Secure **Enterprise Collaboration**

Wire's platform is purpose-built to deliver a comprehensive workspace for enterprise-class collaboration. Wire provides audio, video, messaging, and file sharing for at-scale enterprise teams, protected by the industry's most stringent security. Wire makes it possible to foster the open, productive collaboration that users want while ensuring the data privacy, protection, and compliance that enterprises need.

wire

The Secure Collaboration Conundrum

Open collaboration is at the heart of digitally transformed work today. This means that sensitive data is often passed between a broad variety of parties, including employees, recruits, contractors, clients, partners, and vendors. This trend isn't going away. Enterprises and government agencies are prioritizing the delivery of world-class digital experiences for customers, citizens, and workers.

Yet this openness flies directly in the face of another critical priority – safeguarding data. Data is destiny for modern organizations. For enterprises, sensitive data holds the crown jewels of intellectual property, business relationships and operational practices. For "security-first" organizations such as government, military, and law enforcement agencies, operational data and real-time communications is a life or death matter, and determines mission success or failure.

Unfortunately, the choices to keep these priorities in balance have been severely lacking. Organizations have had to choose between three unpalatable choices:

Compromised collaboration platforms offered by tech giants that actively seek to monetize sensitive customer data and negligently riddle their products with deeply insecure features and default configurations.

Unserious products that deliver a fraction of the range needed for full collaboration, only work for the most technical users, feature security theater more than deep security, and in many cases cater to unprofessional institutions.

Dangerous abdication to deeply inappropriate, shadow IT tools like WhatsApp, that leave enterprises exposed to the worst of all possible worlds–tech giant monetization and endless opportunities to get compromised, like when your sensitive data gets exposed to the next organization or friend your employee associates with via their consumer account.

10+ Years of experience

>1800 Customers world wide

Zero Knowledge Architecture

100% Ease of use

For more information go to: **wire.com/en/security**

The World's Most Secure Collaboration

Wire delivers the only enterprise-class collaboration solution that is comprehensively secured at scale by the Messaging Layer Security (MLS) standard, the industry's first encryption protocol built specifically for real-time collaboration media including messaging, audio and video conferencing.

Unlike compromised or unserious market alternatives, Wire turns world-class MLS encryption on by default with no option (ever) to turn it off, and implements a true zero-knowledge architecture. This means that security is delightfully invisible to users, creating an optimally productive experience that compromises nothing from a security point of view. It also means that even if Wire servers are hacked, your communication stays completely secure. And, there are no by-default, god-like IT administrator powers that allow credential compromises to wreck your data security, reputation, and business.

Mature Platform Capabilities

Following are a sample of Wire's powerful, complete, and thoughtful capabilities:

Secure messaging
Every single message in 1:1 and group conversations is individually encrypted, end-to-end.

Voice and video conferencing
Talk to your team members and externals either on 1:1 or group voice & video calls.

File exchange
Share any type of file format across devices. Every file is individually end-to-end encrypted.

Self-deleting messages
Send confidential messages that disappear after an indicated amount of time.

Secure guest access without registration
Invite externals securely via dedicated guest links or chat rooms.

Verified communications
Digital fingerprinting of all participants' devices for the strongest verification of end-user devices.

Cross-platform
Available on iOS, Android, Windows, Mac, Linux, and web browsers.

Open source
Full transparency with access to the source code, making it the most audited software in the market.

Key Security Principles

Zero Knowledge Architecture
Assumes all data, devices, apps, and users are insecure and require authentication.

End-to-End Encryption
Every message, every file is individually encrypted.

Data Sovereignty
Crucial to maintain control and responsibility over personal data.

For more information go to: **wire.com/en/security**

A Security First Approach

Strongest Protection
Always-on, End-to-End Encryption and Zero Knowledge Architecture for maximum protection – no decryption possible by admins, operators or Wire.

Team Management Console
Enterprise-grade administration console to manage users, roles, and permissions.

Security by Design
Wire solutions have been built with the highest security in mind from day one, made easy and invisible to end-users.

Unrivaled Security
Dedicated apps for mobile devices and desktop ensure end-to-end encryption on all devices.

Self-deleting Messages
Messages can be set to auto delete based on the time they were sent and read.

Perfect Forward and Post-Compromise Secrecy
Every call, message, and file is encrypted with a new random key.

Deployment Agnostic
You can deploy Wire in the way that best meets your needs, whether in your private cloud (Azure, AWS, STACKIT), on-premises or hybrid. Or you can get started instantly with Wire Cloud. It's your choice.

Enabling Compliance
Enables organizations to easily comply with internal and external rules and regulations.

Made in Germany
Built in the country with one of the world's strictest data regulations, privacy and security are in our DNA.

For more information go to: **wire.com/en/security**