lochbox

CYBERSECURITY COMMUNICATIONS

More than just another messenger or meeting tool, Lochbox is a cybersecurity essential that gives you exclusive control over your organization's encryption keys.

🔑 Encryption

Just because something is encrypted doesn't actually mean it's protected. Most service providers have access to your encrypted content *and* its decryption keys. We remove ourselves and any of our potential vulnerabilities from the equation by giving you sole custody of your encryption keys. Greater control by you = greater security.

🛡 Compliance

The data security standards of your industry were created to protect your company and those you work with in some way. Unfortunately, such guidelines often include vague minimum requirements that can simplify compliance but leave you exposed. Lochbox exceeds the secure communication standards for HIPAA, SOC2, Sarbanes-Oxley, and more, so you can rest assured that your privileged conversations stay that way.

🔒 Remediation

Using unsecured channels to communicate after a cyber attack compromises remediation efforts by leaving you vulnerable to persistent threats. Lochbox gives you absolute control of your communications to ensure only those authorized by you have access to the conversations.

Download on the **App Store**

GET IT ON **Google Play**

GET IT IN YOUR **WEB BROWSER**

Key features

- Control of your encryption
- 1:1 and group messaging
- Voice and video calls
- Meetings
- Administrative controls
- User permissions
- Invite-only access

Zero Trust Architecture (Us vs. Them)

	Lochbox	Slack	WhatsApp	Signal	Telegram	Microsoft Teams
A	✓					✓
B	✓	✓			✓	
C	✓			✓		
D	✓	✓		✓	✓	✓
E	✓	✓				
F	✓					
G	✓	✓				✓

A) **Independent device tracking** - Tracking of the device, not just the user.

B) **Two-factor authentication** - Allows the use of third-party authenticator apps.

C) **No cross-device sessions** - All device sessions must be independently validated.

D) **Encryption at rest** - Content is encrypted on service provider's servers.

E) **Independently controlled key server** - Encryption key access is under the sole discretion of the account owner.

F) **Requires mTLS** - Both user and server require mutual verification of each other's TLS certificate.

G) **Industry security compliance** - Meets major security/privacy compliance standards like HIPAA, Sarbanes-Oxley, etc.