



PARTNERSPHERE McAfee and Imperva

Imperva SecureSphere and McAfee® Data Loss Prevention Deliver Enhanced Control and Streamlined Security for File Data

Imperva SecureSphere File Security complements McAfee Data Loss Prevention to help protect sensitive file data stored on file servers and network attached storage devices. SecureSphere adds full visibility into data ownership, user access rights, and file usage to McAfee Data Loss Prevention enabling auditors, security managers, and IT administrators to improve data security and meet compliance mandates.

Using SecureSphere, organizations can ensure that file access rights are based on a need-to-know basis for business use. The integration between McAfee Network Data Loss Prevention Discover (“Which files are sensitive?”) and SecureSphere File Security (“Who is accessing the files?”) enables data classification to drive SecureSphere’s real-time security policies and to guide analysis of the data ownership, access rights, and usage of sensitive data.

The Challenge of Securing File Data

Persistent insider threats and regulatory compliance mandates make protecting sensitive file data a business requirement for virtually every organization. One of the biggest challenges in managing sensitive files stems from the lack of basic file security visibility and control that exists in organizations today. This is compounded by the volume and growth of file data.

According to analyst firm IDC, unstructured data accounts for approximately 80 percent of all enterprise data, and is growing at a rate of 60 percent per year. To keep pace, organizations need solutions that can efficiently monitor, analyze, and protect their file data.

Ensuring Need-To-Know Access for Business Use

Need-to-know access for business use is a security best practice as well as a requirement for regulations such as Sarbanes Oxley (SOX), the Payment Card Industry Data Security Standard (PCI DSS), and a number of data privacy laws. Using SecureSphere with McAfee Data Loss Prevention data discovery and classification helps achieve need-to-know access for business use for sensitive file data in two critical ways. First, once sensitive data is located, SecureSphere will identify existing user access rights to this data and facilitate a complete rights review cycle to ensure that files are accessible only by those with a business need. SecureSphere streamlines rights audits by:

- » Identifying which users have access to sensitive, high-risk file data
- » Highlighting data with excessive access rights
- » Discovering dormant users and unused access rights
- » Providing rights review tracking capabilities

Once rights are aligned with business requirements, the second benefit of the joint solution comes into play: McAfee Data Loss Prevention file classification information can be used in SecureSphere policies to alert on, and even block, file access that deviates from corporate policy. SecureSphere’s flexible policy framework uses a number of criteria, such as file

Integration Benefits

Imperva SecureSphere File Security v8.5 and higher and McAfee Network Data Loss Prevention v9 and higher

- » Identify data owners
- » Identify excessive user access rights
- » Perform file rights audits and reviews
- » Audit all access to files
- » Alert on, or block, file access
- » Accelerate incident response and forensic investigations

classification, metadata (for example, file name, location, type, and more), permissions, and user access activity to take action when undesirable behaviors are observed. For example, a policy can be configured to alert when users outside the finance department access files containing PCI data. This enables security, compliance, and business stakeholders to retain visibility and control over sensitive data.

Identify Owners of Files and Folders

The significant volume and growth of data means that IT staff simply cannot keep track of who owns the majority of the data on shared file systems. However, owner identification is critical for compliance, security, and IT operations because only the owners understand the business relevance of their data and can provide the critical input on how that data should be managed and protected. For example, working with data owners provides the information necessary to craft intelligent data loss prevention policies that protect data without disrupting business. SecureSphere helps in the identification of data owners by providing visibility into the users of files and folders. The primary file and folder users either own the data themselves or can help identify the owner of the data they routinely use.

Audit File Data Access

SecureSphere performs continuous monitoring and detailed auditing of all file operations in real time to provide organizations with a complete audit trail that shows the “who, what, when, where, and how” of each file data access. It monitors file access activity and transparently records every user access of file data without impacting applications, users, or file servers. File access activity is also correlated with user rights information to identify overly accessible data and help reduce access to a business need-to-know level. This also complements McAfee® Integrity Monitor, which offers file integrity monitoring (FIM) of files and directories on a server for changes to content, permissions, or both. It tests and verifies file changes in the environment to ensure security and help achieve compliance with regulations such as those outlined in PCI DSS 10.5.5 and 11.5.

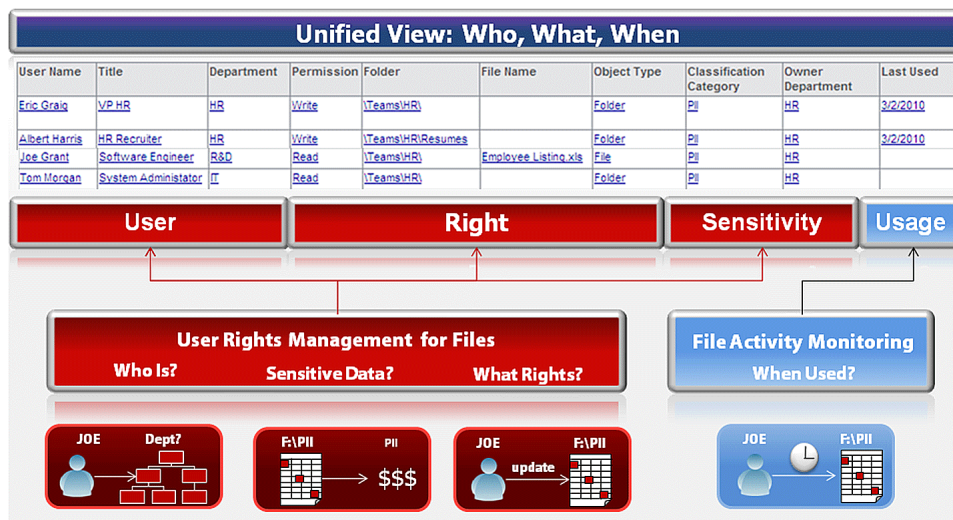


Figure 1. Imperva SecureSphere provides unified views of file activity access for files classified as sensitive by McAfee Network DLP Discover.

About McAfee Data Loss Prevention

McAfee Data Loss Prevention delivers the highest levels of protection for sensitive data, while greatly reducing the cost and complexity of safeguarding business-critical information. McAfee data protection is delivered through our low-maintenance appliance and the McAfee® ePolicy Orchestrator® platform for streamlined deployment, management, updates, and reports.

About Imperva and SecureSphere

Imperva is the global leader in data security. With more than 1,300 direct customers and 25,000 cloud customers, Imperva's customers include leading enterprises, government organizations, and managed service providers who rely on Imperva to prevent sensitive data theft from hackers and insiders. The award-winning Imperva SecureSphere is the only solution that delivers full activity monitoring and protection for databases, Web applications, and file systems. Only Imperva delivers innovative technology to give full audit accountability and separation of duties to meet regulatory compliance.

Visit us at www.imperva.com