SecureSphere for SharePoint

Data Security for SharePoint's File, Web and Database Resources

SecureSphere for SharePoint Benefits
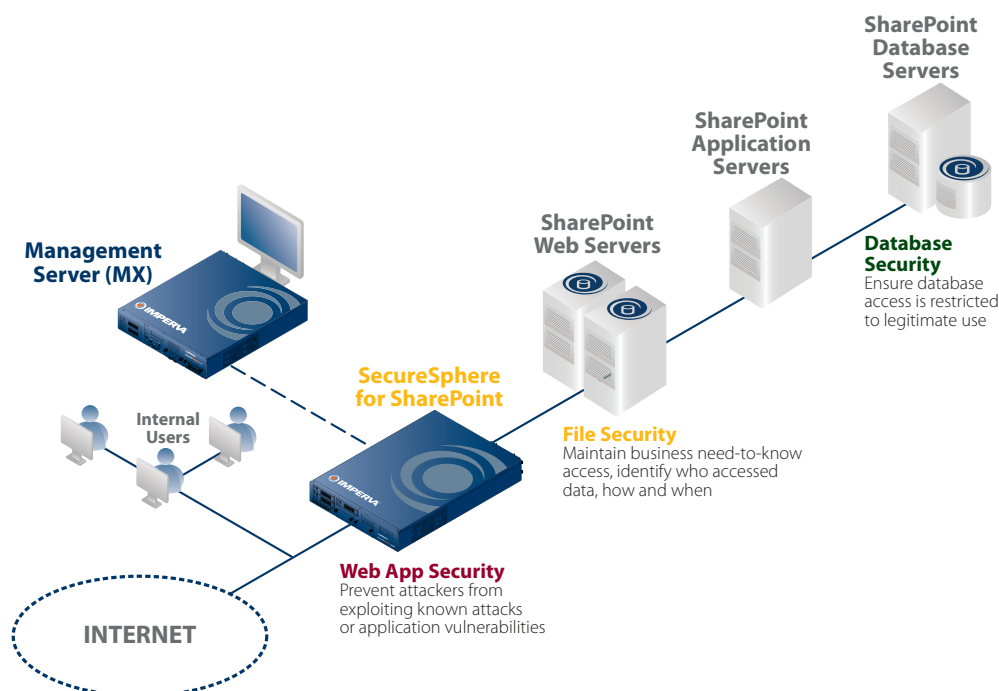
IT Operations

- Save time managing permissions and performing user rights reviews
- Decide how best to manage data
- Find lost, missing or deleted data
- Free valuable storage space

Security

- Enforce business rules by generating alerts or blocking access to files in SharePoint
- Ensure access is based on need-to-know
- Document compliance, conduct forensic investigations and isolate changes
- Determine how best to protect and manage data
- Protect against web-based attacks
- Prevent tampering with SharePoint's Microsoft SQL database
- Rapid time-to-security

SecureSphere for SharePoint helps organizations protect sensitive data stored within Microsoft SharePoint. It 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. SecureSphere for SharePoint provides visibility and analysis of access rights and data usage, and delivers protection against web-based threats.

SecureSphere for SharePoint provides multi-layered security that includes a Web Application Firewall to protect against web-based attacks, user rights management and activity monitoring to safeguard content such as files, folders and lists, and a Database Firewall to prevent unauthorized access to the Microsoft SQL database at the core of SharePoint.

Management Server (MX)

Internal Users

SecureSphere for SharePoint

SharePoint Web Servers

SharePoint Application Servers

SharePoint Database Servers

Database Security
Ensure database access is restricted to legitimate use

File Security
Maintain business need-to-know access, identify who accessed data, how and when

Web App Security
Prevent attackers from exploiting known attacks or application vulnerabilities

INTERNET

Aggregate and report on SharePoint permissions

SecureSphere aggregates and consolidates user rights across SharePoint sites to provide visibility into effective permissions. With SecureSphere for SharePoint, organizations can conduct rights reviews, eliminate excess rights, and identify dormant users, all of which help ensure access is based on business need-to-know.

Allow data owners to control file access

SecureSphere identifies data owners by providing visibility into the top users of SharePoint files, folders and lists. 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.

Audit all data access activity

SecureSphere provides continuous monitoring and detailed auditing of all data access activity so organizations have a complete audit trail showing the "Who, What, When, Where, and How" of each data access. This enables security, compliance and SharePoint administrative staff to understand exactly who accessed, moved, changed or deleted data.

Enforce security policies in real-time

SecureSphere for SharePoint delivers a flexible policy framework that allows business to take action immediately when data access activity deviates from corporate policy. Organizations can respond by generating alerts, or in certain situations, blocking access completely. Your sensitive files are safe with SecureSphere for SharePoint, the only security technology that can stop unwanted access to files stored in SharePoint.

Protect against web-based attacks

SharePoint is a web-based system, subject to online attacks such as SQL injection and cross-site scripting. SecureSphere for SharePoint incorporates market-leading SecureSphere Web Application Firewall, which protects SharePoint from current and future web security threats.

Prevent unauthorized database access

SharePoint stores all data – files, lists, and application data – within a Microsoft SQL database. SecureSphere for SharePoint incorporates market-leading SecureSphere Database Firewall to monitor all database access and ensure unauthorized access is prevented.

Identify unused data

SecureSphere helps alleviate the constant growth of SharePoint data by identifying data that is stored in SharePoint, but which no one is using. This allows organizations to archive or delete the data, which reduces management overhead and frees valuable storage space.

Quickly secure SharePoint

SecureSphere for SharePoint includes pre-packaged security policies based on the expertise of security researchers in the Imperva Application Defense Center (ADC). ADC Insights for SharePoint helps organizations quickly secure their SharePoint deployments.

About Imperva

Imperva, pioneering the third pillar of enterprise security, fills the gaps in endpoint and network security by directly protecting high-value applications and data assets in physical and virtual data centers. With an integrated security platform built specifically for modern threats, Imperva data center security provides the visibility and control needed to neutralize attack, theft, and fraud from inside and outside the organization, mitigate risk, and streamline compliance.