Taming Platform Creep & Breaking Down the Collaboration/Security Divide

Wire Cells redefines the enterprise workspace with secure,seamless, simple-to-use communication and collaboration.
January 2025

Executive Summary

Today's organizations are increasingly prioritizing **security**, **privacy**, and **efficiency** in everything they do. But, when it comes to communications and collaboration tools, those priorities can become a challenge. While there are single-purpose tools for secure messaging and document management, sharing, and collaboration, there are few to no platforms that offer a complete, integrated workspace solution that is secure, private, and easy enough to use so that teams will actually adopt them.

This proliferation of single-usage (or even worse, overlapping) platforms has become known as **platform creep** and, combined with its related end-user problem, **app fatigue**, is becoming an important pain point for modern organizations.

The average number of apps in an enterprise grew from 843 in 2021 to 1,061 in 2023.

Customer Data Platform Institute, 2024

One major issue is the strain it puts on companies' operational efficiency and financial resources. As platforms multiply, managing them becomes increasingly complex, often resulting in duplication of features, inconsistent data flows, and fragmented user experiences that negatively affect productivity, creating double work and increasing the opportunities for human error. This can lead to inefficiencies, higher costs, difficulties in maintaining quality across the board and, unsurprisingly, more security issues.

This whitepaper explores how the new **Wire Cells solution** combines the secure communications capabilities of **Wire** and the powerful, intuitive and security-conscious **Cells** document management, sharing and collaboration platform to create a seamless, low-friction workspace that enables teams to work freely, safely, and privately.

The Challenge: Productivity & Security Need to go Hand in Hand

"Employees will begin to revolt, whether against too many apps or too many platforms in use for the same function. Having too many disparate applications and platforms can waste time, impede productivity and deliver a poor experience," Ali said. "Employees of large organizations may have ten or more work-related apps, each with a different user interface and operating characteristics. Simply finding the desired app can be a chore, and switching apps can interrupt the user's workflow."

Nadir Ali, CEO of Inpixon via SHRM blog

Security breaches, data privacy regulations, and cyber threats have made it essential for organizations to adopt tools that secure both communication and file-sharing/ collaboration. But up until now, there have been no user-friendly solutions that provided a secure by default workspace for organizations, their partners and even clients.

Here are some of the key challenges that are driving the need for a unified workspace solution that combines both communication and document sharing and collaboration.

4 Key Challenges:
Balancing Security and Usability in the Enterprise Workspace

1 - Data Breaches
We've all become a bit blasé about it because it's in the news every day. But, in 2023, a record-breaking **3,205 data breaches were reported**, marking **a 78% increase** from the previous year. The total number of impacted individuals reached 353 million. Key sources of these breaches included cyberattacks, supply chain vulnerabilities, and errors in human or system processes. The trend has continued into 2024, with notable breaches across sectors like healthcare and finance (source: ITRC - Identity Theft Resource Center). And if you are in a compliance-oriented industry or a sector where privacy and security are paramount, these numbers might keep you awake at night.

2 - Compliance
The need to adhere to strict data privacy regulations such as **GDPR, HIPAA**, and **CCPA** is critical in sectors like healthcare, finance, and law and another key challenge to developing a workspace toolset that is both highly usable and highly secure.

This is especially true now, with non-compliance costs skyrocketing. According to a report by DLA Piper, GDPR fines surged by 168% in 2022, with individual penalties costing up to 4% of annual global turnover or €20 million, whichever is higher. Meanwhile, HIPAA violations can result in fines up to $50,000 per violation (and a single breach can yield multiple violations), and CCPA fines reach up to $7,500 per intentional violation; the law even allows private lawsuits in cases of data breaches, exponentially adding to the potential costs – not to mention the hard-to-repair brand damage. Clearly, it does not pay to ignore or minimize the importance of data privacy issues.

3 - Fragmented Workflows
App fatigue is a real thing. As cited above, the average number of apps in an enterprise grew from 843 in 2021 to 1,061 in 2023. That's a lot of interfaces to learn, a lot of switching to do and a lot of reasons to look outside the approved toolset to find a simpler (often less secure) way to get work done. It won't come as a surprise that research has shown using multiple, unintegrated tools can lead to inefficiencies and security vulnerabilities.

According to Qatalog and Cornell University, it takes nearly 9.5 minutes for workers to refocus on tasks after switching applications, with 45% of employees reporting that these shifts make them less productive and lead to mental fatigue. More bad news: a 2023 research piece by Slack found that excessive app switching can drain up to 10 weeks of productivity per employee each year.

4 - Shadow IT
The painful reality is that the slow uptake of complex platforms is a fact of life. So, even the most secure platforms will fail to provide the desired outcome if your team members actively avoid them and use "unapproved" platforms to get their jobs done more quickly. This phenomenon is called "shadow IT."

A study by IBM cited by Cybersecurity specialist SC Media found that **33% of Fortune 1000 employees** regularly save and share company data using unsecured, third-party apps to enhance their work processes. Research by Gartner indicates that **83% of organizations** have experienced employees using unsanctioned apps, with an average of **75 unauthorized cloud services** in use per organization. The same research indicates that **83% of organizations** have experienced employees using unsanctioned apps, with an average of **75 unauthorized cloud services** in use per organization. And according to research by Next Cloud, 67% of teams have introduced their own collaboration tools into an organization, and 82% of teams have pushed back on IT or management about which collaboration tools should be used.

So simple and intuitive design isn't just preferred – it's essential for success in digital products. According to digital adoption specialists Whatfix, 80% of product features go underutilized because users struggle with complex interfaces. User experience is paramount but is often sacrificed for security.

Improving Security and Usability with Wire Cells
The new integrated Wire Cells platform is a significant evolution in the secure workspace market. Let's take a closer look at how Wire Cells can help organizations streamline workflows while ensuring **end-to-end security**, **compliance**, **and usability** for both their communications and file-sharing activities.

Overview of Wire and Pydio

The nature of modern work is communication, both spoken and written. A vast majority of that work takes place in meetings, emails, chats and the creation, sharing and collaboration of documents of all kinds. Hence, the proliferation of productivity and workspace solutions.

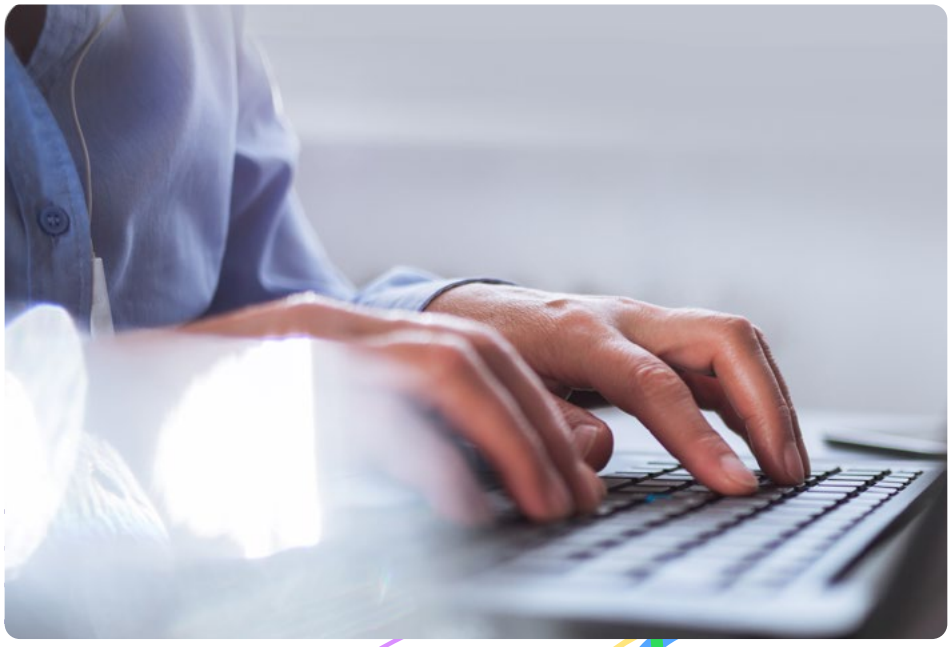
But the current range of available platforms doesn't include a solution that provides all the functionality and ease-of-use the modern worker needs to function effectively while also providing the serious security approach CISOs are looking for and the privacy and visibility that compliance departments require. This is the unmet need behind the creation of the Wire (secure communications) + Cells (secure document sharing and collaboration) integrated platform. Solving both these problems makes Wire Cells the standout solution in the secure workspace market.

First, let's look at the component systems.

Wire: Secure Communication Platform
Wire offers **real-time collaboration** with encrypted messaging, voice, video calls, and file sharing, built to prioritize security and privacy. It supports **end-to-end encryption** at scale across all chat, voice calls, video conferencing, and file sharing. It is designed to comply with the most stringent global privacy regulations based on a transparent and verifiable open-source core.

Core Features:

- → Industry-leading security that is invisible to end users.
- → End-to-end encryption for all messages, calls, files, reactions, voice messages, videos, screen-shares, and more.
- → Group chat and secure conferencing for team collaboration.
- → Cross and multi-platform support (web, desktop, mobile).
- → GDPR and CCPA-compliance
- → Available via Wire Cloud or self-hosted options for full data sovereignty.
- → Simple guest room features for secure collaboration with external stakeholders, no account registration or app download required.



Cells: Secure File Sharing, Collaboration and Management

Cells is an enterprise-grade platform for **file sharing, collaboration and management**. It allows organizations to host their own private file storage infrastructure, giving them full control over their data. Cells integrates advanced security features such as encryption, access control, and audit trails, making it a trusted solution for organizations that need to safeguard sensitive information.

Core Features:

- → Self-hosted, on-prem or private cloud infrastructure for file storage, sharing, and management.
- → Encryption of files is dynamic, fluid and invisible to end users just like Wire messaging (with MLS)
- → Granular permissions and access control for files and folders.
- → Encryption of files both in transit and at rest.
- → Collaboration tools like file versioning, commenting, and file locking.
- → Compliance with data regulations like GDPR.
- → Cross-platform support with web, desktop, and mobile clients.
- → Automation and creation of workflows and integration to source systems.

Wire + Cells Reset the Bar for Workspace Solutions

Let's not beat around the bush. There is a simple, fairly obvious reason why combining Wire and Cells into a single seamless solution is a powerful advance in workspace platforms. In the combined Wire Cells, workers do 80%+ of their daily tasks in a single, secure-by-default and simple-by-design interface — no more code-switching and productivity drains. That's something no other workspace platform can claim.

By integrating end-to-end encrypted messaging and encrypted file management, Wire Cells empowers teams to collaborate effortlessly, stay compliant, and protect sensitive data—all in one flexible, scalable solution. Wire Cells provides security levels elevated beyond what is currently available in the marketplace. Independently used and continuously audited by governments worldwide, Pydio and Wire are at the cutting edge of collaboration for organizations of all sizes, with zero compromises on all levels. The combined platform represents a revolution in workspace technology, delivering solutions for a variety of use cases:

1. Unified, Secure Collaboration Ecosystem

Why Does It Matter?
We've all been in a video call, needed to share a document from our file system, and then shared the link in a messenger app so it doesn't disappear when the call is over. Put aside the inconvenience and time wastage, the security and privacy risks are enormous. Even if you are using a more convenient, unified productivity platform, there is a lot of evidence out there to show that your data is not secure from others (and even from your platform provider, who may be using it to train AI models... or worse).

How Does Wire Cells Address the Issue?
Combining Wire's secure communication capabilities with Cells' secure file management results in a **unified workspace platform** where security is maintained across all layers of communication and data exchange:

- → The **real-time communication layer** ensures that messaging, calls, and video conferencing are fully encrypted and secure.
- → The **data management layer** ensures secure storage and access control for files being shared and collaborated on.

This combination means that both **communication and file-sharing are encrypted and protected** at every stage, from discussion to document exchange.

2. Enhanced Data Security and Control

Why Does It Matter?
If you are in the military, government, law enforcement, or an industry that places a premium on privacy, security, and compliance, like finance, healthcare or law, the reality of your operational environment precludes using platforms with an unserious approach to data security. You can't afford to adopt solutions where you don't have complete control over how your data is transmitted, stored, shared or processed. Wire Cells is the serious secure workspace solution.

How Does Wire Cells Address the Issue?
Pydio's ability to **self-host file storage** ensures that sensitive information is not stored on third-party servers (meaning you can ensure data sovereignty and privacy), while Wire's **on-premise hosting** option allows for similar control over real-time communication.

- → **Wire's end-to-end encryption** ensures that all discussions, whether text or voice, remain private.
- → **Pydio's eight levels of ACL protection** and encryption ensure that files are secure from unauthorized access, even when shared across teams.

In industries like **healthcare, legal, finance, and government**, this dual-layered security ensures compliance with data protection laws such as **HIPAA**, **GDPR**, and **CCPA**.

3. Streamlined Workflows

Why Does It Matter?
As was mentioned in the introduction to this whitepaper, app fatigue and the constant context switching between different interfaces take a serious toll on productivity in most modern organizations. We won't waste your time with more stats and studies to support this thesis. Most of us are all too familiar with lost focus, lost time, and lost energy, which are caused by having to use too many tools to do common daily work tasks. OK, maybe one more stat from the Qatalog / Cornel study cited earlier: "The proliferation of software tools in the typical workplace is undermining fair access to information. 54% of people say that applications can sometimes make it harder to find information."

How Does Wire Cells Address the Issue?
Incorporating Wire and Pydio into a single workflow eliminates the need to switch between platforms for communication and file-sharing. Teams can have secure discussions and seamlessly transition to collaborating on files on the fly.

Example Workflow:
1. Discussion: Team members discuss project updates in real time using encrypted messaging.
2. File Sharing: Once ready, a team member shares the necessary files, ensuring that all sensitive documents remain encrypted and accessible only to authorized personnel.
3. Collaboration: Team members can comment, edit, or lock files while continuing to discuss their changes.

Bonus: Audit and Compliance: The unified platform maintains an audit trail of file access, ensuring that compliance is maintained, and logs communication metadata for accountability - all encrypted and secured, of course.

4. Privacy-First Collaboration

Why Does It Matter?
Communications privacy is vital for government organizations and enterprises because it safeguards sensitive data, protects national security, ensures regulatory compliance, and maintains public trust. Secure communication channels help prevent breaches that could lead to financial loss, legal issues, and reputational damage. Ensuring privacy in communications is essential for operational security, risk management, and stability in both government and enterprise sectors.

How Does Wire Cells Address the Issue?
Both the original Wire and Pydio platforms have strong privacy-centric foundations. They are **open-source**, allowing organizations to verify their security through independent audits. Additionally, both platforms enable **GDPR compliance**, helping organizations meet even the strictest data protection requirements. All of those privacy-centric foundations are carried over into the new unified platform.

- → **No communications metadata** is stored on servers, protecting the privacy of communication beyond just the content of messages and calls.
- → Allows businesses to host their own storage, giving them the ability to **control where data is stored** and who has access.

This combination offers an environment where organizations can be confident that both their communications and files are **shielded from surveillance and/or unauthorized access**.

And best of all, the **security is almost invisible** to end users, allowing them to focus on their work rather than having to worry about if they've followed a series of complex security procedures or having to hop back and forth between tools.

5. Secure External Collaboration

Why Does It Matter?
If your productivity platform allows you to add guest users but doesn't ensure those connections are private and secure, that's actually a bigger problem than not allowing guest connections at all. If your documents and comms end up getting inappropriately shared or, even worse, breached due to being shared with a partner, the impact is every bit as serious as an internal breach or leak.

How Does Wire Cells Address the Issue?
Wire Cells enables secure collaboration not only within an organization but also with **external partners** or stakeholders. Wire's **guest access** allows temporary, secure communication channels for third parties, while Cells' **granular permissions** allow for controlled file sharing with external collaborators. Also, by staying within a single platform, the solution reduces the likelihood of data spillage due to human error.

For example, a legal firm can use Wire for secure client-lawyer communication while sharing case files with clients via Cells' virtual data rooms, ensuring that all interactions are both encrypted and compliant with data privacy regulations.

Use Cases for Wire and Cells Integration

1. Healthcare

Challenge:
Healthcare professionals, such as doctors, nurses, and administrative staff, need to coordinate on patient care, which often requires sharing sensitive information (PII) like medical histories, imaging files, and treatment plans. However, communicating this information over regular channels like email or consumer messaging apps risks violating HIPAA standards, putting patient privacy and organizational compliance at risk. The challenge intensifies when specialists and other facilities need to access records remotely or consult on a case, adding another layer of security requirements and data-sharing hurdles.

Solution:
Wire Cells offers an all-in-one platform specifically designed for secure healthcare communication. With end-to-end encryption on messages and video consultations, doctors can confidently discuss cases, share insights, and provide real-time guidance without the risk of unauthorized access. Additionally, Wire Cells' role-based access ensures that only authorized personnel can view or edit specific files, supporting easy collaboration while maintaining strict access controls.

2. Financial Services

Challenge:
Financial institutions manage highly sensitive client information, from investment portfolios and personal financial statements to contracts and regulatory filings. Advisors and financial analysts need to communicate securely with clients and colleagues to discuss strategies, review performance, and manage complex transactions. At the same time, they face stringent data privacy regulations such as GDPR and CCPA, which mandate strict control over personal data handling and access, as well as transparency in data management practices. These compliance requirements make it crucial for financial institutions to protect client information against unauthorized access, data breaches, and accidental disclosure.

Solution:
Wire Cells offers a full workspace solution for secure communication and document management within financial institutions, as well as with clients and partners. Wire Cells gives financial institutions the tools they need to communicate with confidence, knowing they are protecting sensitive data and privacy and complying with financial and privacy regulations.

3. Legal Firms

Challenge: Lawyers and legal teams handle highly sensitive and confidential information, including case files, contracts, and legal briefs. Effective communication with clients and secure collaboration on documents is essential to managing cases efficiently. However, these interactions and files often contain privileged information, requiring strict access controls and comprehensive audit trails to meet ethical obligations and regulatory compliance standards, like attorney-client privilege. Standard email and file-sharing tools lack the necessary security, putting confidential data at risk of exposure.

Solution: Wire and Pydio provide a secure, compliant platform for both lawyer-client communication and document management, addressing the unique needs of the legal sector.

Features in Action:

- → **Encrypted Lawyer-Client Communication:** Lawyers can securely message and hold video consultations that safeguard all interactions. For example, a lawyer preparing a case can share sensitive updates with a client through a secure video call, ensuring that privileged information is kept private and cannot be intercepted.
- → **Secure Document Storage and Controlled Collaboration:** Role-based access controls and audit trails mean legal teams can collaborate on documents while ensuring that only authorized team members can access or modify files.
- → **Compliance with Confidentiality Requirements:** Communication encryption, audit trails and secure storage for documents help firms meet compliance requirements for handling sensitive legal documents.

4. Government and Defense

Challenge: Government agencies handle highly confidential information, from classified documents to sensitive citizen data, often related to national security, law enforcement, or regulatory matters. These agencies require a secure way to communicate internally, collaborate on documents, and manage data across departments while maintaining strict control over where and how their data is stored. Additionally, compliance with policies on data sovereignty and security standards is essential, as many government regulations mandate that data be stored within the agency's own infrastructure or within national borders.

Solution: The integrated Wire Cells solution provides encrypted messaging and conferencing to allow for secure internal communication while also enabling agencies to securely store and collaborate on confidential documents on their own infrastructure.

Conclusion

The integrated Wire Cells solution creates a robust, secure workspace environment that helps address major pain points (platform creep and app fatigue) for organizations and industries requiring stringent compliance and privacy protections, from healthcare and law to finance and government. Wire Cells represents an essential, future-proof workspace solution that balances security, productivity, and data sovereignty.

wire.com