Accellion Share Securely™

Content Monitoring

Extends Accellion secure file sharing to enable policy-based content-aware data leak prevention for file sharing across devices.

KEY BENEFITS

- Extends Accellion secure file sharing to enable policy based content-aware data leak prevention.
- Provides additional security protection for intellectual property and sensitive information subject to industry and government compliance regulations.
- Monitors and filters Accellion file sharing according to corporate data protection policies.
- Enables integration of Accellion secure file sharing with industry leading
- Integrated file content monitoring and filtering for data leak prevention.
- Best-of-breed managed file sharing combined with best-of-breed DLP.

The Accellion DLP Module for Content Monitoring and Filtering addresses the increasing need to secure and control the movement of sensitive enterprise data to protect intellectual property and ensure compliance. The Accellion Content Monitoring and Filtering module enables organizations to not only secure the sharing of files but also monitor and analyze the contents of file sharing, and filter file sharing based on corporate policy, for protection of IP and compliance requirements.

Securing Data-in-Motion

An important element of any enterprise strategy for data leak prevention is ensuring security and compliance for data-in-motion. Many organizations have invested in email security and encryption technologies, however with 10MB limits of email attachments the lion share of data-in-motion is moving over unsecured, un-monitored channels. Secure file sharing needs to be major considerations in moving enterprise data. Accellion extends its solutions with content monitoring and filtering to ensure that file sharing is not only secure and tracked but also is monitored and filtered based on policy-based content-awareness.

Impact of Data-Leakage

- Compliance violations
- Loss of competitive advantage
- Negative branding
- Financial consequences
- Customer trust

Avoiding Data Breaches

No company wants to experience a data breach. Data breaches make headline news and have serious financial consequences.

Corporations and government agencies need to demonstrate that they are controlling sensitive information. SOX, HIPAA, GLBA, FDA regulations require auditable records of all data transfers and sharing to demonstrate compliance.

No company wants to fail a security audit. Yet if file sharing security is not addressed – it will be flagged. Un-secure, un-monitored, and un-filtered file sharing are data breaches waiting to happen.

Important Security Questions

How can I share information?

- How can I send and share files too big for email?
- Is it okay for me to transfer information on a thumb drive?
- Is consumer–based file sharing safe for corporate use?
- Is IM suitable for employees to transfer digital information?

What information can I share and with whom?

- Who decides what files can be shared and with whom?
- What information is considered valuable intellectual property?
- What information is controlled by compliance regulations?

Who is responsible for protecting sensitive information?

- What controls are in place to safeguard employees?

Best-of-Breed Technologies

The Accellion DLP Module for Content Monitoring and Filtering is designed to integrate with commercially available Data Leak Prevention solutions via the industry standard ICAP protocol. Accellion supports Symantec (Vontu), RSA, Fidelis, Palisades, WebSense, and Code Green Networks.

Enhanced Data Protection

An enterprise strategy for data leak prevention must consider data-in-motion. The Accellion DLP Module for Content Monitoring and Filtering enhances file sharing data protection. Files shared and sent via Accellion are not only securely shared, transferred, and tracked, but file content can also be inspected against corporate security policies and either quarantined or blocked.

Enhanced Data Security

The Accellion DLP Module for Content Monitoring and Filtering extends Accellion secure file sharing security features.

File/Data Security

For each transferred and shared document, Accellion provides a secure link generated by a double 128-bit MD5 token. SSL/TLS is used for encrypting file uploads and downloads using HTTPS. IPSec is used as files are replicated between appliances.

Business Level Security

Accellion contains authentication check points to validate recipients so confidential information is not overexposed. Users get return receipts with every file transfer and Accellion provides an audit trail with its file tracking.

Policy-based Content-Aware DLP

All files are subject to deep content inspection. Once inspected the Accellion DLP Module for Content Monitoring and Filtering either shares or transfers the file, or quarantines or blocks based on content inspection results.

Accellion® Share Securely™

Accellion, Inc.
1804 Embarcadero Road
Suite 200
Palo Alto, CA 94303

Tel +1 650 485-4300
Fax +1 650 485-4308
www.accellion.com
info@accellion.com