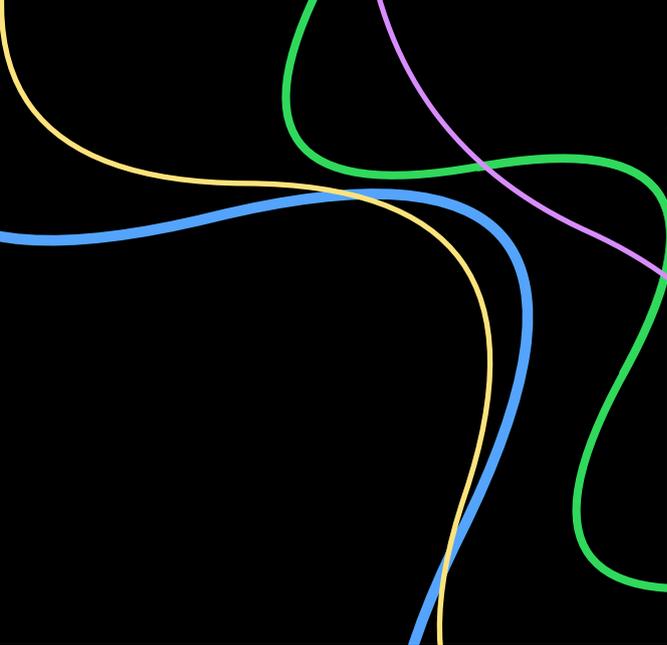




Sichere Zusammenarbeit für Europäische Unternehmen

Wire wurde speziell entwickelt, um einen umfassenden Arbeitsbereich für die Zusammenarbeit auf Unternehmensebene bereitzustellen. Die Plattform vereint Audio-, Video-, Messaging- und Dateiaustauschfunktionen und unterstützt damit die effiziente Kommunikation großer Teams. Alle Inhalte sind durch branchenführende Sicherheitsstandards geschützt. Wire ermöglicht die offene und produktive Zusammenarbeit, die Benutzer sich wünschen, und erfüllt gleichzeitig die Anforderungen an Datenschutz, Sicherheit und Compliance, die Unternehmen erwarten.



Das Problem der sicheren Zusammenarbeit

Offene Zusammenarbeit ist heute das Herzstück der digitalen Transformation der Arbeitswelt. Das bedeutet, dass sensible Daten oft zwischen einer Vielzahl von Parteien ausgetauscht werden, darunter Mitarbeiter, Personalverantwortliche, Auftragnehmer, Kunden, Partner und Lieferanten. Dieser Trend wird nicht verschwinden. Unternehmen und Behörden legen den Schwerpunkt auf die Bereitstellung erstklassiger digitaler Erlebnisse für Kunden, Bürger und Mitarbeiter.

Doch diese Offenheit steht im direkten Widerspruch zu einer anderen wichtigen Priorität – dem Schutz von Daten. Daten sind der Schlüssel für moderne Unternehmen. Sensible Daten sind die Krönung des geistigen Eigentums, der Geschäftsbeziehungen und der betrieblichen Abläufe. Für Organisationen, bei denen Sicherheit an erster Stelle steht, wie z. B. Regierungen, Militär und Strafverfolgungsbehörden, sind operative Daten und Echtzeitkommunikation eine Frage von Leben und Tod und entscheiden über Erfolg oder Misserfolg einer Mission.

Leider fehlte es bisher an Möglichkeiten, diese Prioritäten in Einklang zu bringen. Die Unternehmen mussten sich zwischen drei ungenießbaren Möglichkeiten entscheiden:



Kompromittierte Kollaborations-Plattformen von Tech-Giganten, die aktiv versuchen, sensible Kundendaten zu monetarisieren und ihre Produkte fahrlässig mit äußerst unsicheren Funktionen und Standardkonfigurationen ausstatten.



Unseriöse Produkte, die nur einen Bruchteil des für eine vollständige Zusammenarbeit erforderlichen Umfangs bieten, nur für die technisch versiertesten Benutzer funktionieren, eher einen Schein von Sicherheit als echten Schutz bieten und sich in vielen Fällen an unprofessionelle Einrichtungen richten.



Gefährliche Abkehr zu völlig unangemessenen Schatten-IT-Tools wie WhatsApp, die Unternehmen dem Schlimmsten aller möglichen Welten aussetzen – der Monetarisierung durch Tech-Giganten und endlosen Möglichkeiten, kompromittiert zu werden, z. B. wenn Ihre sensiblen Daten dem nächsten Unternehmen oder Freund, mit dem Ihr Mitarbeiter über sein Privatkundenkonto verkehrt, zugänglich gemacht werden.

10+

Jahre
Erfahrung

>1800

Kunden in
aller Welt

Zero

Knowledge
Architektur

100%

Einfache
NutzU



Die sicherste Zusammenarbeit der Welt

Wire ist die einzige Collaboration-Lösung auf Unternehmensniveau, die durch den Messaging Layer Security (MLS)-Standard geschützt wird – das erste Verschlüsselungsprotokoll der Branche, das speziell für Echtzeit-Kommunikation wie Messaging, Audio- und Videokonferenzen entwickelt wurde.

Im Gegensatz zu kompromittierten oder unsicheren Alternativen ist bei Wire die erstklassige MLS-Verschlüsselung standardmäßig aktiviert – und kann niemals deaktiviert werden. Zusätzlich setzt Wire auf eine echte Zero-Knowledge-Architektur: Sicherheit bleibt für die Nutzer unsichtbar und ermöglicht so eine optimale Benutzererfahrung ohne Kompromisse. Selbst im Fall eines Angriffs auf die Wire-Server bleibt Ihre Kommunikation vollständig geschützt. Zudem existieren keine standardmäßigen, übergeordneten IT-Administratorrechte, die im Falle eines gestohlenen Zugangs kompromittierte Daten, Reputationsschäden oder geschäftliche Risiken verursachen könnten.



Wichtige Funktionen

Im Folgenden finden Sie einige Beispiele für die leistungsstarken Funktionen von Wire:



Sicheres Messaging

Jede einzelne Nachricht in 1:1 und Gruppengesprächen ist individuell verschlüsselt, Ende-zu-Ende



Sprach- und Videokonferenzen

Sprechen Sie mit Ihren Teammitgliedern und externen Personen – entweder 1:1 oder in Gruppenanrufen per Sprache und Video



Dateiaustausch

Tauschen Sie beliebige Dateiformate geräteübergreifend aus. Jede Datei ist individuell Ende-zu-Ende verschlüsselt



Selbstlöschende Nachrichten

Senden Sie vertrauliche Nachrichten, die nach einer bestimmten Zeitspanne verschwinden



Sicherer Gastzugang ohne Registrierung

Laden Sie externe Personen auf sichere Weise über spezielle Gastlinks oder Chaträume ein



Verifizierte Kommunikation

Digitaler Fingerabdruck der Geräte aller Teilnehmer für die stärkste Verifizierung der Endgeräte



Plattformübergreifend

Verfügbar für iOS, Android, Windows, Mac, Linux und Webbrowser



Open source

Vollständige Transparenz mit Zugriff auf den Quellcode, was sie zur am meisten geprüften Software auf dem Markt macht

Wichtige Sicherheitsgrundsätze

Zero Knowledge Architektur

Geht davon aus, dass alle Daten, Geräte, Anwendungen und Benutzer unsicher sind und eine Authentifizierung erfordern

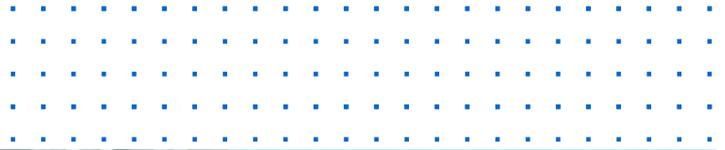
Ende-zu-Ende-Verschlüsselung

Jede Nachricht, jede Datei ist einzeln verschlüsselt

Datensouveränität

Wichtig, um die Kontrolle und Verantwortung über persönliche Daten zu behalten





Sicherheit hat Vorrang

Stärkster Schutz

Immer aktive Ende-zu-Ende-Verschlüsselung und Zero-Knowledge-Architektur für maximalen Schutz – keine Entschlüsselung durch Administratoren, Betreiber oder Wire möglich

Team-Management-Konsole

Eine Verwaltungskonsole auf Unternehmensniveau zur Verwaltung von Benutzern, Rollen und Berechtigungen

Sicherheit durch Design

Die Lösungen von Wire wurden vom ersten Tag an mit Blick auf höchste Sicherheit entwickelt und sind für den Endbenutzer einfach und unsichtbar

Unübertroffene Sicherheit

Spezielle Apps für Mobilgeräte und Desktop gewährleisten eine Ende-zu-Ende-Verschlüsselung auf allen Geräten

Selbstlöschende Nachrichten

Nachrichten können so eingestellt werden, dass sie automatisch gelöscht werden, je nachdem, wann sie gesendet und gelesen wurden

Perfect-Forward und Post-Compromise-Secrecy

Jeder Anruf, jede Nachricht und jede Datei wird mit einem neuen Zufallsschlüssel verschlüsselt

Unabhängig vom Einsatz

Sie können Wire so einsetzen, wie es Ihren Anforderungen am besten entspricht, ob in Ihrer privaten Cloud (Azure, AWS, STACKIT), vor Ort oder als Hybridlösung. Oder Sie können mit Wire Cloud sofort loslegen. Sie haben die Wahl

Ermöglicht Compliance

Ermöglicht Unternehmen die einfache Einhaltung interner und externer Regeln und Vorschriften

Made in Germany

Da wir in dem Land mit einer der strengsten Datenschutzbestimmungen der Welt entwickelt wurden, liegen Datenschutz und Sicherheit in unserer DNA

