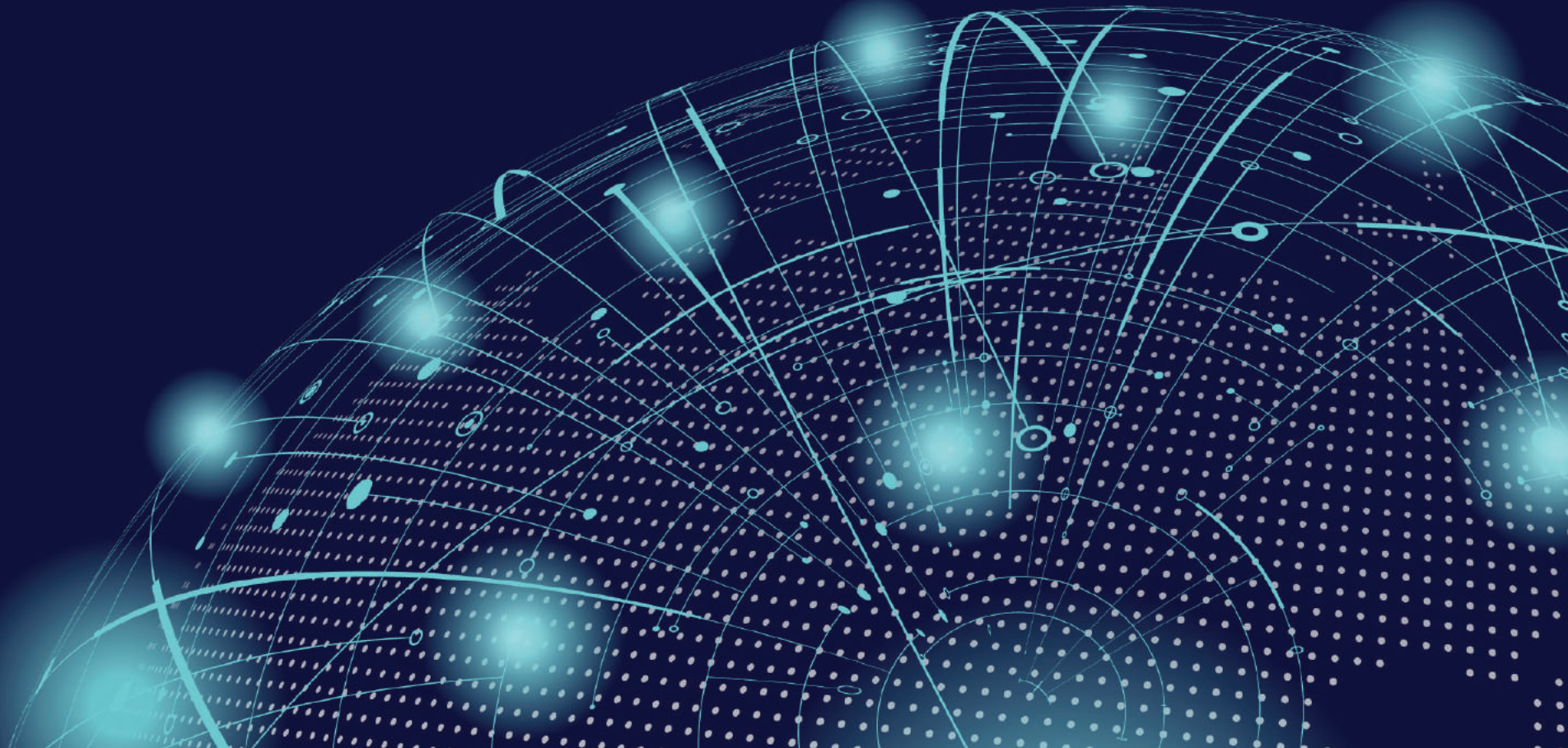


# Sicherer Datenaustausch mit Dritten - so machen Sie es richtig!

ENTERPRISE CONTENT FIREWALL



## VERTRAULICHKEIT. INTEGRITÄT. **VERFÜGBARKEIT.**

Geschäftsbeziehungen eröffnen Unternehmen viele Möglichkeiten, doch was passiert, wenn Geschäftspartner zum Compliance-Risiko werden? Dieses sogenannte "Third Party"-Risiko hat im Ernstfall nicht nur finanzielle Folgen, sondern kann sich auch negativ auf die Reputation und das Image eines Unternehmens auswirken.

Die Enterprise Content Firewall von Accellion verhindert Datenschutzverletzungen und Compliance-Verstöße, die durch die Kommunikation mit Dritten und damit verbundene Risiken entstehen. Dies ermöglicht es Fachleuten aus allen Bereichen ihre Arbeit effizient zu erledigen - ohne ihre Unternehmen dabei zu gefährden.

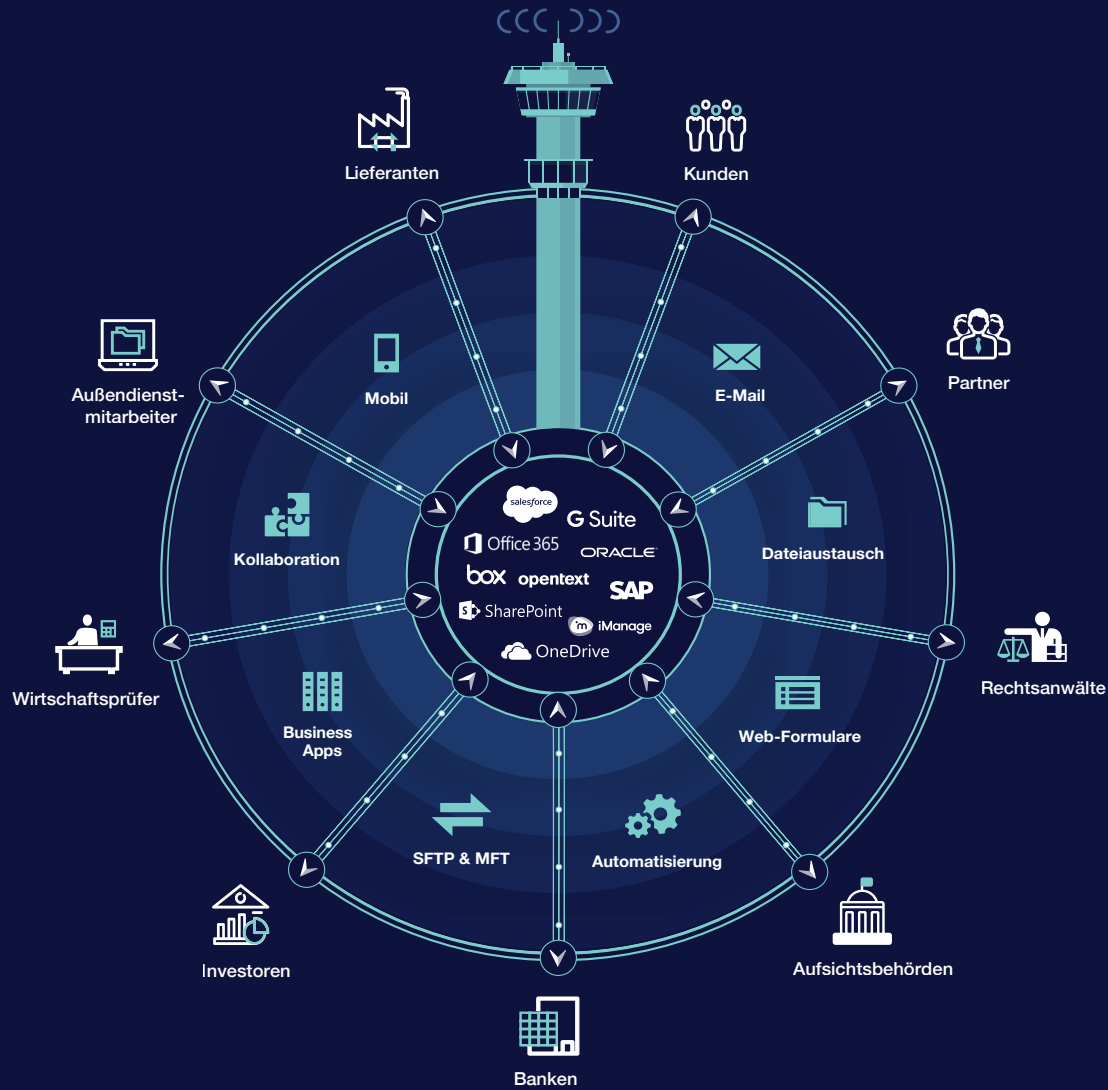
CIOs und CISOs verlassen sich auf die Accellion-Plattform, um vollständige Transparenz, Compliance und Kontrolle über den Austausch von geistigem Eigentum, personenbezogenen Daten, Patienteninformationen und anderen sensiblen Inhalten über alle Kommunikationskanäle mit Drittanbietern zu gewährleisten, einschließlich E-Mail, Dateifreigabe, Mobilgeräte, Business Applikationen und Webportale, SFTP und automatisierte unternehmensübergreifende Workflows. Wenn Benutzer auf die Accellion-Schaltfläche klicken, können sie sich darauf verlassen, dass dies die sicherste Möglichkeit ist, vertrauliche Informationen mit der Außenwelt auszutauschen.

Mit On-Premise-, Private Cloud-, Hybrid Cloud- und FedRAMP-Bereitstellungsoptionen bietet die Accellion-Plattform die Sicherheit und Governance, die CISOs benötigen, um ihr Unternehmen zu schützen, Risiken zu minimieren und strenge Compliance-Vorschriften wie beispielsweise DSGVO, NIST 800-171, HIPAA, SOX, GLBA und FISMA einzuhalten.

# Accellion

## ENTERPRISE CONTENT FIREWALL

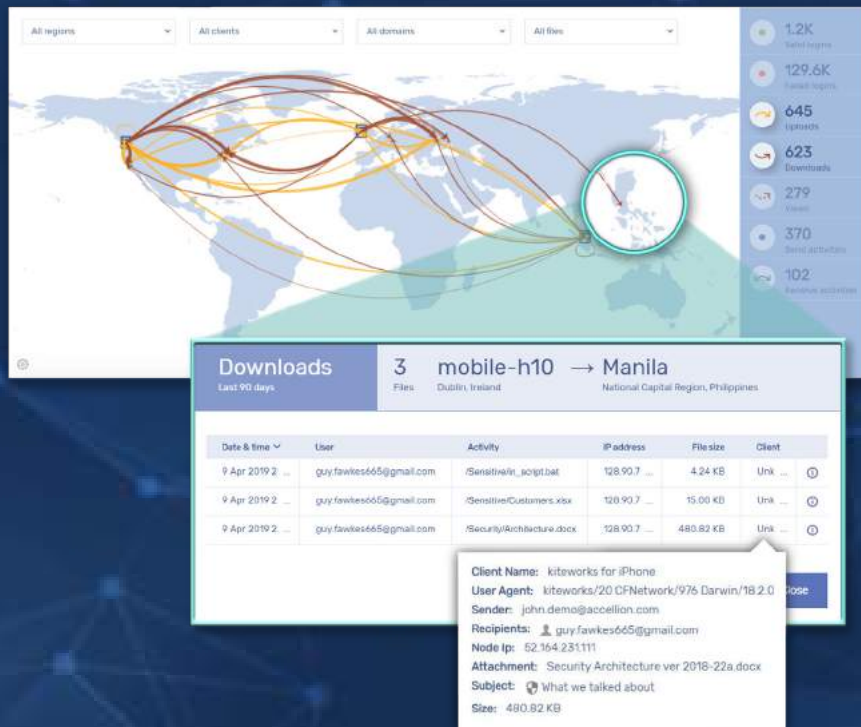
TRANSPARENZ, COMPLIANCE UND KONTROLLE ÜBER SENSIBLE KOMMUNIKATION MIT DRITTPARTEIEN



# VOLLKOMMENE TRANSPARENZ

## **Was Sie nicht sehen, können Sie auch nicht schützen**

Um sensible Informationen wie Kundendaten und geistiges Eigentum zu schützen, müssen Unternehmen einen vollständigen Überblick darüber haben, welche Informationen wohin weitergegeben werden und wer darauf zugreift. Die Enterprise Content Firewall von Accellion gewährleistet, dass Unternehmen sensible Informationen über ihre Unternehmensgrenzen hinweg sicher und gesetzeskonform austauschen.



### **Anzeige aller sensiblen Inhalte, die mit Dritten geteilt werden**

Das Accellion CISO-Dashboard überwacht jede Datei, die in Ihr Unternehmen gelangt oder es verlässt und bietet eine vollständige Übersicht über sämtliches geistiges Eigentum, Gesundheitsdaten, personenbezogenen Daten und andere sensible Informationen, die mit externen Parteien ausgetauscht werden. Detaillierte Recherchen und Ad-hoc-Berichte dokumentieren das Wer, Was, Wo, Wann und Wie jeder externen Dateiübertragung. Mit dem CISO-Dashboard trennen CISOs schnell normale Geschäftsaktivitäten von verdächtigen Anomalien, um die Governance zu verbessern und einen Datenverlust zu verhindern.

### **Aufdecken von Anomalien bei der Freigabe von Daten**

CISOs und Sicherheitsteams verlassen sich auf das Accellion CISO Dashboard, um anomale Content-Kommunikation zu erkennen, die auf potenzielle Bedrohungen durch Dritte und Insider hinweisen. Sofort einsatzbereite Sicherheitsanalysen liefern Echtzeit- und historische Daten darüber, wie Ihr Unternehmen sensible Inhalte teilt und verarbeitet, während maschinelles KI-Lernen und Warnmeldungen Ihnen helfen, Bedrohungen zu identifizieren, bevor sie zu einem Sicherheitsproblem werden.





### **Verkürzen Sie die Reaktionszeiten**

Die Accellion-Plattform unterstützt Sicherheitsteams bei der Untersuchung und schnellen Reaktion auf potenzielle Vorfälle mit Drill-Downs jeder verdächtigen Kommunikation und liefert die granulareren Details, die sie zum Einleiten von Maßnahmen benötigen. Trennen Sie ungewöhnliches, aber harmloses Verhalten von Sicherheitsvorfällen, priorisieren Sie Bedrohungen und ermitteln Sie den genauen Inhalt, die Benutzer, die Quellen und Ziele verdächtiger Transaktionen. Darüber hinaus können detaillierte Audit-Protokolle in Ihr eigenes SIEM geleitet werden, um benutzerdefinierte, integrierte Ansichten zu erstellen, die auf Ihre Sicherheitsprozesse zugeschnitten sind.

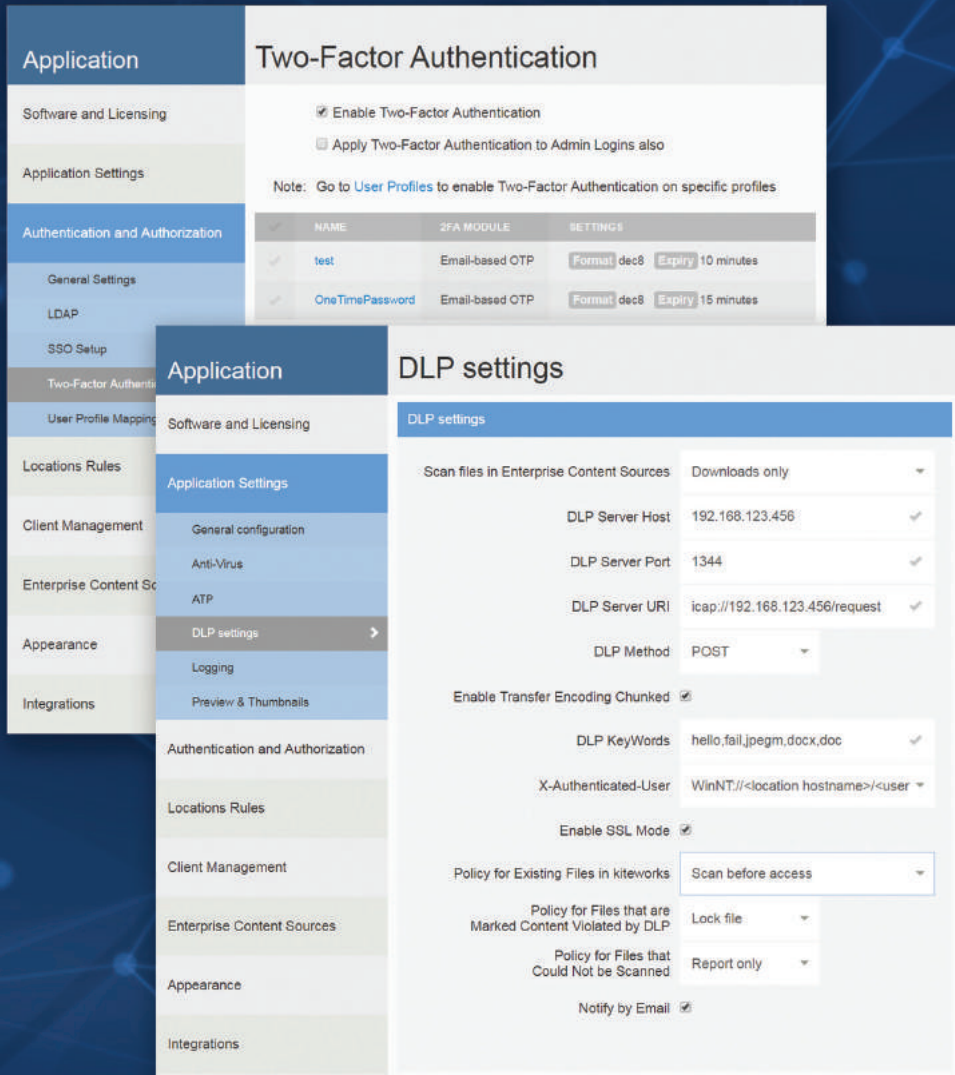
*“Wir sind unseren Kunden gegenüber verpflichtet, sicherzustellen, dass ihre Daten sicher, kontrolliert und nachvollziehbar transportiert werden. Accellion macht dies möglich.”*

**- Andy Jurczyk, Seyfarth Shaw LLP**

### **Durchsetzen von Regularien**

Ob Sie in einer stark regulierten Branche wie dem Gesundheits- oder Finanzwesen tätig sind oder Geschäfte mit Regierungsbehörden tätigen: die Accellion-Plattform ermöglicht Ihrem Unternehmen, strenge Branchenvorschriften und -standards einzuhalten. CISOs nutzen erstklassige Sicherheits- und Datenschutzmaßnahmen, um interne Richtlinien durchzusetzen und die Einhaltung gesetzlicher Vorgaben wie HIPAA, DSGVO, SOC2, FedRAMP und FIPS nachzuweisen. Mit nur einem Klick erbringen Sie anhand reversionssicherer Compliance-Berichte den Nachweis, dass Sie volle Transparenz und Kontrolle über die sensiblen Informationen haben, die Sie verarbeiten und weitergeben.





## ZERO-TRUST-SICHERHEIT

### **Verhindern Sie Datenschutzverletzungen und Cyberangriffe**

Von der Architektur, über den Datenschutz, die Authentifizierung bis hin zur Autorisierung - die Enterprise Content Firewall von Accellion wurde mit Blick auf Sicherheit entwickelt und bietet einen sicheren Datenübertragungskanal, der Ihre sensiblen Informationen während der Übertragung und im ruhenden Zustand schützt.

### **Datenschutz 24/7/365**

CISOs müssen die Vertraulichkeit von Kundendaten, geistigem Eigentum und anderen sensiblen Informationen, die von ihren Unternehmen erfasst werden, sicherstellen. Gewährleisten Sie Schutz sensibler Daten mit granularen Richtlinien und rollenbasierten Benutzerrechten für alle Clients (Plugins, Web, Mobile, Desktop, SFTP und APIs) und kontrollieren Sie, wo sensible Informationen gespeichert sind, wer Zugriff darauf hat und was mit diesen Daten geschehen darf. Mit der Accellion-Plattform stellen CISOs sicher, dass nur autorisierte Benutzer auf sensible Informationen zugreifen und diese austauschen können.

### **Integriert in Ihre Sicherheitsinfrastruktur**

Die Accellion Enterprise Content Firewall lässt sich in die bestehende Sicherheitsinfrastruktur Ihres Unternehmens integrieren, um Datenschutz für alle im Unternehmen ein- und ausgehenden Dateien zu gewährleisten. Die SSO-Unterstützung für SAML 2.0 und Kerberos sowie die Integration mit LDAP und Active Directory ermöglichen es CISOs, die Benutzerfreundlichkeit über Web, Mobile, SFTP, Windows, Mac und APIs auf einfache und sichere Weise zu gewährleisten. Schließlich hilft die Integration mit den besten DLP- und ATP-Lösungen, den unerwünschten Abfluss von Daten sowie Zero-Day-Angriffe zu verhindern.

### **Starke Datenverschlüsselung im Transit und ruhenden Zustand**

Mit der Accellion-Plattform verfügen Unternehmen über eine umfassende Datenverschlüsselung, einschließlich SSL/TLS 1.2 bei der Übertragung, AES-256 im ruhenden Zustand und den alleinigen Zugriff auf die Verschlüsselungscodes. Diese Funktionen gewährleisten, dass sensible Informationen auf allen Ebenen sicher bleiben, von der physischen Datenspeicherung bis zur Netzwerkkommunikation. Die Accellion-Plattform ist gemäß FIPS 140-2 zertifiziert und unterstützt FedRAMP Authorized Hosting, damit CISOs sicher sein können, dass ihre Daten immer vor unbefugtem Zugriff geschützt sind.

*“Wir wollten nicht, dass die Mitarbeiter die Dinge selbst in die Hand nehmen und sich für kostenlose Tools für den Privatgebrauch entscheiden. Unsere Dokumente enthalten vertrauliche Informationen, wie z. B. Finanzpläne und technische Spezifikationen. Deshalb war es von größter Bedeutung, eine sichere File-Sharing-Lösung zu finden.”*

**- Iljo Bundeovski, Auxitec Ingénierie**

#### **Starke Cloud-Storage-Sicherheit für den externen Datenaustausch**

Mit der Accellion Enterprise Content Firewall haben CISOs Einblick in alle Inhalte, die in das Unternehmen gelangen und es verlassen, selbst wenn diese Inhalte von verbreiteten Cloud-Services wie OneDrive, SharePoint Online, Box, Dropbox und Google Drive gesendet oder empfangen werden. Durch die Bereitstellung eines sicheren Informationsaustauschkanals für diese Dienste setzen CISOs die Sicherheit, Compliance und Governance durch, die ihre Unternehmen benötigen. Schließlich bieten ATP- und DLP-Scans sowie detaillierte Audit-Protokolle aller Dateiübertragungen zusätzlichen Schutz und Governance für Cloud-Datenspeicher.

#### **Sichere, einfach zu wartende, gehärtete virtuelle Appliance**

Die Accellion-Plattform läuft als gehärtete virtuelle Appliance, die in sich geschlossen ist und ein Höchstmaß an Sicherheit bietet. Unnötige Dienste werden ausgeschaltet, ungenutzte Ports und SSH-Zugriff werden standardmäßig deaktiviert, Verschlüsselung, Virenschutz und Intrusion Detection sind integriert. Die Accellion-Plattform ist optimiert für Sicherheit und schnelle, einfache Bereitstellung in jeder Cloud oder virtualisierten Umgebung. Darüber hinaus ist sie je nach Nutzung skalierbar und Upgrades können schnell und unkompliziert durchgeführt werden. Accellion führt regelmäßige Penetrationstests und Sicherheitsaudits durch und erstellt gezielte Sicherheits-Updates, um ein Höchstmaß an kontinuierlichem Schutz zu gewährleisten.



# BENUTZERFREUNDLICHE KOMMUNIKATION

## **Umgehen Sie Schatten-IT und erhöhen Sie die Anwenderakzeptanz**

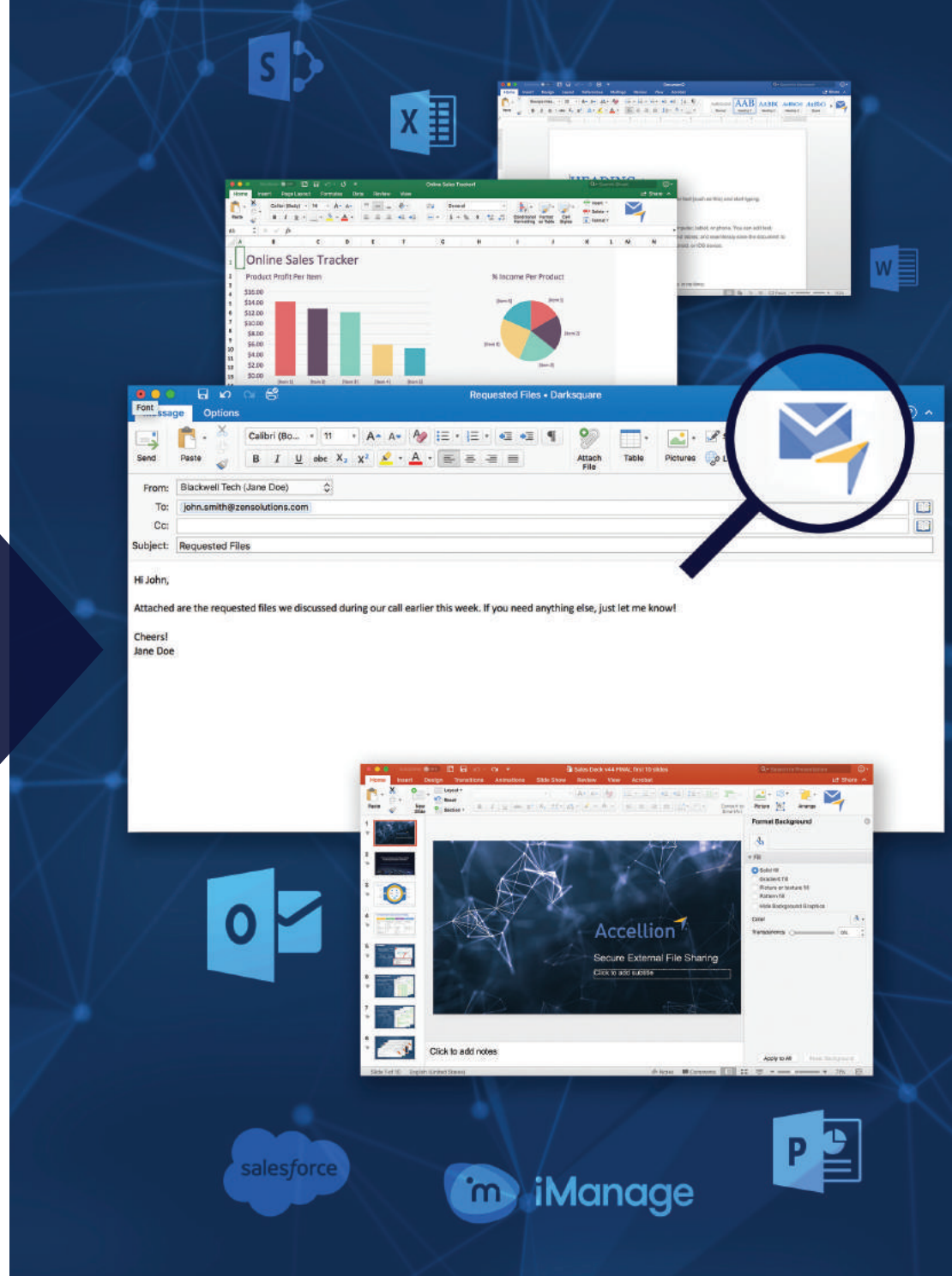
Die Enterprise Content Firewall von Accellion erlaubt es Millionen von Fachleuten, ihre Aufgaben zu erledigen, und gleichzeitig die Unternehmensinformationen zu schützen. Wenn Benutzer in einer E-Mail-, Web-, Mobil-, Büro- oder Unternehmensanwendung auf das Accellion-Logo klicken, können sie sich darauf verlassen, dass dies der sicherste Weg ist, vertrauliche Informationen mit der Außenwelt zu teilen.

### **Sicherer Austausch von Dateien mit Plugins**

Ermöglichen Sie Ihren Mitarbeitern, sensible Dokumente aus den Anwendungen, die sie tagtäglich nutzen, sicher zu teilen. Die Accellion-Plattform bietet einfache Plugins für Microsoft Office-Anwendungen, einschließlich Word, Excel, PowerPoint und Outlook, sowie für Unternehmensanwendungen, einschließlich Salesforce, iManage und SharePoint. Während Sie mit diesen Produkten arbeiten, setzt Accellion Ihre IT-Sicherheits- und Datenschutzrichtlinien durch, führt DLP- und ATP-Scans bei Datei-Downloads und -Uploads durch und erstellt einen detaillierten Audit-Trail.

### **Unterbinden Sie private E-Mail-Kommunikation**

CISOs haben ein großes Interesse daran, es Mitarbeitern so einfach wie möglich zu machen, sicher und effizient zu arbeiten. Die Accellion-Plattform bietet ein benutzerfreundliches Microsoft Outlook-Plugin, einen Web-Client und eine mobile Anwendung, die es Benutzern einfach machen, passwortgeschützte E-Mails und sichere E-Mail-Anhänge jeder Größe und jedes Formats von jedem Ort und Gerät aus zu teilen, mit unternehmensgerechter Verschlüsselung während der Übertragung und im ruhenden Zustand. Flexible Kontrollen, detaillierte Auditprotokolle und ein CISO-Dashboard helfen Ihnen bei der Verwaltung der Compliance auf Benutzer- und Admin-Ebene.





### **Sichere gemeinsame Ordner**

Die sicheren Freigabe-Ordner von Accellion ermöglichen einfache Online-Zusammenarbeit und erhöhen gleichzeitig die Datensicherheit, Compliance und Governance. Bieten Sie Anwendern die gleiche einfache Anwendung, die sie von Consumer-File-Sharing-Apps kennen, während Sie die Möglichkeit haben, den Zugriff zu sperren, granulare Berechtigungen durchzusetzen und gleichzeitig die Einhaltung gesetzlicher Vorgaben bei voller Transparenz zu erreichen.

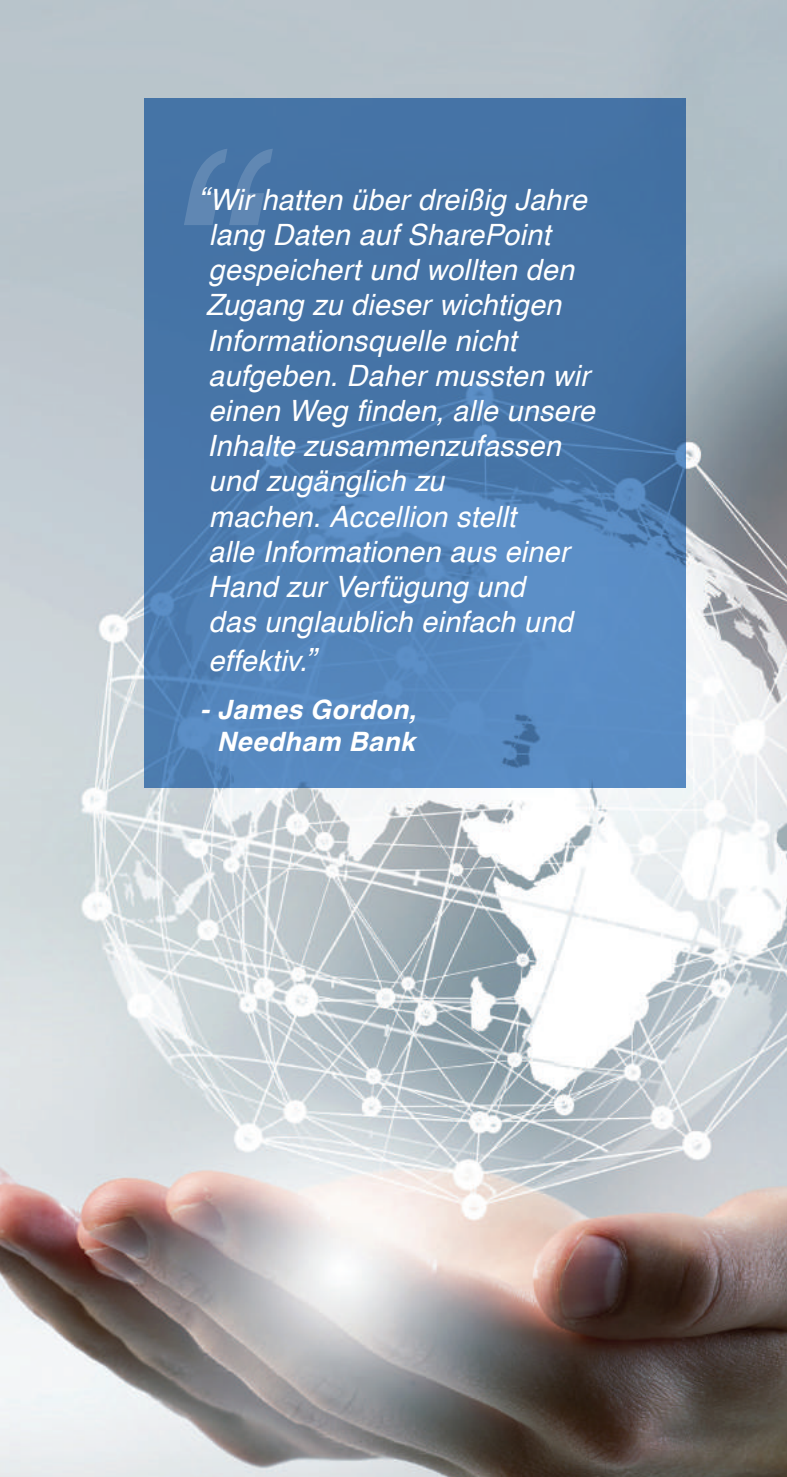
### **Sorgen Sie dafür, dass mobile Mitarbeiter sicher und produktiv arbeiten**

Viel beschäftigte Außendienstmitarbeiter sollten beim Thema Effizienz keine Kompromisse in puncto Sicherheit eingehen. Mit den mobilen Apps von Accellion für iOS und Android können Mitarbeiter auf Geschäftsreisen produktiv und sicher arbeiten. Die Accellion-Plattform bietet einen sicheren und einfachen Zugriff auf Inhalte, sodass Benutzer die Inhalte, die sie benötigen, schnell finden, leicht überprüfen und bearbeiten und diese sicher und absolut gesetzeskonform weitergeben können. Sollte ein mobiles Gerät verloren gehen oder gestohlen werden oder ein Mitarbeiter das Unternehmen verlassen, können alle sensiblen Daten, die sich in einem von Accellion gesicherten Container befinden, mittels Remote Wipe gelöscht werden.

*“Der rasante Anstieg der Anwenderakzeptanz ist ein direktes Resultat des Outlook-Plugins. Die Akzeptanz ist höher, weil es wie eine E-Mail aussieht und sich auch so verhält. Der Komfort für die Mitarbeiter ist enorm.”*

**- Soma Bhaduri, NYC Health + Hospitals**





*“Wir hatten über dreißig Jahre lang Daten auf SharePoint gespeichert und wollten den Zugang zu dieser wichtigen Informationsquelle nicht aufgeben. Daher mussten wir einen Weg finden, alle unsere Inhalte zusammenzufassen und zugänglich zu machen. Accellion stellt alle Informationen aus einer Hand zur Verfügung und das unglaublich einfach und effektiv.”*

**- James Gordon,  
Needham Bank**

## FLEXIBLE BEREITSTELLUNG

### **Individuell anpassbar an Ihre spezifischen Bedürfnisse**

Die Enterprise Content Firewall von Accellion bietet robuste Integrations-, Automatisierungs- und Bereitstellungsoptionen, um Ihre spezifischen Anforderungen an Sicherheit, Geschäftsprozesse und IT-Infrastruktur zu erfüllen. Die Flexibilität der Accellion-Plattform gewährleistet eine komplette, kostengünstige Lösung, die sich nahtlos in Ihre aktuelle Umgebung einfügt.

### **Einheitlicher Zugriff auf Inhalte ohne Migration**

Die Accellion-Plattform bietet Mitarbeitern in Unternehmen eine einzige, sichere Zugriffsquelle auf die Inhalte, die im Unternehmen gespeichert sind, unabhängig davon, ob sie lokal oder in der Cloud liegen. Mit Schnittstellen für Netzwerk-Dateifreigaben und ECM-Systeme wie SharePoint und OpenText sowie Cloud-Speicherlösungen wie OneDrive, Box und SharePoint Online vermeiden Unternehmen kostspielige und riskante Content-Migrationen. Darüber hinaus ermöglichen REST-APIs die Integration in bestehende Unternehmenssysteme. Alle Inhalte, unabhängig davon, wo sie gespeichert sind, sind jederzeit verfügbar - von jedem Ort, über jedes Gerät - ohne VPN. Da Inhalte über eine einzige Benutzeroberfläche leicht zugänglich sind, sind die Mitarbeiter von Unternehmen produktiver beim Auffinden und Teilen von Dateien.

### **Bereitstellungsoptionen, die Ihren individuellen Sicherheitsbedürfnissen entsprechen**

Weil Ihr Unternehmen einzigartige Sicherheitsanforderungen hat, bietet die Accellion-Plattform flexible, skalierbare Bereitstellungsoptionen, die das richtige Gleichgewicht zwischen Datenschutz, Compliance, Skalierbarkeit und Kosten schaffen. Mit einer On-Premise-Bereitstellung erreichen Sie vollständigen Datenschutz und Sicherheit. Senken Sie Kosten und erhöhen Sie die Sicherheit mit einer hybriden Cloud-Bereitstellung, bei der Sie die Verschlüsselungscodes besitzen. Vermeiden Sie die Vermischung von Daten mit einer privaten Cloud-Bereitstellung oder lagern Sie das Hosting an Accellion mit einer dedizierten, isolierten, von FedRAMP autorisierten Bereitstellung aus.

### **Automatisieren Sie Dateiübertragungen**

Sparen Sie Zeit, reduzieren Sie Fehler und verbessern Sie die Compliance mit einem zuverlässigen unternehmensgerechten Workflow-Automatisierungs-Toolkit. Wählen Sie aus drei flexiblen Ansätzen für das automatisierte Senden und Empfangen sowie die Verteilung von Unternehmensinhalten: SFTP zur Skalierung und Konsolidierung von Servern und Systemen und zur Reduzierung der Verwaltungskosten; konfigurierbare, codefreie Automation Agents für gesetzeskonforme Dateiübertragungen; leistungsstarke, flexible REST-APIs ermöglichen es Ihnen, inhaltsfähige Anwendungen und Integrationen zu erstellen.

Unabhängig davon, welchen Ansatz Sie wählen, die Workflow-Automatisierung mit Accellion unterstützt CISOs dabei, die Einhaltung gesetzlicher Vorgaben und Sicherheit zu gewährleisten, während gleichzeitig manuelle Prozesse im Unternehmen eliminiert werden.



# FEATURE HIGHLIGHTS



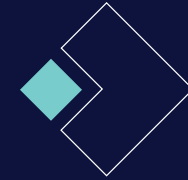
## VOLLKOMMENE TRANSPARENZ



## ZERO-TRUST-SICHERHEIT



## BENUTZERFREUNDLICHE KOMMUNIKATION



## FLEXIBLE BEREITSTELLUNG

### Sicherheits-Analysen

- CISO-Dashboard
- Überblick über alle im Unternehmen ein- und ausgehenden Dateien
- Warnmeldungen auf Grundlage maschinellen Lernens
- Benutzerdefinierte und geplante Berichte
- Splunk- und SIEM-Integrationen
- Transaktions-Filter und Aufschlüsselung nach Absender, Empfänger, Ort, Dateityp, etc.

### Compliance

- Detaillierte Compliance-Berichte mit nur einem Klick
- Konform mit gesetzlichen Vorgaben wie DSGVO, HIPAA, FIPS, SOC2, NIST 800-171, ITAR und FedRAMP.

### Governance-Kontrollen

- Detaillierte Richtlinienkontrollen und Berechtigungen für den Datenschutz
- Authentifizierungsrichtlinien basierend auf Rolle und Standort
- Dynamische Richtlinien-Automatisierung basierend auf der Klassifizierung von Daten und weiteren Faktoren
- Standardwerte für die minimalste Berechtigung
- Dynamische Quarantäne
- Gehärtete virtuelle Appliance
- Kein Zugriff des Anbieters auf Inhalte oder Metadaten
- Datenhoheit

### Sicherheits-Framework

- Gehärtete virtuelle Appliance
- Verschlüsselung während der Übertragung (TLS 1.2) und im ruhenden Zustand (AES-256)
- Alleiniger Zugriff auf Verschlüsselungscodes
- Integriertes AV and native 2FA
- SMS Passcode-Authentifizierung
- Integration mit SSO, LDAP/AD, DLP, ATP, SIEM, MDM, MFA/2FA und HSM

### Accellion Funktionen

- Sichere E-Mail-Kommunikation
- Sichere Web-Ordner mit der gleichen Benutzerfreundlichkeit wie bei Consumer-File-Sharing-Apps
- Sichere Zusammenarbeit, Vorstandskommunikation und virtuelle Datenräume
- Spezielle mobile Anwendungen für iOS und Android
- SFTP und Managed File Transfer
- Sichere Online-Formulare
- Unbegrenzte Dateigrößen

### Enterprise-App-Sharing-Plugins

- Sichere Plugins für Microsoft Office und MS Office 365 für Outlook, Word, Excel und PowerPoint
- Sichere Plugins für Google Docs und Google Drive
- Enterprise-Plugins für Salesforce, iManage und SharePoint

### Zugriff auf Inhalte

- Einheitlicher Zugriff auf ECMs und Dateifreigaben ohne VPN
- Einheitlicher Zugriff auf Cloud-Speichersysteme wie Box, Dropbox, OneDrive und Google Drive
- Keine Migration von Inhalten

### Benutzerspezifische Automatisierung

- Automatisierte, code-freie und sichere Dateiübertragungen
- Konsolidiertes Self-Service-SFTP
- Umfangreiche REST API
- Sicheres Mail-Gateway

### Bereitstellung

- On-premise, Private Cloud-, Hybrid Cloud- oder FedRAMP-Bereitstellungsoptionen
- Cluster für den globalen Einsatz und High Availability

# Accellion<sup>™</sup>

Die Enterprise Content Firewall von Accellion verhindert Datenschutzverletzungen und Compliance-Verstöße, die durch die Kommunikation mit Dritten und damit verbundene Risiken entstehen. Mit Accellion haben CIOs und CISOs die vollständige Transparenz, Compliance und Kontrolle über den Austausch von geistigem Eigentum, personenbezogenen Daten, Patienteninformationen und anderen sensiblen Inhalten über alle Kommunikationskanäle von Drittanbietern hinweg, einschließlich E-Mail, Dateifreigabe, Mobilgeräte, Business Applikationen, Webportale, SFTP und automatisierte geschäftsübergreifende Workflows.

Accellion-Lösungen schützen mehr als 25 Millionen Endbenutzer in mehr als 3.000 Unternehmen und Regierungsbehörden weltweit, darunter KPMG, Latham & Watkins, Linde Gas, NHS, das National Institute for Standards and Technology (NIST) sowie Pfizer und die Paul Hartmann AG.

[www.accellion.com](http://www.accellion.com) | [sales@accellion.com](mailto:sales@accellion.com)

© 2019 ACCELLION. Alle Rechte vorbehalten.

#### Accellion USA, LLC

1804 Embarcadero Road, Palo Alto, CA 94303

**Telefon:** +1 650 485 4300

#### EMEA Headquarters

Löwen-Markt 5, 70499 Stuttgart, Germany

**Telefon:** +49 711 252861 0

#### APAC Headquarters

Blk 750A Chai Chee Rd #08-01B

Viva Business Park, Singapore 469001

**Telefon:** +65 62445670

