Wire **für öffentliche Sicherheit & Notfalldienste**

Wire ist eine sichere Kommunikationsplattform, die speziell für die hohen Anforderungen von Organisationen der öffentlichen Sicherheit und des Rettungswesens entwickelt wurde.
Mit Ende-zu-Ende-verschlüsselten Audio, Video, Messaging und Dateiaustausch ermöglicht Wire eine reibungslose Zusammenarbeit und erfüllt höchste Sicherheitsstandards.

Entwickelt für missionskritische Einsätze, bietet Wire „Blaulicht"-Teams eine schnelle, nahtlose und zuverlässige Kommunikation. So können sie effektiv reagieren und gleichzeitig die von Organisationen der öffentlichen Sicherheit und Notfalldiensten geforderte Vertraulichkeit, Ausfallsicherheit und Datensicherheit gewährleisten.

wire

Wire – Wo Sicherheit und Zuverlässigkeit aufeinander treffen

Die Dienste der öffentlichen Sicherheit und des Rettungswesens – wie Krankenwagen, Polizei, Feuerwehr und Rettungsdienst – sind naturgemäß auf hochgradig sichere und zuverlässige Echtzeitkommunikation angewiesen. Sie müssen Notfälle bewältigen, sensible Informationen schützen und mehrere Teams koordinieren, die in dynamischen, schnell wechselnden Situationen agieren. Das hohe Risiko dieser „Blaulicht"-Einsätze bedeutet, dass Sicherheitsverletzungen, Abhörversuche oder unbefugter Zugriff schwerwiegende Folgen haben können. Auch der Schutz sensibler und persönlicher Daten hat höchste Priorität. Dabei dürfen Sicherheit und Datenschutz jedoch niemals auf Kosten der Benutzerfreundlichkeit gehen – insbesondere, wenn jede Sekunde zählt.

Mit Wire geht die sichere Kommunikation nie auf Kosten der Benutzerfreundlichkeit. Die Plattform bietet die neueste Ende-zu-Ende-Verschlüsselung, eine dezentralisierte Architektur und die Einhaltung strenger Sicherheits- und Datenschutzvorschriften (GDPR, ISO, NIS2.) und ist damit ideal für Notdienste. Und das Beste ist, dass diese Sicherheit für die Endbenutzer absolut unsichtbar ist – sie erleben einfach einen leistungsstarken, benutzerfreundlichen Kommunikationskanal, auf den sie sich verlassen können, wenn sie ihn am meisten brauchen.

10+
Jahre Erfahrung

>1800
Kunden in aller Welt

Zero
Knowledge Architektur

100%
Einfache Nutzu

*Messaging Layer Security (MLS) ist der fortschrittlichste, offene Standard für eine Ende-zu-Ende-verschlüsselte Gruppenkommunikation. Wire hat MLS mitbegründet und ist die einzige Collaboration Suite, die MLS standardmäßig in allen Produkten, Funktionen und Merkmalen vollständig implementiert.

© 2025 Alle Rechte vorbehalten

Weitere Informationen finden Sie unter: **wire.com/de/sicherheit**

Kernfunktionen für öffentliche Sicherheit und Notfalldienst

Sichere, verschlüsselte und nahtlose Kommunikation

Immer verfügbare Ende-zu-Ende-Verschlüsselung
Alle Funktionen – Chat, Konferenzen, Dateifreigabe, Reaktionen und Nachrichten-Zeitstempel – sind immer über MLS* Ende-zu-Ende-verschlüsselt. Egal, ob Sie einen Standort, ein GIF oder ein Dokument senden, nur der vorgesehene Empfänger kann auf die Informationen zugreifen. Teamadministratoren und Operatoren haben keinen Zugriff auf die ausgetauschten Informationen und können so das Team verwalten, ohne sensible Informationen zu riskieren.

Multi-tenancy
Führen Sie getrennte Teams innerhalb derselben Serverinfrastruktur und sorgen Sie für eine rollenbasierte Trennung. Jedes Team bleibt sicher und arbeitet ohne Unterbrechung.

Sichere Standortmitteilung
Die Fähigkeit, Mitglieder verschiedener Dienste über Wire zu verfolgen und eng zu koordinieren, ohne das Risiko einzugehen, Standortdaten preiszugeben, ist eine entscheidende Fähigkeit für Organisationen der öffentlichen Sicherheit und Notfalldienste. Administratoren können den Föderationszugang regulieren und die Suchsichtbarkeit steuern, wobei Optionen wie keine Suche, exakter Handle oder nur E-Mail-Adresse möglich sind.

Föderation
Kommunizieren Sie nahtlos mit anderen Organisationen über die Federation-Funktionen von Wire. Jede Organisation kann ihre eigene unabhängige Wire-Instanz mit administrativer Kontrolle unterhalten, wobei jedoch nahtlose Verbindungen über eine Wire-Federation hergestellt werden können. Administratoren können den Federation-Zugriff regeln und die Sichtbarkeit der Suche steuern, indem sie Optionen wie No Search, Exact Handle oder Only Email Address zulassen.

Out-of-Band-Kommunikation
Out-of-Band-Kommunikation (OOB) wird verwendet, wenn die primären Kanäle kompromittiert oder gefährdet sind. Wire unterstützt die OOB-Kommunikation durch die Bereitstellung separater, vorab eingerichteter verschlüsselter Kanäle, die im Falle von Cyberangriffen, Insider-Bedrohungen, Netzwerkausfällen oder verdeckten Operationen aktiviert werden können.

*Messaging Layer Security (MLS) ist der fortschrittlichste, offene Standard für eine Ende-zu-Ende-verschlüsselte Gruppenkommunikation.
Wire hat MLS mitbegründet und ist der einzige Anbieter, der MLS standardmäßig in allen Produkten und Funktionenvollständig implementiert hat.

© 2025 Alle Rechte vorbehalten

Anwendungsfälle aus der Praxis

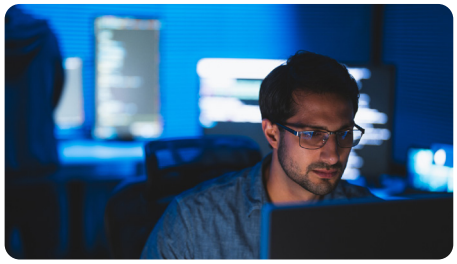
Reaktion auf schwere Verkehrsunfälle
(Einsatzleitung & Koordination)

Eine **Massenkarambolage mit 15 Fahrzeugen** auf einer Autobahn erfordert den Einsatz von **Krankenwagen, Polizei und Feuerwehr**

- → **Wire-Gruppenanrufe die Reaktio**n, damit alle Einheiten Echtzeit-Updates erhalten.
- → Sanitäter kontaktieren Krankenhäuser per Live-Video vom Einsatzort, um die Versorgung von Verletzten vorzubereiten.
- → **Feuerwehr und Rettungsdienst** erhalten Blaupausen eines Treibstofflagers, um das Explosionsrisiko einzuschätzen.

Wire Funktion	Vorteil
Sichere Gruppenanrufe	Real-time coordination between services
End-to-End verschlüsselte Nachrichten	Sichere Weitergabe von Informationen über Orte und Patienten
Videoanrufe	Medizinische Triage und Beurteilung aus der Ferne
Versand von Dateien	Echtzeitzugriff auf Vorlagen und Informationen

Koordinierte Reaktion zur Terrorismusbekämpfung
(Geheime und sensible Polizeieinsätze)



Die Polizei hat einen Vorfall mit einem aktiven Schützen gemeldet, der möglicherweise Verbindungen zu einer **Terrorgruppe** hat. Die Reaktion erfordert die Koordinierung zwischen Polizei, Geheimdiensten, Spezialkräften sowie Krankenwagen und Feuerwehr.

- → **Interorganisationale Kommunikation** wird über Wire-Federation vereinfacht. federation
- → Außeneinsatz nutzen das verschlüsselte **Messaging von Wire**, um mit dem Hauptquartier zu kommunizieren, ohne Gefahr zu laufen, abgehört zu werden.
- → **Die Standortmitteilung** in Echtzeit stellt sicher, dass taktische Einheiten effizient arbeiten.
- → **Out-of-Band-Kommunikation** Wire kann als sicheres OOB-Backup für die primären Instrumente dienen, falls diese kompromittiert werden.

Wire Funktion	Vorteil
Verschlüsseltes Messaging	Schützt vertrauliche Daten vor Cyber-Bedrohungen
Sichere Standortmitteilung	Echtzeit-Tracking für taktische Teams
Multi-Geräte-Synchronisierung	Sicherer Zugriff auf Nachrichten und Dateien von jedem Gerät aus
Out-of-Band-Kommunikation	Verwendung alternativer sicherer Kanäle im Falle einer Kompromittierung

© 2025 Alle Rechte vorbehalten

Notfalltransfer von Schlaganfallpatienten
(Sicherer Austausch medizinischer Daten)

Eine 55-jährige Frau erleidet einen kritischen Schlaganfall und benötigt schnelle Hilfe in der Notaufnahme eines Fachkrankenhauses.

- → **Rettungssanitäter nutzen Wire, um in Echtzeit die Vitalwerte und die Krankengeschichte des Patienten** mit den Spezialisten im Krankenhaus auszutauschen.
- → **Bereitschaftsärzte nehmen an einer verschlüsselten Videokonferenz teil**, um den Patienten vor seiner Ankunft zu beurteilen.
- → Das System **unterstützt den sicheren Dateiaustausch von medizinischen Bildern und Testergebnissen** ohne HIPAA/GDPR-Verstöße

Wire Funktionen	Vorteil
Sicheres Messaging	Sichere Weitergabe von Patientendaten und Krankengeschichte
Verschlüsselte Videoanrufe	Fernkonsultation mit Spezialisten
Dateiaustausch	Übermittlung von medizinischen Berichten und Testergebnissen
Konformität mit GDPR & HIPAA	Gewährleistet vollständigen Schutz der Privatsphäre

Evakuierungskoordination bei Waldbränden
(Katastrophenhilfe und großflächiges Krisenmanagement)

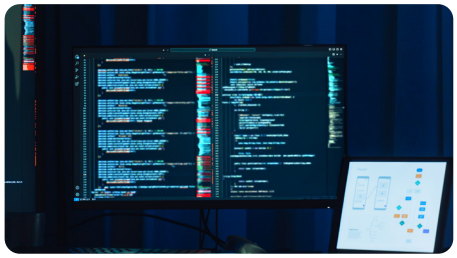
Ein sich **schnell ausbreitender Flächenbrand** bedroht mehrere Gemeinden und erfordert eine koordinierte Reaktion von Feuerwehr und Rettungsdienst, Polizei und Notfallteams.

- → Teams **nutzen die Gruppenanruf-Funktion von Wire** für Live-Updates über die Ausbreitung von Bränden und Evakuierungsanweisungen.
- → Notfallhelfer in abgelegenen Gebieten nutzen das **Offline-Message-Queuing von Wire**, um Updates zu erhalten, sobald die Verbindung wiederhergestellt ist.
- → **Sicherer Dateiaustausch** ermöglicht die Übertragung von Drohnenaufnahmen, Satellitenbildern und Strategien zur Feuereindämmung.

Wire Funktion	Vorteil
Sichere Gruppenanrufe und Messaging	Koordinierung in Echtzeit
Offline-Nachrichtenwarteschlange	Gewährleistet die Zustellung von Nachrichten in Gebieten mit schlechter Konnektivität
Sicherer Dateiaustausch	Ermöglicht datengestützte Entscheidungen

© 2025 Alle Rechte vorbehalten

Verhinderung interner Datenverstöße
(Cybersecurity & Insider-Bedrohungen)



Nachdem sie einige glaubwürdige Beweise erhalten haben, ermitteln Polizeibeamte in **einem hochkarätigen Korruptionsfall**. Dabei geht es um Regierungsbeamte, die verdächtigt werden, Staatsgeheimnisse zu verraten und sie an kriminelle Organisationen zu verkaufen. Es besteht die Sorge, dass interne Lecks die Ermittlungen vor Kriminellen bloßstellen könnten.

- → **Die Ermittler nutzen die geschützten Kanäle von Wire anstelle der offiziellen Netzwerke**, um sicher zu kommunizieren.
- → **Wire ID Shield** stellt sicher, dass nur verifiziertes Personal auf kritische Daten zugreifen kann.

Wire Funktion	Vorteil
Zero-Trust-Sicherheitsmodell	Schützt vor Insider-Bedrohungen
Ende-zu-Ende-Verschlüsselung	Stellt sicher, dass Gespräche privat bleiben
Wire ID Shield	Verhindert unbefugten Zugriff
Sicherer Gastzugang	Ermöglicht sichere Unterstützung durch überprüfte externe Experten

Multinationale Ermittlungen zur Bekämpfung des Menschenhandels
(Grenzüberschreitende Sicherheitsoperationen)

Ein **Menschenhändler-Netzwerk** operiert in Deutschland, Frankreich und Großbritannien. Um es zu zerschlagen und das Risiko für die Opfer zu minimieren, müssen die Strafverfolgungsbehörden auf mehreren Ebenen und in verschiedenen Ländern im Gleichschritt und unter völliger Geheimhaltung zusammenarbeiten, um es zu zerschlagen.

- → **Strafverfolgungsbehörden kooperieren auf sichere Weise** über Wire.
- → Fallakten, Verdächtigenlisten und forensische Beweise werden über den verschlüsselten Dateiaustausch von Wire weitergegeben.
- → Live-Videoanrufe mit Polizeichefs und Geheimdiensten gewährleisten Echtzeit-Updates.

Wire Funktion	Vorteil
Interoperables sicheres Messaging und Anrufe	Keine Abhängigkeit von lokalen Telekommunikationsnetzen
Verschlüsselter Austausch von Dateien und Beweisen	Verhindert die Weitergabe vertraulicher Informationen
Out-of-Band-Kommunikation	Gewährleistet den Erfolg der Mission, selbst wenn die primären Kanäle versagen

© 2025 Alle Rechte vorbehalten

Gewährleistung einer sicheren unternehmenskritischen Kommunikation

Wire gewährleistet eine **sichere, verschlüsselte Echtzeit-Kommunikation** für Blaulicht-Dienste und erfüllt damit kritische Anforderungen in den Bereichen Notrufzentrale, Terrorismusbekämpfung, medizinische Versorgung, Katastrophenmanagement und Cybersicherheit. Mit fortschrittlichen Sicherheitsfunktionen **schützt Wire sensible Daten, verbessert die Koordination und sorgt für Widerstandsfähigkeit gegen Cyber-Bedrohungen.**

Das Wire Versprechen für sichere Kommunikation

Egal welcher Anwendungsfall, Wire bietet immer diese Vorteile

Alles E2EE

End-to-End-Verschlüsselung (E2EE) der nächsten Generation macht Sicherheit unsichtbar und einfach für große und komplexe Organisationen

End-to-End-Verschlüsselung (E2EE) der nächsten Generation macht Sicherheit unsichtbar und einfach für große und komplexe Organisationen

Produktivität ohne Risiken

Genießen Sie alle Funktionen bekannter Kollaborationsplattformen, ohne die Gefahren von kompromittierten Sicherheitsdesigns. Die Lösung lässt sich ganz nach Ihren Bedürfnissen konfigurieren.

Wire ist die einzige Arbeitsplattform, die Sicherheit und Produktivität in einer Anwendung vereint

Open-Source-Transparenz

Vertrauen Sie nicht nur uns. Der Quellcode von Wire ist auf GitHub verfügbar und wird häufig von unabhängigen Stellen überprüft.

Von Grund auf transparent: Die einzige Kollaborationsplattform, die von der deutschen Regierung unterstützt wird

Zero-Trust-Architektur

Alle Daten werden vollständig authentifiziert, autorisiert und verschlüsselt, bevor der Zugriff gewährt wird

Niemals vertrauen, immer verifizieren – Schutz vor Betrügern und anderen schlechten Akteuren.

© 2025 Alle Rechte vorbehalten

Weitere Informationen finden Sie unter: **wire.com/de/sicherheit**