately when unusual file access behavior occurs. SecureSphere File Firewall augments native file permissions by alerting on access activity that deviates from corporate policy. Additionally, organizations can leverage policy-based blocking which allows organizations to guard against mistakes introduced in directory and file level permissions.

These flexible responses are based on the industry leading Imperva security policy framework that allows companies to create policies that consider a variety of criteria, such as file metadata, organizational context, and access activity. Then, administrators can take action right away when undesirable behaviors are observed.

Investigate and Respond to Security Incidents

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

Quickly & Efficiently Document Secuity Events with Graphical Reports

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

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.

Protect Files from Insider Threats

Enterprises are constantly exposed to data theft caused by compromised, careless or malicious insiders. It only takes one curious insider to jeopardize your intellectual property, financial data, business plans, and other business-critical data.

To safeguard organizations from the theft and loss caused by insider threats, the Imperva CounterBreach solution leverages advanced, machine learning technology to protect enterprise data stored in enterprise file shares, SaaS applications, and databases.

By dynamically learning users' normal file access patterns and then identifying inappropriate or abusive access activity, CounterBreach proactively alerts IT teams to dangerous behavior.

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 cyber security demands of even the largest organizations and is backed by the Imperva Defense Center, a world-class security research organization that maintains the product's cutting-edge protection against evolving threats.