Wire **for Public Safety & Emergency Services**

Wire is a secure communications platform built to meet the demanding needs of public safety and emergency services organizations. With end-to-end encrypted audio, video, messaging, and file sharing, Wire ensures frictionless collaboration while adhering to the highest security standards. Designed for mission-critical operations, Wire empowers “bluelight” teams with fast, seamless, and dependable communication—helping them respond effectively while maintaining the privacy, resilience, and data protection required by Public Safety and Emergency Services organizations.

wire

Wire - Where Security and Reliability Meet

By their nature, public safety and emergency services (Ambulance, Police, Fire & Rescue) need highly secure, real-time, and reliable communication to deal with emergencies, protect sensitive information, and coordinate multiple teams dealing with fast-evolving situations. The high-risk nature of these “Bluelight” operations means that security breaches, eavesdropping, or unauthorized access can have serious consequences. And the sensitive and private information being shared also needs to be properly safeguarded. However, security and privacy can never come at the cost of useability when every second counts.

With **Wire**, secure communications never comes at the expense of useability. The platform provides the latest end-to-end encryption, decentralized architecture, and compliance with strict security and data privacy regulations (GDPR, ISO, NIS2.), making it ideal for emergency services – and best of all, that security is absolutely invisible to end users–who simply experience a powerful, easy-to-use, communications channel they can depend on when they need it most.

10+
Years of experience

>1800
Customers world wide

Zero
Knowledge Architecture

100%
Ease of use

[1]* Messaging Layer Security (MLS) is the only global open standard for end-to-end encrypted communication. Wire, along with other organizations like Meta, Google, Mozilla, Oxford University, co-founded MLS as the standard for next-gen information security and efficiency for groups in the tens of thousands.

© 2025 All rights reserved

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

Key Features - Public Safety & Emergency Services

Secure, Encrypted, and Seamless Communication

Always-On End-to-End Encryption
All features - chat, conferencing, file sharing, reactions, and message timestamps – are always end-to-end encrypted via MLS*. Whether sending a location, a GIF, or a document, only the intended recipient can access the information. Team admins and operators have no access to any of the information shared, enabling them to manage the team without risking sensitive information.

Multi-tenancy
Maintain separate teams within the same server infrastructure while ensuring role-based segregation. Each team stays secure and operates without disruption.

Federation
Communicate seamlessly with other organizations via Wire's federation capabilities. Each organization can have its own independent Wire instance with administrative control, but seamless connections can be made through a Wire federation. Administrators can regulate federation access and control search visibility, allowing options such as no search, exact handle, or email address only.

Secure Location Sharing
The ability to track and provide close coordination of members from multiple services via Wire without running the risk of exposing that location data is a key capability for public safety and emergency services organizations.

Out of Band Communications
Out-of-band (OOB) communication is used when primary channels are compromised or at risk. Wire supports OOB communication by providing separate, pre-established encrypted channels that can be activated in case of cyberattacks, insider threats, network failures, or covert operations.

* Messaging Layer Security (MLS) is the most advanced, open standard for end-to-end encrypted group communication. Wire co-founded MLS and is the only collaboration suite that fully implements it by default across all products, capabilities, and features.

© 2025 All rights reserved

Real-World Use Cases

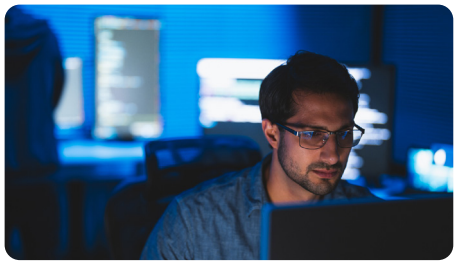
Major Traffic Accident Response
(Dispatch & Coordination)

A **15-vehicle pile-up** on a motorway requires **ambulance, police, and fire & rescue** services.

- → Dispatch centers coordinate response **via Wire's secure group calling**, ensuring all units receive real-time updates
- → Paramedics send live video calls from the scene to hospitals to prepare for incoming casualties
- → **Fire & Rescue** service receives **blueprints** of a nearby fuel depot to assess explosion risks

Wire Capabilities Used	How it Helps
Secure Group Calling	Real-time coordination between services
End-to-End Encrypted Messaging	Securely share accident location, patient PII, or hazardous material information
Video Calling	Remote medical triage & assessment
File Sharing	Real-time access to blueprints and hazardous material info

Coordinated Counter-Terrorism Response
(Classified & Sensitive Law Enforcement Operations)



Law enforcement has signalled an active shooter incident with possible links to a **terror group**. The response requires coordination between police, intelligence agencies, special forces and emergency services teams (ambulance and fire).

- → **Inter-organizational comms** are streamlined via Wire federation
- → Officers in the field use **Wire's encrypted messaging** to communicate with headquarters without risk of interception
- → **Real-time location sharing** ensures tactical units operate efficiently
- → **Out-of-band communication** Wire can act as a secure OOB back up to primary tools in case they are compromised

Wire Capabilities Used	How it Helps
Encrypted Messaging	Protects confidential data from cyber threats
Secure Location Sharing	Real-time tracking for tactical teams
Multi-Device Synchronization	Access messages and files securely from any device
Out-of-Band Communications	Use alternative secure channels in case of compromise

© 2025 All rights reserved

Stroke Patient Emergency Transfer
(Secure Medical Data Exchange)

A 55-year-old woman has a critical stroke and needs rapid response at the ER of a specialist hospital.

- → **Paramedics use Wire to share real-time patient vitals** and medical history with hospital specialists
- → **Doctors on-call join an encrypted video conference** to assess the patient before arrival
- → The system supports **secure file sharing of medical images and test results** without HIPAA/GDPR violations

Wire Capabilities Used	How it Helps
Secure Messaging	Securely share patient vitals and medical history
Encrypted Video Calling	Remote consultation with specialists
File Sharing	Transfer of medical reports and test results
Compliance with GDPR & HIPAA	Ensures full privacy protection

Wildfire Evacuation Coordination
(Disaster Response & Large-Scale Emergency Management)

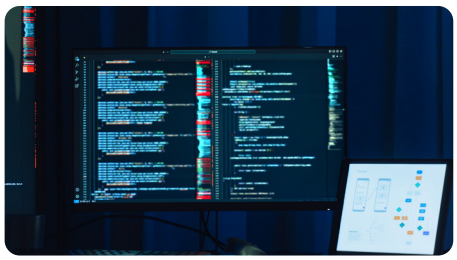
A **fast-moving wildfire** threatens multiple communities, requiring a coordinated response from fire & rescue, police, and emergency response teams.

- → Teams **use Wire's group calling feature** for live updates on fire spread and evacuation orders
- → Emergency responders in remote areas rely on **Wire's offline message queuing**, ensuring they receive updates when connectivity is restored
- → **Secure file sharing** enables the transfer of drone footage, satellite images, and fire containment strategies

Wire Capabilities Used	How it Helps
Secure Group Calling & Messaging	Real-time coordination
Offline Message Queuing	Ensures message delivery in poor connectivity areas
Secure File Sharing	Enables data-driven decision-making

© 2025 All rights reserved

Preventing Internal Data Breaches
(Cybersecurity & Insider Threats)



After receiving some credible evidence, police officers **investigate a high-profile corruption case** involving government officials suspected of exfiltrating state secrets and selling them to criminal organizations. Concerns arise that internal leaks may expose the investigation to criminals.

- → Investigators use **Wire's secure channels instead of official networks** to communicate safely
- → **Wire ID Shield** ensures that only verified personnel can access critical data

Wire Capabilities Used	Function
Zero-Trust Security Model	Protects against insider threats
End-to-End Encryption	Ensures conversations remain private
Wire ID Shield	Prevents unauthorized access
Secure Guest Access	Allows vetted external experts to contribute securely

Multi-National Anti-Trafficking Investigation
(Cross-Border Security Operations)

A **human trafficking network** operates across Germany, France, and the UK. To shut it down and minimize the risk to the victims, multiple levels and jurisdictions of law enforcement will need to work in lockstep with complete secrecy to shut it down.

- → Law enforcement **agencies collaborate securely** via Wire
- → Case files, suspect lists, and forensic evidence are shared using Wire's encrypted file transfer
- → Live video calls with police chiefs and intelligence agencies ensure real-time updates

Wire Capabilities Used	How it Helps
Interoperable Secure Messaging & Calls	No reliance on local telecom networks
Encrypted File & Evidence Sharing	Prevents leaks of confidential information
Out-of-Band Communications	Ensures mission success even if primary channels fail

© 2025 All rights reserved

Ensuring Secure Mission-Critical Communications

Wire ensures **secure, encrypted, and real-time communication** for Bluelight services, addressing mission-critical needs in emergency dispatch, counter-terrorism, medical response, disaster management, and cybersecurity. With advanced security features, Wire **protects sensitive data, enhances coordination, and ensures resilience against cyber threats.**

The Wire Secure Communications Promise

No matter the use case, Wire always brings you these benefits

E2EE Everything

Next-gen End-to-end encrypted (E2EE) makes security invisible and easy for large and complex orgs

Every piece of data is encrypted, no one – not even Wire – can access your content

Productivity without Risks

Enjoy all the features of well-known collaboration platforms, without the pitfalls of compromised security design choices, and it's configurable to meet your needs

Wire is the only workspace that provides security and productivity in one app

Open Source Transparency

Don't just "trust us", Wire's source code is available on GitHub, frequently independently audited

Transparent by design, the only collaboration platform endorsed by the German government

Zero Trust Architecture

Every piece of data is fully authenticated, authorized, and encrypted before granting access

Never trust, always verified – protects against impersonators and other bad actors

© 2025 All rights reserved

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