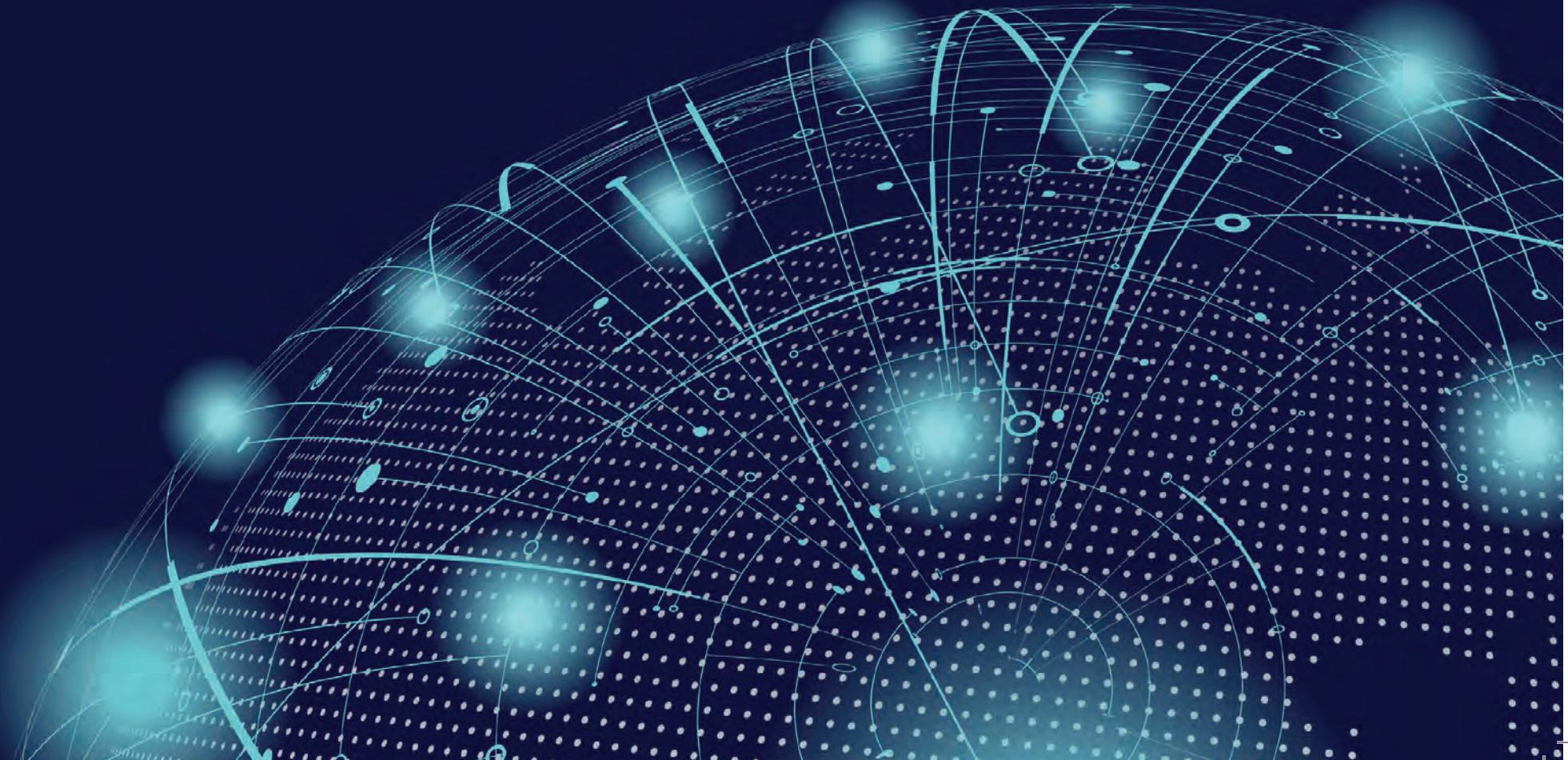


Protection, Privacy And Peace Of Mind For Sharing Sensitive Enterprise Information

EXTERNAL FILE SHARING SECURITY & GOVERNANCE PLATFORM



PROTECTION. PRIVACY. **PEACE OF MIND.**

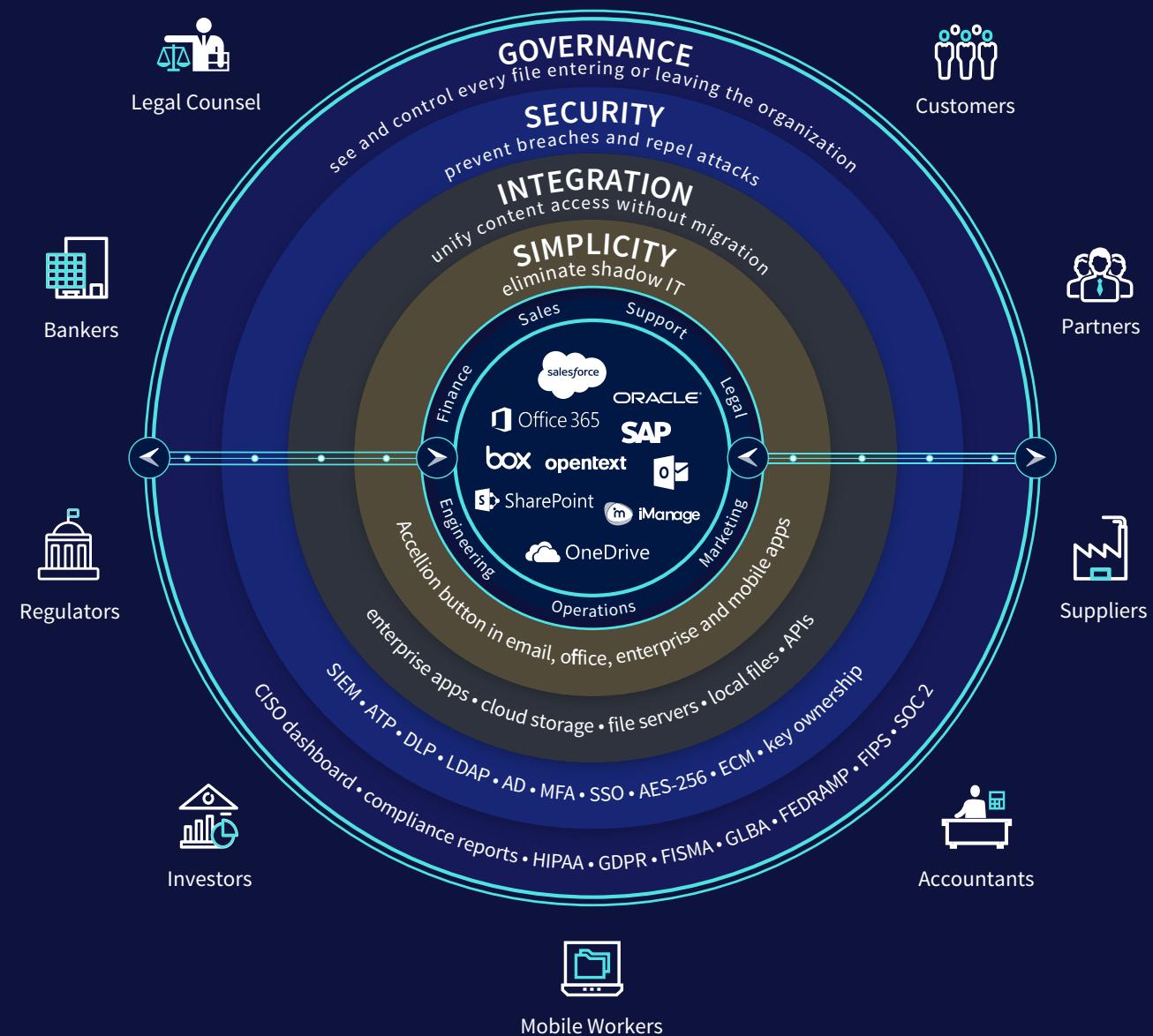
The Acceilion secure file sharing and governance platform empowers millions of executives, employees, government workers, customers, vendors, partners, investors, attorneys, doctors, patients, and professionals from every walk of life to do their jobs efficiently—without putting their organizations at risk.

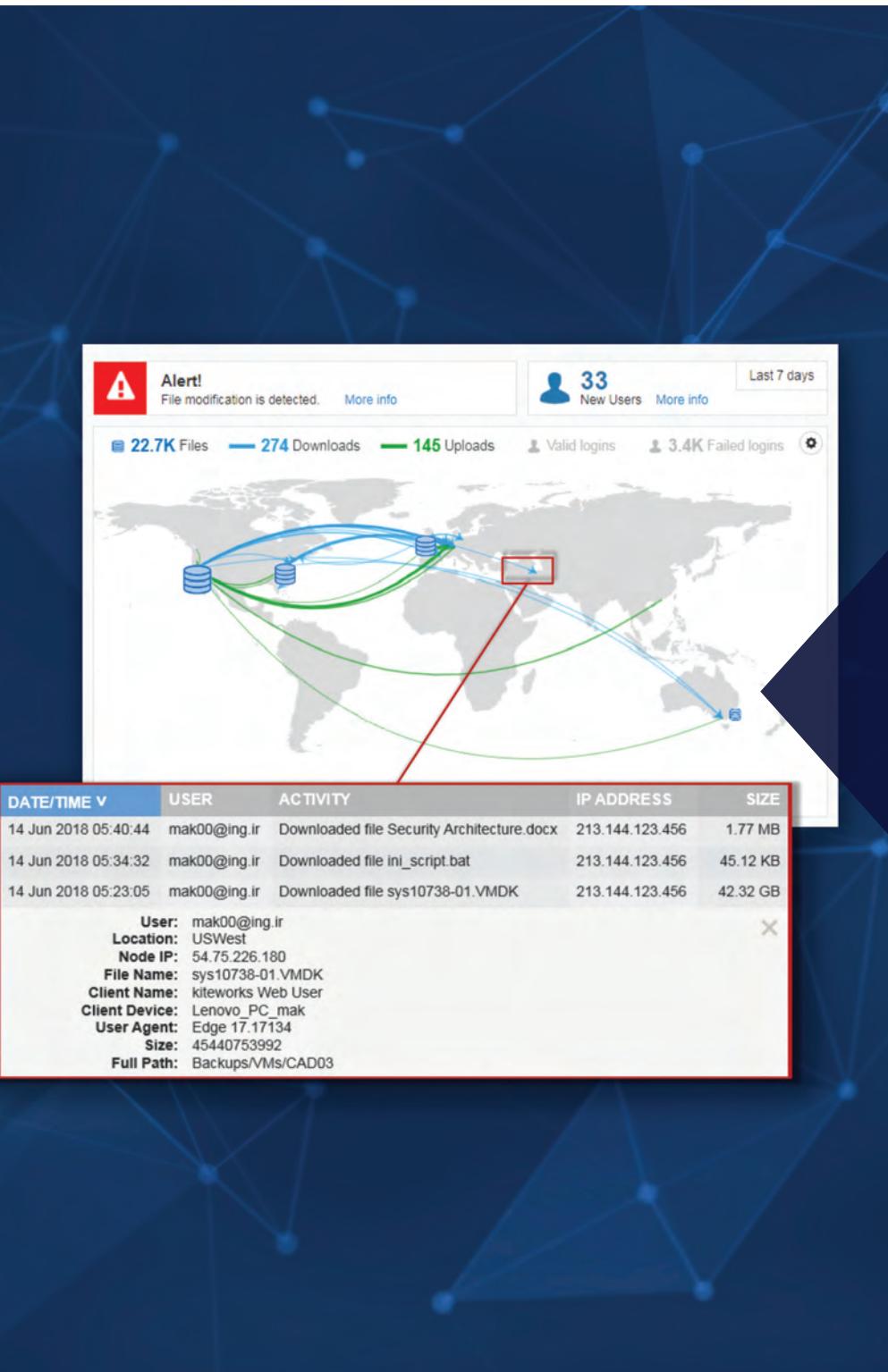
When users click the Acceilion button inside email, Web, mobile, office or enterprise apps, they know it's the safe and secure way to share sensitive information with the outside world. By giving users an easy, secure external communication channel, CISOs prevent data leaks, protect against malicious attacks, eliminate shadow IT, and gain visibility to all sensitive content entering and leaving the organization.

With on-premise, private cloud, hybrid and FedRAMP deployment options, the Acceilion platform provides the security and governance you need to protect your organization, mitigate risk, and adhere to rigorous compliance regulations, such as NIST 800-171, HIPAA, GDPR, FISMA, GLBA, ITAR, and FedRAMP.



EXTERNAL FILE SHARING SECURITY AND GOVERNANCE PLATFORM





GOVERNANCE

Visibility, Compliance and Control of Sensitive Content

To protect sensitive information like customer records and intellectual property, businesses must have full visibility into how information is shared, who is accessing it, and where it is stored. The Accelion secure file sharing and governance platform ensures businesses share sensitive information beyond their enterprise borders securely and in compliance.

See Every File Enter and Leave Your Organization

The Accelion CISO Dashboard monitors every file that enters or leaves your organization, providing a complete map of all IP, PII, and other sensitive information shared with external parties. Detailed drill-downs and ad-hoc reports provide the who, what, where, when and how of every external file transfer. With the CISO Dashboard, CISOs quickly separate normal business activity from suspicious anomalies to improve data governance and prevent a data breach.

Enforce Industry Compliance

Whether you're in a highly-regulated industry like healthcare or financial services, or do business with government agencies, the Accelion platform enables your organization to comply with rigorous industry regulations and standards. CISOs leverage best-in-class security and privacy protections to enforce internal policies and demonstrate compliance with HIPAA, GDPR, SOC2, FedRAMP, FIPS, and more. One-click, audit-ready compliance reports provide proof that you have full visibility and control over the sensitive information you handle and share.



Ensure Data Privacy 24/7/365

CISOs must ensure the confidentiality of customer data, intellectual property and other sensitive information their organizations collect. Protect data privacy with granular policy controls and role-based user privileges across all clients (plugins, web, mobile, desktop, SFTP, and APIs) to control where sensitive information is stored, who has access to it, and what can be done with it. With the Accellion platform, CISOs ensure only authorized users – internal and external – access and share sensitive information.

"We have an obligation to our clients to make certain that their information is transported in a secure, managed, and trackable manner and Accellion makes that possible."

- Andy Jurczyk, Seyfarth Shaw LLP

Maintain Control of Sensitive Data

Organizations must enforce data sovereignty policies as data privacy laws become increasingly rigorous. With the Accellion platform, organizations choose between on-premise, private cloud, hybrid, or fully hosted deployment to fit their needs and ensure customer data stays where it belongs. Assign access privileges to users and define storage locations by country. Use the CISO Dashboard to get a complete picture of all sensitive information by geography. All file activity is logged and reported, so CISOs ensure and prove compliance with local regulations.

The screenshot displays two overlapping configuration panels from the Accellion platform:

- Two-Factor Authentication Panel:**
 - Left Sidebar:** Application, Software and Licensing, Application Settings, Authentication and Authorization (selected), General Settings, LDAP, SSO Setup, Two-Factor Authentication (selected).
 - Content:** A checkbox labeled "Enable Two-Factor Authentication" is checked. Below it is another checkbox "Apply Two-Factor Authentication to Admin Logins also". A note at the bottom says "Note: Go to User Profiles to enable Two-Factor Authentication on specific profiles".
- DLP settings Panel:**
 - Left Sidebar:** Application, Software and Licensing, Locations Rules, Client Management, Enterprise Content Sources, Appearance, Integrations, Authentication and Authorization (selected), Locations Rules, Client Management, Enterprise Content Sources, Appearance, Integrations.
 - Content:** Configuration for DLP settings, including "Scan files in Enterprise Content Sources" set to "Downloads only", "DLP Server Host" set to "192.168.123.456", "DLP Server Port" set to "1344", "DLP Server URI" set to "icap://192.168.123.456/request", "DLP Method" set to "POST", and "Enable Transfer Encoding Chunked" checked. It also includes fields for "DLP KeyWords" (set to "hello,fail,jpegm,docx,doc"), "X-Authenticated-User" (set to "WinNT://<location hostname>/<user >"), and "Enable SSL Mode" checked. Under "Policy for Existing Files in kiteworks", the "Scan before access" option is selected. Policies for "Marked Content Violated by DLP" (set to "Lock file") and "Files that Could Not be Scanned" (set to "Report only") are listed. "Notify by Email" is checked.

SECURITY

Prevent Data Breaches and Cyber Attacks

Designed with security in mind from the ground up—architecture, data protection, authentication and authorization—the Accellion secure file sharing and governance platform offers a protected data transfer channel that guards your sensitive information in transit and at rest.

Strong Data Encryption In-transit and at Rest

CISOs know their organizations' sensitive information needs to be protected at all times. With the Accellion platform, organizations have comprehensive data encryption, including SSL/TLS 1.2 in transit, AES-256 at rest, and sole encryption key ownership. These capabilities ensure sensitive information stays safe at all levels, from physical data storage to network communications. The Accellion platform is FIPS 140-2 certified and supports FedRAMP Authorized hosting, so CISOs know their data is always protected against unauthorized access.

Integrated With Your Security Infrastructure

Organizations in highly regulated industries must have an extensive security infrastructure in place to prevent internal data breaches and repel cyber attacks. The Accellion platform integrates with your organization's existing security infrastructure to assure data privacy for all files going in and out of the organization. SSO support for SAML 2.0 and Kerberos as well as integration with LDAP and Active Directory allow CISOs to simplify and secure the user experience across Web, mobile, SFTP, Windows, Mac, and APIs. Lastly, integration with best-in-class DLP and ATP solutions help prevent data leaks and zero-day attacks.

“We didn’t want employees to take matters into their own hands and turn to consumer-driven solutions. Our documents contain proprietary information, such as financial budgets and engineering specifications. Therefore, finding a secure file sharing solution was paramount.”

- Iljo Bundebski, Auxitec Ingénierie

Deployment Options to Fit Your Unique Security Needs

Because your organization has unique security needs, the Accellion platform offers flexible, scalable deployment options that strike the right balance between privacy, compliance, scalability, and cost. Achieve full privacy and security with an on-premise deployment. Reduce costs while increasing security with a hybrid cloud deployment where you own the encryption keys. Avoid co-mingling of data with a private cloud deployment or outsource hosting to Accellion with a dedicated, isolated FedRAMP Authorized deployment.

Secure, Easy to Maintain Hardened Virtual Appliance

The Accellion platform runs as a hardened virtual appliance that's self-contained and pre-configured to the most secure posture available. Unnecessary services are disabled, unused ports and SSH access are shut off by default, and encryption, anti-virus protection, and intrusion detection are embedded. Optimized for security and fast, easy deployment on any cloud or virtualized environment, the Accellion platform is scalable based on usage and upgrades are fast and painless. Accellion also performs periodic penetration tests, conducts regular security audits, and issues targeted security updates to ensure the highest level of ongoing protection.



SIMPLICITY

Prevent Shadow IT and Speed Adoption

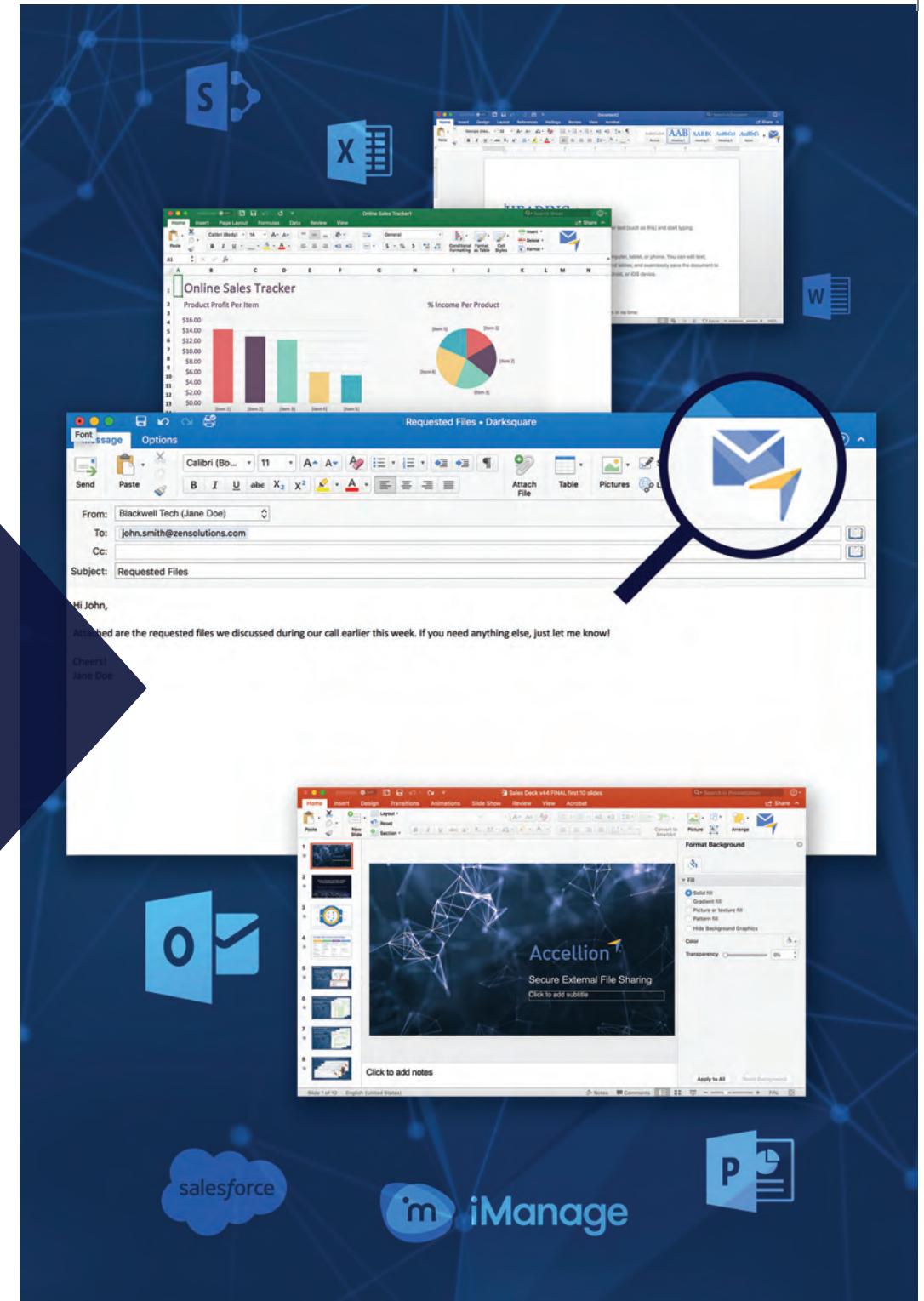
The Accellion secure file sharing and governance platform empowers millions of professionals to do their jobs without putting their organizations at risk. When they click the Accellion button inside email, web, mobile, office and enterprise apps, they know it's the safe and secure way to share sensitive information with the outside world.

Share Files Securely with Plugins

Empower employees to securely share sensitive documents from the apps they use all day, every day. The Accellion platform provides simple plugins for Microsoft Office apps, including Word, Excel, PowerPoint, and Outlook, as well as for enterprise apps, including Salesforce, iManage and SharePoint. While working inside these products, Accellion enforces your IT security and privacy policies, performs DLP and ATP scans on file downloads and uploads, and provides a detailed audit trail.

Lock Down Private Email Communications

CISOs have a vested interest in making it easy for employees to work securely and efficiently. The Accellion platform provides an easy-to-use Microsoft Outlook plugin, web client, and mobile app that make it simple for users to share password-protected emails and secure email attachments of any size or format from any location or device, with enterprise-grade encryption in transit and at rest. Flexible controls, detailed audit logs, and a CISO Dashboard help you manage compliance at both end-user and admin levels.



Keep Mobile Workers Secure and Productive

Busy road warriors shouldn't compromise security in the name of efficiency. With the Accellion mobile apps for iOS and Android, employees stay both productive and secure while they're travelling. The Accellion platform provides safe and simple access to content, so users can find what they need quickly, review and edit it easily, and share it securely with complete compliance. Should a mobile device be lost or stolen, or an employee leave the organization, all sensitive data stored in the Accellion secured container can be remotely wiped.

Secure Shared Folders

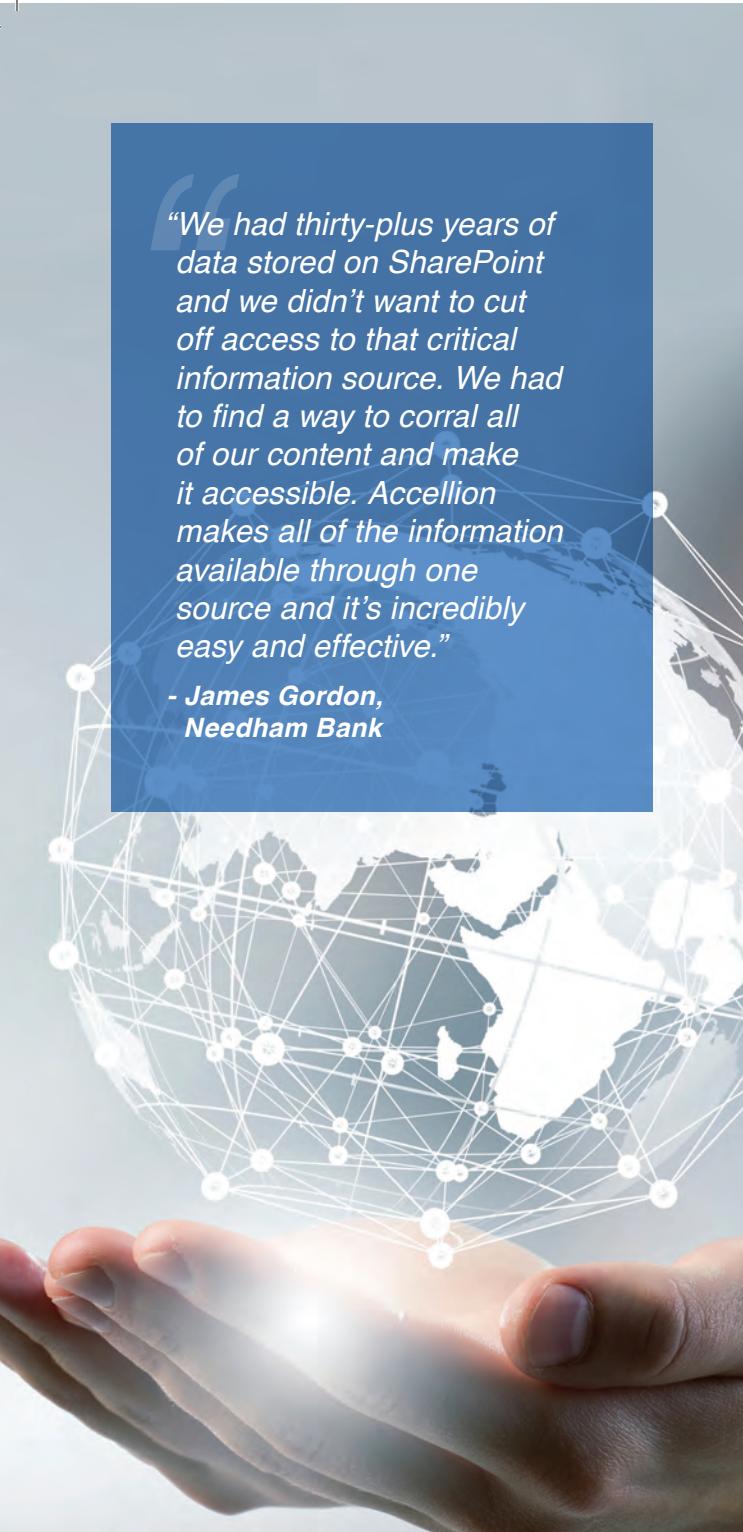
Accellion secure shared Web folders enable easy online collaboration and simultaneously increase data security, compliance, and governance. Give users the same simple experience that they understand from consumer file sharing apps, while locking down access, enforcing granular permissions, and achieving compliance with total visibility.



"The rapid increase in adoption is a direct result of the Accellion Outlook plugin. Because it looks and feels like email, adoption is higher — the convenience it delivers to employees is huge."

*- Soma Bhaduri,
NYC Health + Hospitals*





"We had thirty-plus years of data stored on SharePoint and we didn't want to cut off access to that critical information source. We had to find a way to corral all of our content and make it accessible. Accellion makes all of the information available through one source and it's incredibly easy and effective."

- James Gordon,
Needham Bank

INTEGRATION

Unify Access to Content Without Migration

The Accellion secure file sharing and governance platform provides organizations robust enterprise content integration and workflow automation that allow users to simply and securely access and share confidential enterprise content from applications, content management systems, network file shares, and cloud storage, just as easily as sharing local files.

Share Content from Core Systems Securely and Simply

The Accellion platform provides enterprise employees with a single, secure source of access to the content that's stored across the organization, whether it's on-premise or in the cloud. With connectors to network file shares and ECM systems like SharePoint and OpenText, as well as cloud storage solutions like OneDrive, Box, and SharePoint Online, organizations avoid costly and risky content migrations. In addition, REST APIs enable integrations with legacy enterprise systems. All content, no matter where it's stored, is readily available – from any location, using any device – without a VPN. Because content is easily accessible from a single interface, enterprise employees are more productive when locating and sharing files.

Strengthen Cloud Storage Security for External Sharing

With the Accellion platform, CISOs have visibility into all the content entering and leaving the organization, even when that content is sent or received from popular cloud services like OneDrive, SharePoint Online, Box, Dropbox, and Google Drive. By providing a secure information exchange channel for these services, CISOs enforce the security, compliance, and governance their enterprises require. Lastly, ATP and DLP scans and detailed audit logs of all file transfers provide additional protection and governance for cloud storage repositories.

Automate File Transfers

Save time, reduce errors, and strengthen compliance with a robust enterprise workflow automation toolkit. Choose from three flexible approaches for automated sending, receiving, and distributing enterprise content: SFTP for scaling out and consolidating servers and reducing admin costs; configurable, code-free automation agents for compliant file transfers; and powerful, flexible REST APIs allow you to create content-enabled apps and integrations. Whichever approach you choose, Accellion-enabled workflow automation helps CISOs ensure compliance and security, while eliminating manual processes in your organization.

FEATURE HIGHLIGHTS



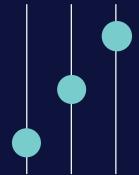
GOVERNANCE

- CISO Dashboard
- Visibility into all files entering and leaving the organization
- Complete audit trails and system logs
- Detailed one-click compliance reports
- Granular policy controls and permissions for data privacy
- Data sovereignty
- Compliant with HIPAA, GDPR, FIPS, SOC 2, NIST 800-171, ITAR, FedRAMP, and others



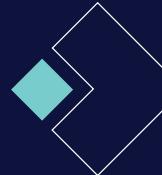
SECURITY

- Encryption in transit (TLS 1.2) and at rest (AES-256)
- Encryption key ownership
- FIPS 140-2 certified
- Integration with SSO, LDAP/AD, DLP, ATP, SIEM, MDM, and MFA/2FA
- Hardened virtual appliance
- On-premise, private cloud, hybrid or FedRAMP deployment options
- No vendor access to content or metadata
- Embedded AV and native 2FA



SIMPLICITY

- Secure email communications, including MS Outlook plugin
- Secure Web folders with the same ease of use found in consumer file sharing apps
- Dedicated mobile apps for iOS and Android
- Secure Microsoft Office and MS Office 365 plugins for Word, Excel and PowerPoint
- Enterprise plugins for Salesforce, iManage and SharePoint
- Unlimited file sizes
- Online forms



INTEGRATION

- Unified access to ECMs and file shares without a VPN
- Unified access to cloud storage systems like Box, Dropbox, and OneDrive
- No content migration
- Governance wrapper around Microsoft OneDrive for Business
- Automated, code-free secure file transfers
- Consolidated, self-service SFTP
- Comprehensive REST API
- SMTP integration



The Accellion platform enables organizations to securely share sensitive information beyond enterprise borders while maintaining the controls and visibility needed to demonstrate compliance. Accellion's solutions have been used by more than 25 million end users and have been installed at more than 3,000 of the world's leading corporations and government agencies including NYC Health + Hospitals; KPMG; Kaiser Permanente; Latham & Watkins; National Park Service; Umpqua Bank; Cargill; and the National Institute for Standards and Technology (NIST).

www.accellion.com | sales@accellion.com

© 2018 ACCELLION. All rights reserved

Accellion, Inc.

1804 Embarcadero Road, Palo Alto, CA 94303

Phone: +1 650 485 4300

EMEA Headquarters

Löwen-Markt 5, 70499 Stuttgart, Germany

Phone: +49 711 252861 0

APAC Headquarters

Blk 750A Chai Chee Rd #08-01B

Viva Business Park, Singapore 469001

Phone: +65 62445670

