App-Müdigkeit und Kluft zwischen Zusammenarbeit und Sicherheit überwinden

Wire Cells revolutioniert die Arbeitsweise in Organisationen mit sicherer und nahtloser Kommunikation und Zusammenarbeit.
Januar 2025

Zusammenfassung für Führungskräfte

Heutige Organisationen priorisieren zunehmend Sicherheit, Datenschutz und Effizienz in all ihren Tätigkeiten. Doch wenn es um Kommunikationstools geht, können diese Prioritäten zur Herausforderung werden. Während es spezialisierte Tools für sichere Nachrichtenübermittlung und Dokumentenverwaltung gibt, existieren kaum Plattformen, die eine vollständige, integrierte Lösung bieten, die sicher und gleichzeitig so einfach zu bedienen ist, dass Teams sie tatsächlich annehmen.

Diese Ausbreitung von Plattformen mit nur einer Nutzung oder, schlimmer noch, mit Überschneidungen wird als Plattform-Müdigkeit bezeichnet. In Kombination mit dem damit verbundenen Benutzer-Problem, der sogenannten App-Müdigkeit, stellt dies ein wachsendes Problem für moderne Organisationen dar.

Die durchschnittliche Anzahl an Apps in Unternehmen stieg von 843 im Jahr 2021 auf 1.061 im Jahr 2023.

Quelle: Customer Data Platform Institute, 2024

Ein großes Problem ist die Belastung, die es auf die betriebliche Effizienz und die finanziellen Ressourcen von Unternehmen ausübt. Mit der Zunahme von Plattformen wird deren Verwaltung immer komplexer. Dies führt oft zu doppelten Funktionen, inkonsistenten Datenflüssen und fragmentierten Nutzererfahrungen. Es beeinträchtigt die Produktivität, verursacht doppelte Arbeit, erhöht die menschliche Fehleranfälligkeit und schafft zusätzliche Sicherheitsprobleme.

Dieses Whitepaper zeigt, wie die neue Wire-Cells-Lösung die sicheren Kommunikationsfunktionen von Wire mit der leistungsstarken, intuitiven und sicherheitsbewussten Cells-Plattform für Dokumentenmanagement kombiniert, um den Mitarbeitern ein sicheres Arbeiten zu ermöglichen.

Die Herausforderung: Produktivität & Sicherheit müssen Hand in Hand gehen

“Mitarbeiter werden revoltieren, sei es aufgrund zu vieler Apps oder Plattformen für dieselbe Funktion. Zu viele unterschiedliche Anwendungen und Plattformen können Zeit verschwenden, die Produktivität beeinträchtigen und ein schlechtes Erlebnis liefern, sagte Nadir Ali. Mitarbeiter großer Unternehmen haben möglicherweise zehn oder mehr arbeitsbezogene Apps, jede mit einer anderen Benutzeroberfläche und Betriebscharakteristik. Allein die gewünschte App zu finden, kann mühsam sein, und das Wechseln zwischen Apps unterbricht den Arbeitsfluss.”

Nadir Ali, CEO of Inpixon via SHRM blog

Sicherheitsverletzungen, Datenschutzbestimmungen und Cyber-Bedrohungen haben es für Organisationen essenziell gemacht, Tools einzusetzen, die sowohl Kommunikation als auch Dateifreigabe absichern. Doch bisher gab es keine benutzerfreundlichen Lösungen, die ein sicheres Arbeiten für Organisationen, ihre Partner und sogar Kunden bieten.

Hier sind einige der wichtigsten Herausforderungen, die die Notwendigkeit einer einheitlichen Lösung vorantreiben, die sowohl Kommunikation als auch Dokumentenfreigabe kombiniert:

Vier zentrale Herausforderungen: Sicherheit und Benutzerfreundlichkeit im Gleichgewicht halten

1 - Datenverstöße
Wir alle haben uns daran gewöhnt, da sie täglich in den Nachrichten vorkommen. Doch im Jahr 2023 wurden rekordverdächtige 3.205 Datenschutzverletzungen gemeldet, was einen Anstieg von 78% im Vergleich zum Vorjahr darstellt. Die Gesamtzahl der betroffenen Personen erreichte 353 Millionen. Hauptursachen dieser Verstöße waren Cyberangriffe, Schwachstellen in der Lieferkette sowie Fehler in menschlichen oder systematischen Prozessen. Dieser Trend setzte sich 2024 fort, mit bemerkenswerten Verstößen in Sektoren wie Gesundheitswesen und Finanzen.
Quelle: ITRC - Identity Theft Resource Center

2 - Compliance
Die Einhaltung strenger Datenschutzvorschriften wie DSGVO, HIPAA und CCPA ist in Sektoren wie Gesundheitswesen, Finanzen und Recht entscheidend und eine weitere große Herausforderung bei der Entwicklung eines beruflichen Toolsets, das sowohl benutzerfreundlich als auch sicher ist.

Dies gilt insbesondere jetzt, wo die Kosten für die Nichteinhaltung der Vorschriften in die Höhe schnellen. Laut einem Bericht von DLA Piper stiegen die DSGVO-Bußgelder 2022 um 168%, wobei einzelne Strafen bis zu 4% des jährlichen weltweiten Umsatzes oder 20 Millionen Euro betrugen, je nachdem, welcher Betrag höher ist. Gleichzeitig können Verstöße gegen HIPAA zu Bußgeldern von bis zu 50.000 US-Dollar pro Verstoß führen und ein einziger Verstoß kann mehrere Verstöße umfassen. CCPA-Bußgelder können bis zu 7.500 US-Dollar pro absichtlichem Verstoß erreichen. Darüber hinaus ermöglicht das Gesetz private Klagen bei Datenschutzverletzungen, was die potenziellen Kosten exponentiell erhöht – ganz zu schweigen von schwer zu reparierendem Imageschaden. Es zahlt sich eindeutig nicht aus, die Bedeutung von Datenschutzfragen zu ignorieren oder zu minimieren.

3 - Fragmentierte Arbeitsabläufe
App-Müdigkeit ist ein reales Problem. Wie oben erwähnt, stieg die durchschnittliche Anzahl an Apps in Unternehmen von 843 im Jahr 2021 auf 1.061 im Jahr 2023. Das sind viele Schnittstellen, die erlernt werden müssen, viele Wechsel und viele Gründe, außerhalb des genehmigten Toolsets nach einer einfacheren und oftmals weniger sicheren Lösung zu suchen. Es ist keine Überraschung, dass Studien gezeigt haben, dass die Nutzung mehrerer, nicht integrierter Tools zu Ineffizienzen und Sicherheitslücken führen kann.

Laut Qatalog und Cornell University dauert es fast 9,5 Minuten, bis Mitarbeiter nach einem Wechsel der Anwendungen wieder fokussiert arbeiten können. 45% der Mitarbeiter geben an, dass diese Wechsel sie weniger produktiv machen und zu mentaler Ermüdung führen. Eine Untersuchung von Slack aus dem Jahr 2023 ergab sogar, dass exzessives App-Wechseln pro Mitarbeiter jährlich bis zu zehn Wochen Produktivität kosten kann.

4 - Schatten-IT
Die schmerzhafte Realität ist, dass die langsame Akzeptanz komplexer Plattformen ein Fakt ist. Selbst die sichersten Plattformen werden nicht das gewünschte Ergebnis liefern, wenn Ihre Mitarbeiter diese aktiv meiden und inoffizielle Plattformen nutzen, um ihre Arbeit schneller zu erledigen. Dieses Phänomen wird als Schatten-IT bezeichnet.

Eine Studie von IBM, die von der Cybersicherheits-Expertin SC Media zitiert wurde, ergab, dass 33% der Mitarbeiter von Fortune 1000, die 1000 umsatzstärksten amerikanischen Unternehmen, regelmäßig Unternehmensdaten mithilfe ungesicherter Drittanbieter-Apps speichern und teilen, um ihre Arbeitsprozesse zu verbessern. Forschungen von Gartner zeigen, dass 83% der Organisationen erlebt haben, wie Mitarbeiter nicht genehmigte Apps verwenden, wobei im Durchschnitt 75 nicht autorisierte Cloud-Dienste pro Organisation im Einsatz sind. Laut Next Cloud haben 67% der Teams ihre eigenen Kommunikationstools in eine Organisation eingeführt, und 82% der Teams haben gegenüber der IT-Abteilung oder dem Management Einwände darüber erhoben, welche Tools verwendet werden sollten.

Einfaches und intuitives Design ist nicht nur wünschenswert – es ist entscheidend für den Erfolg digitaler Produkte. Laut Spezialisten für digitale Adaption, Whatfix, bleiben 80% der Produktfunktionen ungenutzt, weil Benutzer mit komplexen Oberflächen zu kämpfen haben. Benutzerfreundlichkeit ist von entscheidender Bedeutung, wird jedoch oft zugunsten von Sicherheit geopfert.

Verbesserung von Sicherheit und Benutzerfreundlichkeit mit Wire Cells
Die neue integrierte Wire-Cells-Plattform stellt eine bedeutende Weiterentwicklung im Markt für sichere Arbeitsbereiche dar. Schauen wir uns genauer an, wie Wire Cells Organisationen dabei helfen kann, Arbeitsabläufe zu optimieren und gleichzeitig Ende-zu-Ende-Sicherheit, Compliance und Benutzerfreundlichkeit sowohl für die Kommunikations als auch für Dateifreigaben zu gewährleisten.

Übersicht über Wire und Pydio

Die Natur der modernen Arbeit ist Kommunikation, sowohl gesprochen als auch geschrieben. Ein Großteil dieser Arbeit findet in Besprechungen, E-Mails, Chats sowie in der Erstellung, Freigabe und Zusammenarbeit an Dokumenten aller Art statt. Daher die Vielzahl an Produktivitäts- und Workspace-Lösungen.

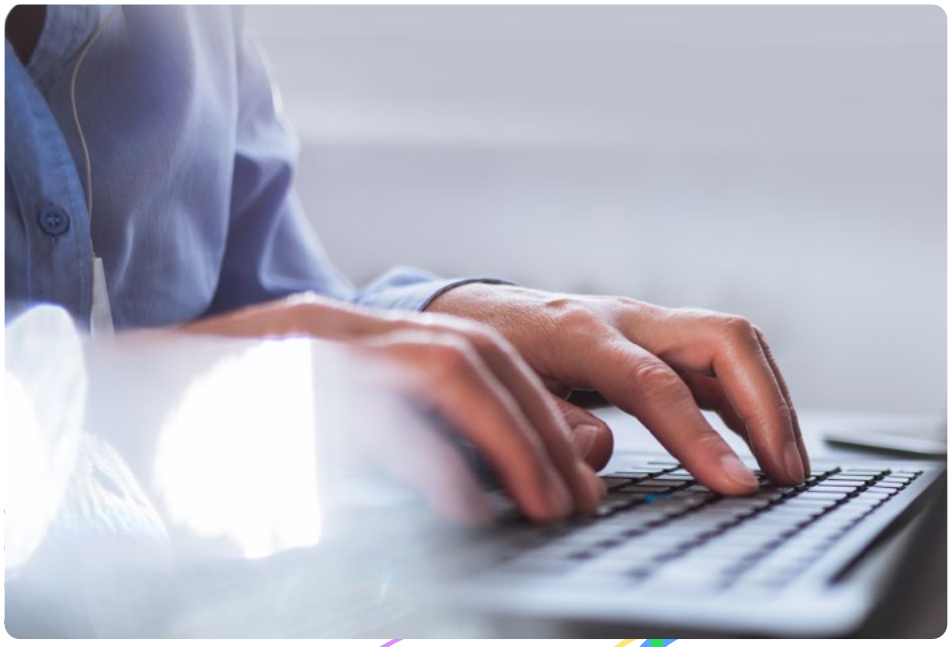
Doch die derzeit verfügbaren Plattformen bieten keine Lösung, die alle Funktionen und die Benutzerfreundlichkeit umfasst, die der moderne Arbeitnehmer benötigt, um effektiv zu arbeiten, und gleichzeitig den strengen Sicherheitsansatz, den CISOs suchen, sowie die Privatsphäre und Transparenz, die Compliance-Abteilungen verlangen. Diese Lücke füllt die Entwicklung der integrierten Wire (sichere Kommunikation) + Cells-Plattform (sichere Dokumentenfreigabe und -zusammenarbeit). Die Lösung beider Probleme macht Wire Cells zur herausragenden Lösung auf dem Markt für sichere Workspaces.

Zuerst werfen wir einen Blick auf die Komponenten-Systeme.

Wire: Plattform für sichere Kommunikation
Wire bietet Echtzeit-Zusammenarbeit mit verschlüsselter Nachrichtenübermittlung, Sprach- und Videoanrufen sowie Dateifreigabe und wurde entwickelt, um Sicherheit und Datenschutz zu priorisieren. Wire bietet Ende-zu-Ende-Verschlüsselung in großem Umfang für alle Chats, Anrufe, Videokonferenzen und Dateifreigaben. Die Apps wurden so konzipiert, dass sie die strengsten globalen Datenschutzbestimmungen einhalten, basierend auf einem transparenten und überprüfbaren Open-Source-Kern.

Kernfunktionen:

- Branchenführende Sicherheit, die für Benutzer unsichtbar ist
- Ende-zu-Ende-Verschlüsselung für alle Nachrichten, Anrufe, Dateien, Reaktionen, Sprachnachrichten, Videos, Bildschirmfreigaben und mehr
- Gruppenunterhaltungen und sichere Telefon- und Videokonferenzen
- Plattformübergreifend: verfügbar auf Mobilgeräten, Desktop und im Webbrowser
- DSGVO- und CCPA-konform
- Verfügbar über Wire Cloud oder selbstgehostete Optionen für volle Datenhoheit
- Einfache Gäste-Funktionen für sichere Zusammenarbeit mit externen Beteiligten, keine Kontoanmeldung oder App-Downloads erforderlich



Cells: Sichere Dateifreigabe, Zusammenarbeit und Verwaltung

Pydio ist eine Plattform für Dateifreigabe, Zusammenarbeit und Verwaltung. Sie ermöglicht Organisationen, ihre eigene private Dateispeicherinfrastruktur zu hosten und die volle Kontrolle über ihre Daten zu behalten. Pydio integriert fortschrittliche Sicherheitsfunktionen wie Verschlüsselung, Zugriffssteuerung und Prüfprotokolle und ist somit eine vertrauenswürdige Lösung für Organisationen, die sensible Informationen schützen müssen.

Kernfunktionen:

- → Selbstgehostete On-Premises- oder Private-Cloud-Infrastruktur für Dateispeicherung, -freigabe und -verwaltung
- → Verschlüsselung von Dateien ist dynamisch, fließend und für Benutzer unsichtbar, ähnlich wie bei der Wire-Messaging-Verschlüsselung mit MLS
- → Granulare Berechtigungen und Zugriffskontrollen für Dateien und Ordner
- → Verschlüsselung von Dateien sowohl während der Übertragung als auch im Ruhezustand
- → Tools wie Versionskontrolle, Kommentarfunktionen und Dateisperren
- → Einhaltung von Datenschutzvorschriften wie der DSGVO
- → Plattformübergreifend: verfügbar auf Mobilgeräten, Desktop und im Webbrowser
- → Automatisierung und Erstellung von Workflows sowie Integration in Quellsysteme.

Wire + Cells setzen neue Maßstäbe für Workspace-Lösungen

Kommen wir direkt auf den Punkt. Es gibt einen einfachen, ziemlich offensichtlichen Grund, warum die Kombination von Wire und Cells zu einer nahtlosen Lösung einen bedeutenden Fortschritt darstellt. Mit der kombinierten Lösung erledigen Mitarbeiter über 80% ihrer täglichen Aufgaben in einer einzigen, standardmäßig sicheren und einfachen Benutzeroberfläche – kein ständiges Wechseln zwischen Tools mehr, keine Produktivitätsverluste. Das kann keine andere Workspace-Plattform von sich behaupten.

Durch die Integration von Ende-zu-Ende-verschlüsselter Nachrichtenübermittlung und verschlüsseltem Dateimanagement ermöglicht Wire Cells Teams eine mühelose Zusammenarbeit, die Einhaltung von Vorschriften und den Schutz sensibler Daten – alles in einer flexiblen, skalierbaren Lösung. Wire Cells bietet Sicherheitsniveaus, die weit über das hinausgehen, was derzeit auf dem Markt verfügbar ist. Pydio und Wire, die unabhängig verwendet und kontinuierlich von Regierungen weltweit auditiert werden, sind führend in der Zusammenarbeit für Organisationen jeder Größe – ohne Kompromisse auf allen Ebenen. Die kombinierte Plattform repräsentiert eine Revolution in der Arbeitsplatztechnologie und liefert Lösungen für eine Vielzahl von Anwendungsfällen:

1. Einheitliches und sicheres System für Zusammenarbeit

Warum ist das wichtig?
Wir haben alle schon einmal an einer Videokonferenz teilgenommen, mussten ein Dokument aus unserem Dateisystem teilen und haben den Link dann in einer Messenger-App geteilt, damit er nicht verloren geht, wenn der Anruf beendet ist. Abgesehen von der Unannehmlichkeit und Zeitverschwendung sind die Sicherheits- und Datenschutzrisiken enorm. Selbst wenn Sie eine bequemere, einheitliche Produktivitätsplattform verwenden, gibt es viele Hinweise darauf, dass Ihre Daten weder vor anderen noch vor Ihrem Plattformanbieter sicher sind, der diese möglicherweise für das Training von KI-Modellen oder Schlimmeres nutzt.

Wie löst Wire Cells das Problem?
Die Kombination der sicheren Kommunikationsfunktionen von Wire mit dem sicheren Dateimanagement von Cells führt zu einer einheitlichen Workspace-Plattform, bei der die Sicherheit über alle Ebenen der Kommunikation und des Datenaustauschs hinweg gewährleistet ist:

- → Die Echtzeit-Kommunikations stellt sicher, dass Nachrichten, Anrufe und Videokonferenzen vollständig verschlüsselt und sicher sind
- → Das Datenmanagement sorgt für eine sichere Speicherung und Zugriffskontrolle für freigegebene und gemeinsam genutzte Dateien
- → Diese Kombination bedeutet, dass sowohl Kommunikation als auch Dateifreigabe in jeder Phase, von der Diskussion bis zum Dokumentenaustausch, verschlüsselt und geschützt sind

2. Verbesserte Datensicherheit und Kontrolle

Warum ist das wichtig?
Wenn Sie im Militär, in der Regierung, in der Strafverfolgung oder in einer Branche arbeiten, die hohen Wert auf Datenschutz, Sicherheit und Compliance legt, wie Finanzen, Gesundheitswesen oder Recht, schließt die Realität Ihrer Betriebsumgebung die Verwendung von Plattformen mit einer unseriösen Herangehensweise an Datensicherheit aus. Sie können es sich nicht leisten, Lösungen zu nutzen, bei denen Sie nicht die volle Kontrolle darüber haben, wie Ihre Daten übertragen, gespeichert, freigegeben oder verarbeitet werden. Wire Cells ist die sichere Lösung.

Wie löst Wire Cells das Problem?

- → Die Self-Hosting-Fähigkeit von Pydio für Dateispeicherung stellt sicher, dass sensible Informationen nicht auf Servern Dritter gespeichert werden. Das bedeutet, dass Sie Datenhoheit und Datenschutz sicherstellen können. Gleichzeitig bietet die On-Premises-Hosting-Option von Wire ähnliche Kontrolle über die Echtzeit-Kommunikation
- → Die Ende-zu-Ende-Verschlüsselung von Wire stellt sicher, dass alle Diskussionen, sei es in Text- oder Sprachform, privat bleiben
- → Die acht Schutzebenen von Pydios Zugriffskontrolllisten (ACL) und die Verschlüsselung stellen sicher, dass Dateien vor unbefugtem Zugriff geschützt sind, selbst wenn sie über Teams hinweg geteilt werden
- → In Branchen wie Gesundheitswesen, Recht, Finanzen und Regierung stellt diese doppelschichtige Sicherheit die Einhaltung von Datenschutzgesetzen wie HIPAA, DSGVO und CCPA sicher

3. Optimierte Workflows

Warum ist das wichtig?
Wie in der Einleitung dieses Whitepapers erwähnt, belasten App-Müdigkeit und der ständige Wechsel zwischen verschiedenen Oberflächen die Produktivität in den meisten modernen Organisationen erheblich. Wir ersparen Ihnen an dieser Stelle weitere Statistiken und Studien, um diese These zu untermauern – die meisten von uns kennen den Verlust von Fokus, Zeit und Energie, der durch den Einsatz zu vieler Tools für alltägliche Aufgaben entsteht, nur allzu gut. Aber eine Statistik aus der bereits zitierten Qatalog/Cornell-Studie sei dennoch erwähnt: Die Zunahme von Softwaretools am typischen Arbeitsplatz untergräbt den fairen Zugang zu Informationen. 54% der Befragten sagen, dass Anwendungen es manchmal erschweren, Informationen zu finden.

Wie löst Wire Cells das Problem?
Durch die Integration von Wire und Pydio in einen einzigen Workflow entfällt die Notwendigkeit, zwischen Plattformen für Kommunikation und Dateifreigabe zu wechseln. Teams können sicher kommunizieren und nahtlos an Dateien zusammenarbeiten.

Beispiel für einen Workflow:

- → **Diskussion:** Mitarbeiter besprechen Projekt-Updates über verschlüsselte Nachrichten
- → **Dateifreigabe:** Sobald die Dateien bereit sind, teilt ein Team-Mitglied die erforderlichen Dokumente. Dabei bleiben alle sensiblen Inhalte verschlüsselt und sind nur für autorisierte Personen zugänglich
- → **Zusammenarbeit:** Mitarbeiter können Dateien kommentieren, bearbeiten oder sperren, während sie weiterhin ihre Änderungen diskutieren
- → **Audit und Compliance als Bonus:** Die einheitliche Plattform führt ein Prüfprotokoll der Dateizugriffe, um die Einhaltung von Vorschriften sicherzustellen, und protokolliert Metadaten zu Kommunikationszwecken – selbstverständlich alles verschlüsselt und gesichert

4. Datenschutzorientierte Zusammenarbeit

Warum ist das wichtig?
Datenschutz in der Kommunikation ist für Regierungsorganisationen und Unternehmen unerlässlich, da er sensible Daten und die nationale Sicherheit schützt, die Einhaltung gesetzlicher Vorschriften gewährleistet und das öffentliche Vertrauen stärkt. Sichere Kommunikationskanäle verhindern Datenpannen, die zu finanziellen Verlusten, rechtlichen Problemen und Reputationsschäden führen können. Der Schutz der Kommunikation ist entscheidend für die Betriebssicherheit, das Risikomanagement und die Stabilität in Regierung und Unternehmen.

Wie löst Wire Cells das Problem?
Die ursprünglichen Plattformen Wire und Pydio zeichnen sich durch eine starke datenschutzorientierte Basis aus. Sie sind open source, sodass Organisationen ihre Sicherheit durch unabhängige Prüfungen verifizieren können. Außerdem ermöglichen beide Plattformen die Einhaltung der DSGVO, wodurch selbst die strengsten Anforderungen an den Datenschutz erfüllt werden. Diese datenschutzorientierten Grundlagen werden in die neue einheitliche Plattform übernommen.

- → Es werden keine Kommunikationsmetadaten auf Servern gespeichert. Dies gewährleistet den Datenschutz über den Inhalt von Nachrichten und Anrufen hinaus
- → Organisationen können ihren eigenen Speicher hosten und so kontrollieren, wo die Daten gespeichert werden und wer darauf zugreifen darf

Diese Kombination bietet ein Umfeld, in dem Organisationen sicher sein können, dass sowohl ihre Kommunikation als auch ihre Dateien vor Überwachung und unbefugtem Zugriff geschützt sind.

Das Beste daran: Die Sicherheit ist für die Benutzer nahezu unsichtbar. Sie können sich auf ihre Arbeit konzentrieren, ohne sich Gedanken über komplexe Sicherheitsverfahren oder ständige Wechsel zwischen Tools machen zu müssen.

5. Sichere Zusammenarbeit mit Externen

Warum ist das wichtig?
Wenn Ihre Produktivitätsplattform das Hinzufügen von Gästen zulässt, jedoch keine private und sichere Verbindung gewährleistet, ist dies ein größeres Problem, als wenn keine Gastverbindungen erlaubt wären. Werden Dokumente und Kommunikationsdaten unangemessen geteilt oder – noch schlimmer – durch die Zusammenarbeit mit einem Partner kompromittiert, sind die Folgen genauso gravierend wie bei einem internen Datenleck.

Wie löst Wire Cells das Problem?
Wire Cells ermöglicht nicht nur eine sichere Zusammenarbeit innerhalb einer Organisation, sondern auch mit externen Partnern oder Stakeholdern. Der Gastzugang von Wire bietet eine temporäre, sichere Kommunikation für Dritte, während die granulare Rechtevergabe von Cells eine kontrollierte Dateifreigabe mit externen Partnern erlaubt. Durch die Nutzung einer einheitlichen Plattform wird zudem das Risiko menschlicher Fehler und damit verbundener Datenlecks deutlich reduziert.

Beispiel:
Eine Anwaltskanzlei kann Wire für die sichere Kommunikation zwischen Mandanten und Anwälten nutzen und gleichzeitig Fallakten über die virtuellen Datenräume von Cells mit Mandanten teilen. So bleiben alle Interaktionen verschlüsselt und entsprechen den Datenschutzvorschriften.

Anwendungsfälle für die Integration von Wire und Pydio

1. Gesundheitswesen

Herausforderung: Gesundheitsfachkräfte wie Ärzte, Pflegekräfte und Verwaltungspersonal müssen sich bei der Patientenversorgung koordinieren. Dies erfordert oft den Austausch sensibler Informationen (PII) wie Krankengeschichten, Bilddateien und Behandlungspläne. Die Kommunikation über reguläre Kanäle wie E-Mails oder Verbraucher-Messaging-Apps birgt jedoch das Risiko von Verstößen gegen HIPAA-Standards, was die Privatsphäre der Patienten und die Compliance der Organisation gefährdet. Diese Herausforderung wird noch größer, wenn Spezialisten oder andere Einrichtungen auf Patientendaten zugreifen oder sich zu einem Fall beraten müssen, da dies zusätzliche Sicherheitsanforderungen und Hürden beim Datenaustausch mit sich bringt.

Lösung: Wire Cells bietet eine All-in-One-Plattform, die speziell für sichere Kommunikation im Gesundheitswesen entwickelt wurde. Mit Ende-zu-Ende-Verschlüsselung für Nachrichten und Videokonsultationen können Ärzte Fälle sicher diskutieren, Einblicke teilen und Echtzeit-Unterstützung leisten, ohne das Risiko eines unbefugten Zugriffs. Darüber hinaus stellt der rollenbasierte Zugriff von Wire Cells sicher, dass nur autorisiertes Personal bestimmte Dateien einsehen oder bearbeiten kann, wodurch eine einfache Zusammenarbeit bei gleichzeitiger strikter Zugangskontrolle ermöglicht wird.

2. Finanzdienstleistungen

Herausforderung: Finanzinstitute verwalten hochsensible Kundeninformationen, darunter Anlageportfolios, persönliche Finanzberichte, Verträge und regulatorische Unterlagen. Berater und Finanzanalysten müssen sicher mit Kunden und Kollegen kommunizieren, um Strategien zu besprechen, Leistungen zu überprüfen und komplexe Transaktionen zu verwalten. Gleichzeitig stehen sie vor strengen Datenschutzvorschriften wie der DSGVO und CCPA, die eine strikte Kontrolle über den Umgang mit personenbezogenen Daten und den Zugriff darauf sowie Transparenz in den Datenmanagementpraktiken erfordern. Diese Compliance-Anforderungen machen es für Finanzinstitute entscheidend, Kundendaten vor unbefugtem Zugriff, Datenlecks und unbeabsichtigter Offenlegung zu schützen.

Lösung: Wire Cells bietet eine vollständige Work-space-Lösung für sichere Kommunikation und Dokument-enverwaltung innerhalb von Finanzinstituten sowie mit Kunden und Partnern. Wire Cells stellt Finanzinstituten die Werkzeuge zur Verfügung, die sie benötigen, um sicher zu kommunizieren, sensible Daten und die Privatsphäre zu schützen und die Einhaltung finanzieller und datenschutz-rechtlicher Vorschriften zu gewährleisten.

3. Kanzleien

Herausforderung: Anwälte und juristische Teams arbeiten mit hochsensiblen und vertraulichen Informationen, wie Fallakten, Verträgen und Schriftsätzen. Effektive Kommunikation mit Mandanten und sichere Zusammenarbeit an Dokumenten sind entscheidend, um Fälle effizient zu bearbeiten. Diese Interaktionen und Dateien enthalten oft Informationen, die strenge Zugriffskontrollen und umfassende Prüfprotokolle erfordern, um ethischen Verpflichtungen und regulatorischen Standards wie dem Verschwiegenheitspflicht gerecht zu werden. Standard-E-Mails und Tools zur Dateifreigabe bieten nicht die notwendige Sicherheit und gefährden vertrauliche Daten.

Lösung: Wire und Pydio bieten eine sichere, konforme Plattform für die Kommunikation zwischen Anwalt und Mandant sowie das Dokumentenmanagement – speziell auf die Bedürfnisse der Rechtsbranche zugeschnitten.

Funktionen in Aktion:

- → **Verschlüsselte Kommunikation zwischen Anwalt und Mandant:** Anwälte können sicher Nachrichten senden und Videokonsultationen durchführen, die alle Interaktionen schützen. Zum Beispiel kann ein Anwalt bei der Fallvorbereitung sensible Updates über einen sicheren Videoanruf mit einem Mandanten teilen und sicherstellen, dass Informationen privat bleiben und nicht abgefangen werden können.
- → **Sichere Dokumentenspeicherung und kontrollierte Zusammenarbeit:** Rollenbasierte Zugriffskontrollen und Prüfprotokolle ermöglichen es juristischen Teams, zusammen an Dokumenten zu arbeiten und sicherzustellen, dass nur autorisierte Mitarbeiter Dateien einsehen oder bearbeiten können.
- → **Einhaltung von Vertraulichkeitsanforderungen:** Verschlüsselte Kommunikation, Prüfprotokolle und sichere Dokumentenspeicherung helfen Kanzleien, die Anforderungen an den Umgang mit sensiblen juristischen Dokumenten zu erfüllen.

4. Regierung und Verteidigung

Herausforderung: Regierungsbehörden verwalten vertrauliche Informationen, von klassifizierten Dokumenten bis hin zu sensiblen Bürgerdaten, die oft mit nationaler Sicherheit, Strafverfolgung oder regulatorischen Angelegenheiten verbunden sind. Diese Behörden benötigen eine Möglichkeit, sicher intern zu kommunizieren, an Dokumenten zusammenzuarbeiten und Daten zwischen Abteilungen zu verwalten, während sie die strikte Kontrolle darüber behalten, wo und wie ihre Daten gespeichert werden. Zudem ist die Einhaltung von Richtlinien zur Datensouveränität und Sicherheitsstandards unerlässlich, da viele staatliche Vorschriften vorschreiben, dass Daten innerhalb der Infrastruktur der Behörde oder innerhalb nationaler Grenzen gespeichert werden müssen.

Lösung: Die integrierte Wire Cells-Lösung bietet verschlüsselte Nachrichten und Videokonferenzen für eine sichere interne Kommunikation und ermöglicht es Behörden, vertrauliche Dokumente auf ihrer eigenen Infrastruktur zu speichern und zu bearbeiten.

Fazit

Die integrierte Wire-Cells-Lösung schafft eine robuste, sichere Arbeitsumgebung, die wesentliche Herausforderungen, wie Plattform-Überlastung und App-Müdigkeit, für Organisationen und Branchen mit strengen Compliance- und Datenschutzanforderungen löst, darunter Gesundheitswesen, Recht, Finanzen und Regierung. Wire Cells ist eine zukunftssichere Lösung, die Sicherheit, Produktivität und Datensouveränität in Einklang bringt.

wire.com