Accellion

Prevent Breaches and Compliance Violations from 3rd Party Communications

ENTERPRISE CONTENT FIREWALL

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

The Accellion enterprise content firewall prevents data breaches and compliance violations from 3rd party communications, empowering professionals from every walk of life to do their jobs efficiently — without putting their organizations at risk.

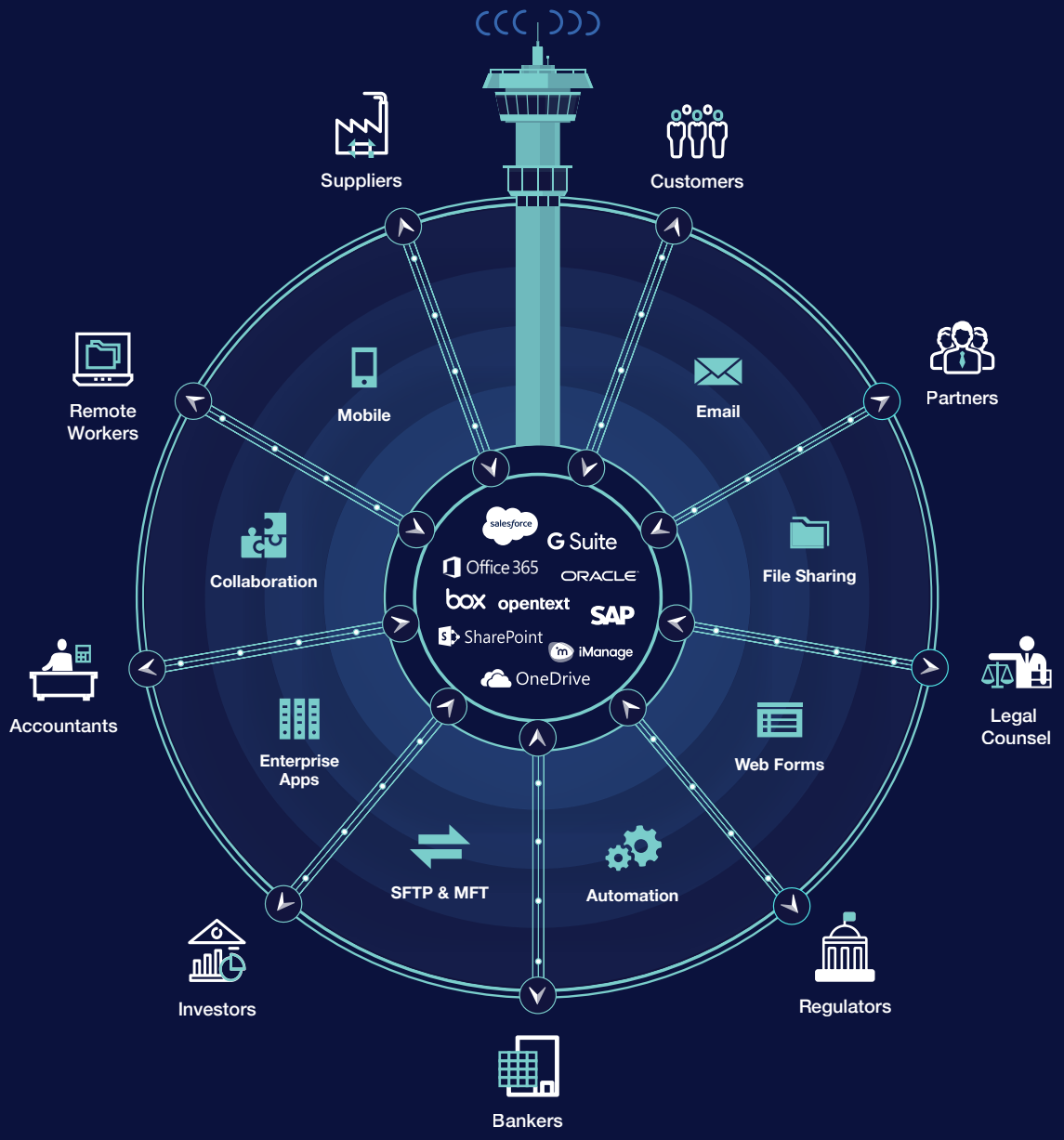
With Accellion, CIOs and CISOs gain complete visibility, compliance and control over IP, PII, PHI, and other sensitive content across all 3rd party communication channels, including email, file sharing, mobile, enterprise apps, web portals, SFTP, and MFT. When users click the Accellion button, they know it's the safe, secure way to share sensitive information with the outside world.

With on-premise, private cloud, hybrid and FedRAMP deployment options, the Accellion platform provides the security and governance CISOs need to protect their organizations, mitigate risk, and adhere to rigorous compliance regulations such as NIST 800-171, HIPAA, SOX, GDPR, GLBA, FISMA, and others.

Accellion

ENTERPRISE CONTENT FIREWALL

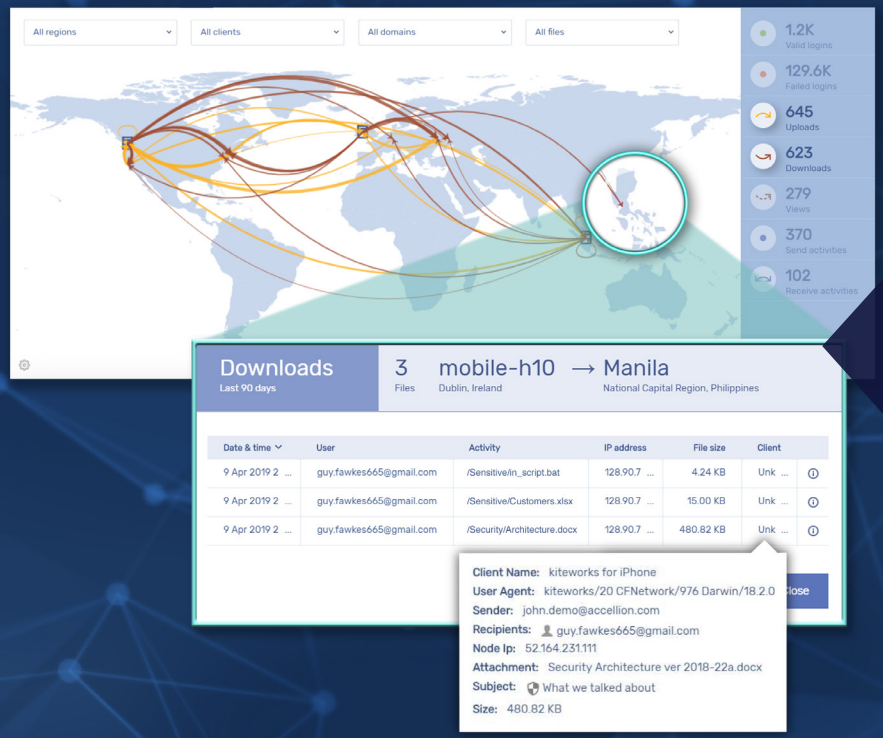
Visibility, Compliance, and Control of Sensitive Third Party Communications



TOTAL VISIBILITY

If You Can't See It, You Can't Protect It

To prevent leaks of sensitive information like customer records and intellectual property, businesses must have full visibility into what information is shared, who is accessing it, and where it is going. You need to know which 3rd parties have custody of your precious digital assets, and you need to know what IP, PII, and PHI has been entrusted to you. The Accellion enterprise content firewall ensures businesses share sensitive information beyond their borders securely and in compliance.



See All Sensitive Content Shared with 3rd Parties

The Accellion CISO Dashboard monitors every file that enters or leaves your organization, providing a complete map of all IP, PII, PHI, 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.

Detect Sharing Anomalies

CISOs and security ops teams rely on the Accellion CISO Dashboard to detect anomalous content communications that indicate potential 3rd party and insider threats. Out-of-the-box security analytics provide real-time and historical views of how your business shares and consumes sensitive content, while AI machine learning and alerts help you identify threats before they turn into breaches.

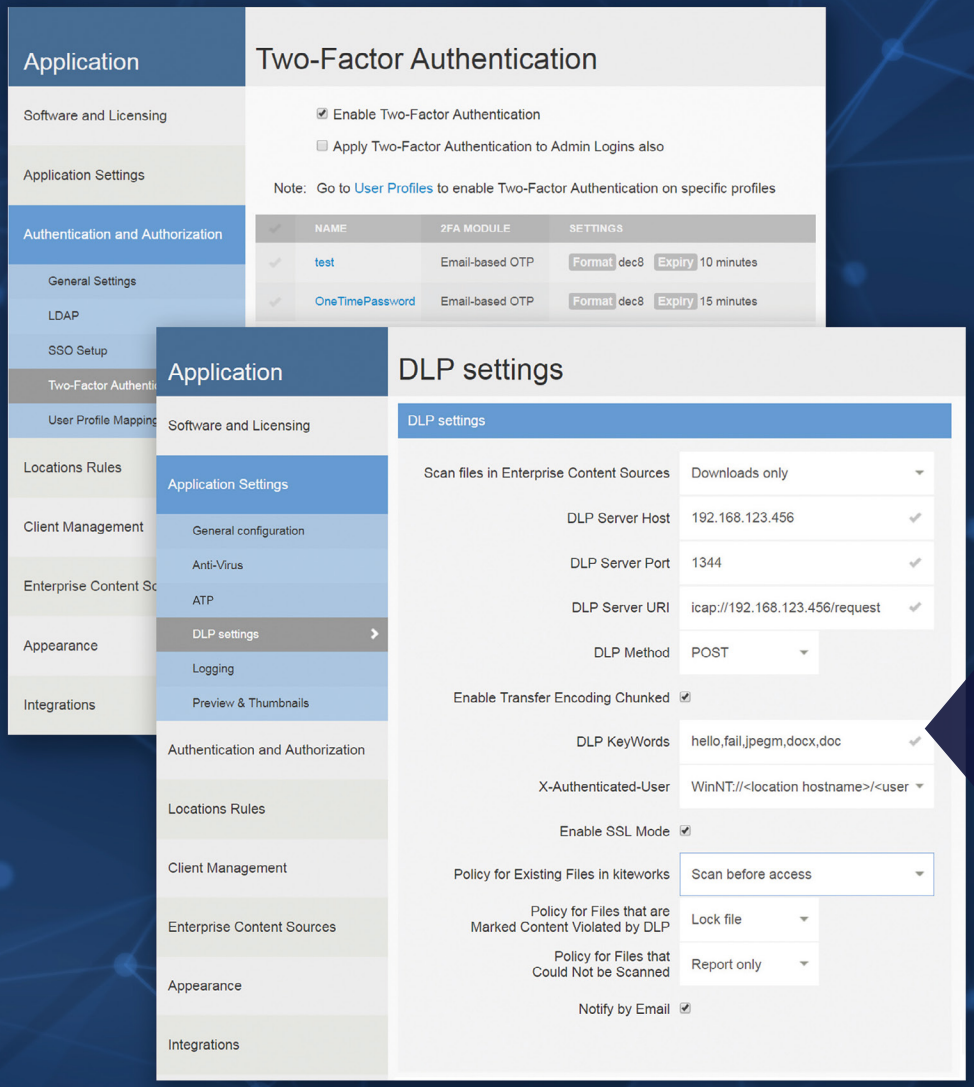
Expedite Incident Responses

The Accellion platform helps security teams investigate and respond rapidly to potential incidents with drill-downs into every suspicious communication, yielding the fine-grained details they need to take action. Separate unusual-but-harmless behavior from security incidents, prioritize threats, and pinpoint the exact content, users, sources, and destinations of suspect transactions. In addition, detailed audit logs can be piped into your own SIEM for custom, integrated views tailored to your security operations.

> *"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***

Demonstrate Regulatory Compliance

Whether you're in a highly-regulated industry like healthcare or financial services, or do business with government agencies, the Accellion 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.



ZERO TRUST SECURITY

Prevent Data Breaches and Cyber Attacks

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

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.

Integrated With Your Security Infrastructure
The Accellion enterprise content firewall integrates with your organization's existing security infrastructure. 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. Integration with best-in-class DLP and ATP solutions help prevent data leaks and zero-day attacks.

Apply Uniform Security and Governance

The Accellion enterprise content firewall protects all content entering and leaving the organization across all communication channels, including content shared from popular cloud services like OneDrive, SharePoint, Box, Dropbox, and Google Drive. Accellion wraps these services in a uniform layer of security and governance, such as centralized ATP and DLP scans. Plus, detailed audit logs provide complete traceability, so you know who has your IP regardless of how it was shared, and you can protect the IP, PII and PHI shared with you.

"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 Bundevski, Auxitec Ingénierie

Strong Data Encryption In-transit and at Rest

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.

Secure Deployment, Easy Maintenance

The Accellion platform offers flexible deployment options to strike the right balance between privacy, compliance, scalability, and cost. Achieve full privacy 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. The Accellion platform runs as a hardened virtual appliance that's self-contained and pre-configured to the most secure posture available. Accellion also performs periodic penetration tests, conducts regular security audits, and issues targeted security updates for the highest level of ongoing protection. So, regardless of the deployment option you choose, the Accellion platform ensures upgrades are fast, painless and secure.

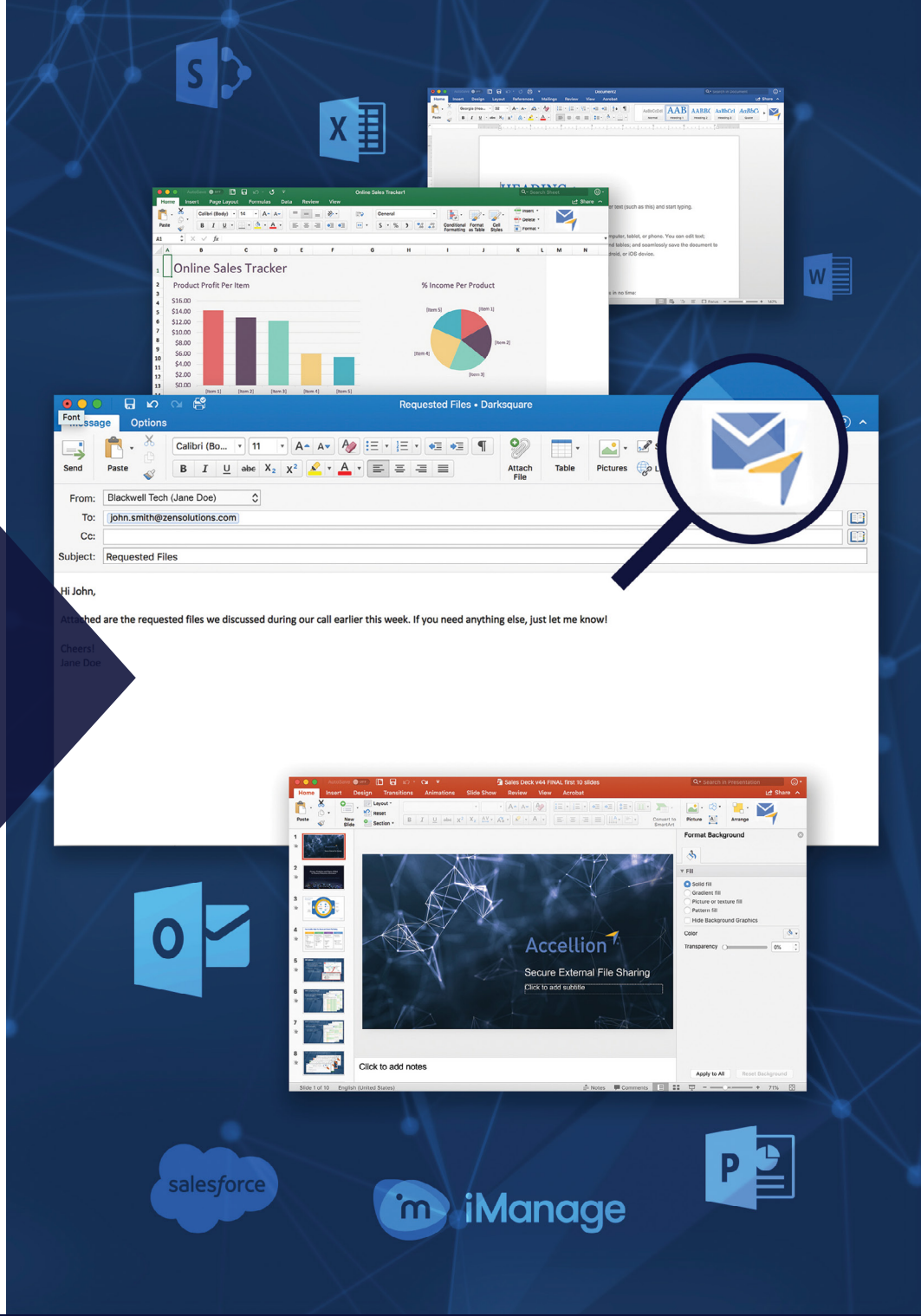
COMMUNICATION SIMPLICITY

Streamline Infrastructure by Consolidating Security

The Accellion enterprise content firewall simplifies IT infrastructure, administration, and usability by consolidating security across 3rd party communication channels, including email, file sharing, enterprise apps, web forms, SFTP, MFT, and mobile. Replace standalone secure sharing apps with a single platform to save money, while simplifying the user experience. When employees click the Accellion button, they know it's the safe and secure way to share information with the outside world.

Share Securely From Enterprise Apps

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 Google Drive, and many 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 makes it simple for users to share secure emails from any location or device, with attachments of any size or format, and enterprise-grade encryption in transit and at rest. Simply route email transparently through the secure mail gateway, or utilize easy-to-use secure mobile apps, web apps, and plugins. Flexible controls, detailed audit logs, and a CISO Dashboard help you manage compliance at both end-user and admin levels.

Secure File Sharing

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.

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.

> *"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***

Simplify and Secure Access to Content

Give employees unified and uniform access to content sources such as file shares and SharePoint, while consistently enforcing security and compliance. Make content, no matter where it's stored, readily available – from any location, using any device – without a VPN and without risky data migrations. Thus users collaborate with 3rd parties via email, shared folders, and other channels without exposing the source systems. 3rd party transfers to and from cloud storage services like OneDrive, Box, SharePoint Online, and Google Drive traverse the Internet through a hardened, compliant channel. Because content is easily accessible from a consistent interface, enterprise employees accomplish more, and confidential information stays private.

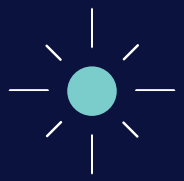
Automate 3rd Party Workflows

Save time, reduce errors, and strengthen compliance with a robust enterprise workflow automation toolkit. Choose from four flexible approaches for automated sending, receiving, and distributing of enterprise content: SFTP for scaling out and consolidating servers and reducing admin costs; no-code visual orchestration for compliant file transfers, data transformations, inter-enterprise integrations, and admin flows; a secure mail gateway for securing email attachments from multi-function scanners and software applications; and flexible REST APIs for securing content-enabled apps and inter-enterprise integrations. Whichever approach you choose, Accellion-enabled workflow automation helps CISOs ensure compliance and security, while eliminating manual processes in your organization.

Modernize Managed File Transfer (MFT)

Automate 3rd party content workflows and business operations where security and compliance are top concerns. Depend on it to keep business processes running smoothly and to protect your organization from breaches and compliance fines. Visually orchestrate managed file transfer workflows, automate email and administrative tasks, and simplify routine file sharing setup – all without coding. And using its extensible visual library, flow authors can leverage system commands, data file manipulations, user forms, and integrations with legacy systems and cloud services. Modernize managed file transfer on Accellion's platform to accelerate your business and protect your organization.

FEATURE HIGHLIGHTS



TOTAL VISIBILITY

Security Analytics

- CISO Dashboard
- Visibility into all content entering and leaving the organization
- Alerts powered by machine learning
- Custom and scheduled reports
- Splunk and SIEM integrations
- Transcription filtering and drill-down by sender, receiver, location, file type, etc.

Compliance

- Detailed one-click compliance reports
- Complete audit trails, system logs, and eDiscovery archives
- Compliant with HIPAA, GDPR, FIPS, SOC 2, NIST 800-171, ITAR, FedRAMP, and others

ZERO TRUST SECURITY

Governance Controls

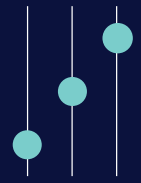
- Granular policy controls and permissions for data privacy
- Authentication policies based on role and location
- Dynamic policy automation based on data classification and other factors
- Least privilege defaults
- Dynamic quarantine
- No vendor access to content or metadata
- Data sovereignty

Security Framework

- Hardened virtual appliance
- Encryption in transit (TLS 1.2) and at rest (AES-256)
- Encryption key ownership
- Embedded AV and native 2FA
- SMS one-time passcode authentication
- Integration with SSO, LDAP/ AD, DLP, ATP, SIEM, MDM, MFA/2FA, SMS, and HSM

Secure Deployment

- On-premise, private cloud, hybrid, or FedRAMP deployment options
- Cluster for global scale and HA



COMMUNICATION SIMPLICITY

Communication Capabilities

- Secure email
- Secure shared Web folders
- Secure collaboration, boardroom communications, and virtual data rooms
- Dedicated mobile apps for iOS and Android
- Secure Web forms
- Self-service SFTP
- Managed File Transfer (MFT)
- Unlimited file sizes

Custom Automation

- Code-free visual workflow orchestration
- Comprehensive REST API
- Secure mail gateway

Secure Content Access

- Unified access to file shares, SFTP, and ECMs
- Unified storage access to Box, Dropbox, OneDrive, and Google Drive
- No content migration; no need for a VPN

Secure Enterprise App Sharing Plugins

- Microsoft Office & MS Office 365
- Google Docs and Google Drive
- Salesforce, iManage, and SharePoint

Accellion

The Accellion enterprise content firewall prevents data breaches and compliance violations from 3rd party communications. With Accellion, CIOs and CISOs gain complete visibility, compliance and control over IP, PII, PHI, and other sensitive content across all 3rd party communication channels, including email, file sharing, mobile, enterprise apps, web portals, SFTP, and automated inter-business workflows.

Accellion has protected more than 25 million end users at more than 3,000 global corporations and government agencies, including NYC Health + Hospitals; KPMG; Kaiser Permanente; Latham & Watkins; National Park Service; Umpqua Bank; Tyler Technologies; and the National Institute for Standards and Technology (NIST).

www.accellion.com I **sales@accellion.com**

© 2020 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
750C Chai Chee Road, #04-12,
Viva Business Park, Singapore - 469003
Phone: +65 62445670