

// THE WICKR PRO DIFFERENCE

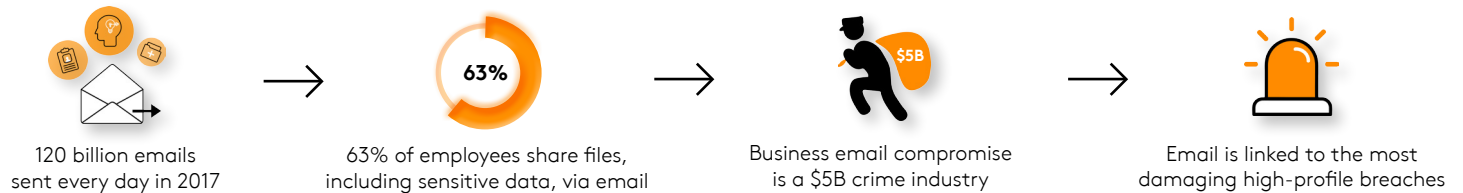
SECURE // EPHEMERAL // AVAILABLE

WickrPro is a vetted, simple to use platform built by an expert security team to protect high-value sensitive communications & files. Messages, large files, calls and video conference. All end-to-end encrypted. All ephemeral.

User data is encrypted on the sender's device and only the recipient can access it. Nobody else has the keys to decrypt your messages or documents, including Wickr. Your communications are not stored on a server. You control how long each message and file lives. Always.

Visit www.wickr.com for more information









We send about 120 Billion business emails per day. Email is still where companies share their most valuable corporate data, discuss high-profile acquisitions, trade secrets and IP. How safe is your information and what can you do to protect your digital assets?



“Wickr allows companies and organizations to bring the security and privacy of a face-to-face conversation to digital collaboration.”

— Thomas Tull, CEO of Tull Investment Group & Founder of Legendary Entertainment

WICKR PRO FEATURES AND CAPABILITIES

-  **1:1 AND SMALL-GROUP MESSAGING**
End-to-End encrypted ephemeral conversations
-  **PROVISIONING & ADMIN CONTROLS**
Easy on-boarding // secure private network deployment in minutes
-  **SECURE ROOMS & CROSS-NETWORK COMMUNICATION**
Invite teams to communicate & collaborate
-  **ADVANCED LAYERED SECURITY**
No third party including wickr can access user messages
-  **FILE TRANSFER**
End-to-End encrypted ephemeral files up to 5GB
-  **CONFIGURABLE EPHEMERALITY**
Messages are not accessible beyond set expiration or burn-on-read time
-  **VOICE, VIDEO & SCREEN SHARE**
End-to-End encrypted calls & video conference
-  **PERFECT FORWARD & BACKWARD SECRECY**
New key generated for every message

WICKR DIFFERENTIATORS

	Wickr
End-to End Encryption/ Crypto with 256-bit secure, FIPS 140-2, NSA Suite B compliant	✓
Ephemerality by Default	✓
End-to-End Encrypted Group Messaging, Calling, Video Conferencing, Screen Sharing and Audio Memos	✓
Peer to peer Group Management Protocol <ul style="list-style-type: none"> - Defends against attacks aimed at manipulating group membership 	✓
End-to-End Encrypted Large File Sharing (5 GB)	✓
Message Recall <ul style="list-style-type: none"> - Delete message from both sender and recipient device 	✓
Starred Messaging (for easy follow up)	✓
User Verification	✓
Federated messaging for secure communications outside of your network	✓
Perfect Forward Secrecy	✓
White Label for Customized UI <ul style="list-style-type: none"> - Customer may personalize with their brand, logo, etc 	✓
Single Sign On <ul style="list-style-type: none"> - Easy adoption and provisioning - Convenience of onboarding and security of offboarding 	✓
Multiple Levels of Ephemerality <ul style="list-style-type: none"> - 365-day max Time to Live in Wickr Pro and fully customer defined with Wickr Enterprise - Additional Burn on Read capability within Wickr per each message 	✓
Enterprise Administrative Controls <ul style="list-style-type: none"> - Powerful management of users, groups, rooms, auto-provision and de-provision to stay within policy guidelines set by customer - Strong account access control options: Wickr password or cryptographic keys - Compliance/data retention (Wickr Enterprise) 	✓
Integration via Bots and APIs <ul style="list-style-type: none"> - Extend Wickr to additional workflows in existing customer applications - Implement scenario-based data sharing/reporting with third parties and affiliates 	✓
Single-Tenant, Multi-Tenant and Customer Hosted Deployment Options	✓
Enterprise-Level Support	✓
iOS, Android, Windows, OS X and Linux Clients	✓