Wire **for National Security**

Wire is a comprehensive secure communications platform for National Security agencies. Wire provides integrated and frictionless productivity with audio and video conferencing, messaging, and file sharing protected by industry-leading security and end-to-end encryption. Wire enables fast, efficient, and secure collaboration, balancing user-friendly productivity with the stringent secrecy, resilience, and data protection that agencies require. Wire is open-source, and based on zero trust architecture.

wire

High Security Meets Productivity

National security teams uphold internal security and law enforcement, requiring secure collaboration tools to protect the nation's most sensitive information across a vast, distributed workforce. Local and state offices need to be able to maintain their data independence while maintaining secure communication with counterparts and central command. Information must be compartmentalized, ensuring only authorized personnel access sensitive discussions.

When exchanging information and files both security and efficiency are essential. It must be easy for employees to get and stay productive while knowing which spaces and colleagues are approved to discuss sensitive topics. Finally, all communications must comply with privacy and other national regulations.

Wire eliminates these challenges by providing an always-on, end-to-end encrypted and easy-to-use collaboration platform. It is the only enterprise-class solution secured at scale by the Messaging Layer Security (MLS) standard[1], while ensuring end-to-end encryption, privacy compliance, and support for thousands of teams.

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.

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

Key Features for National Security

Powered by Messaging Layer Security (MLS)

Always on End-to-end encryption
All features - chat, conferencing, file sharing, reactions, and message timestamps - are always end-to-end encrypted. Whether sending a location, a GIF, or a document, only the intended recipient can access the information. Secure file sharing eliminates the need for physical copies or outdated systems like fax machines.

Administrator and Operator Shielding
Organizational administrators can manage users easily from Wire Team Management, without needing access to user communications, conversations and history. If an administrator account is compromised, the contents of team members' work is protected from unauthorized access.

No Specialized Equipment Needed
Wire can be deployed on standard IT equipment, allowing teams to avoid the long purchasing cycles and high costs associated with procuring specialized secure servers.

Federation
Each agency can operate their own independent Wire instances with full administrative control while enabling seamless connections through Wire federation. Users across different backends can communicate as if on a shared infrastructure, ensuring external parties cannot identify federated users or backends. Administrators can regulate federation access and control search visibility, allowing options such as no search, exact handle, or email address only.

ID Shield
Wire ID Shield offers an additional layer of protection to ensure that employees are communicating with the intended person. Automatic device verification through the organization's Identity Provider (IdP) allows teams to certify, renew, or revoke the verified status of a user's device. Status displays within conversations and calls show who is joining on a trusted device.

Real-World Use Cases

Operational Coordination & Incident Response
Agencies can rely on Wire to help coordinate rapid responses during active incidents—such as riots, protests, or terror threats – ensuring that real-time instructions and updates remain confidential and tamper-proof.

Interagency Collaboration & Data Sharing
Multiple units (e.g., local police, federal law enforcement, and forensic teams) often need to exchange sensitive case details and intelligence. Wire allows for cross-jurisdictional collaboration while maintaining strict data integrity and privacy.

Secure Evidence & Intelligence Transmission
Transmitting sensitive evidence, digital forensics, and investigative intelligence requires robust encryption. Wire ensures that evidence shared between labs, prosecutors, and operational teams is protected from interception or tampering.

Covert Communications for Undercover Operations
Undercover agents and covert operations demand an extra layer of security to protect identities and methods. Wire protects communication even when traffic is intercepted, safeguarding both personnel and operations.

Crisis Management & Emergency Command
During high-stress situations like natural disasters or coordinated criminal activity, Wire secure communications can facilitate reliable command and control. This ensures that all team members receive accurate, secure instructions without delay or compromise.

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