WORKSTORM

On-Premises Deployment

At Workstorm, privacy and security is our highest priority, starting from the moment you deploy.

Hold the keys to your data

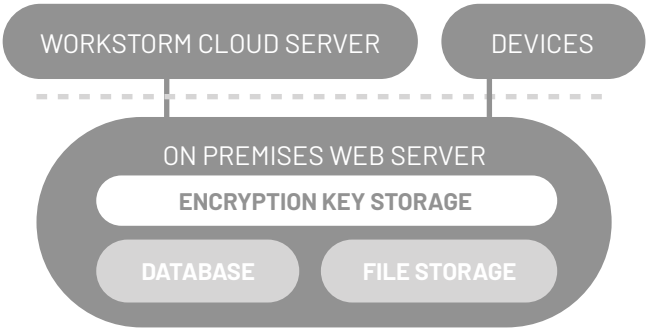
In addition to encrypting communications at rest and in transit, our on-premises solution provides an additional layer of encryption using your locally stored key. That means you have full physical and exclusive control of your data, and neither Workstorm nor anyone else can ever access it.

How It Works

True end-to-end encryption and enterprise-class control paired with our seamless collaboration platform stands up to the most stringent security requirements.

Hardware that safeguards

Workstorm's on-premises solution features locally hosted services that interact with client devices and Workstorm's cloud servers. Database and server access credentials are encrypted, stored locally and never shared with Workstorm.

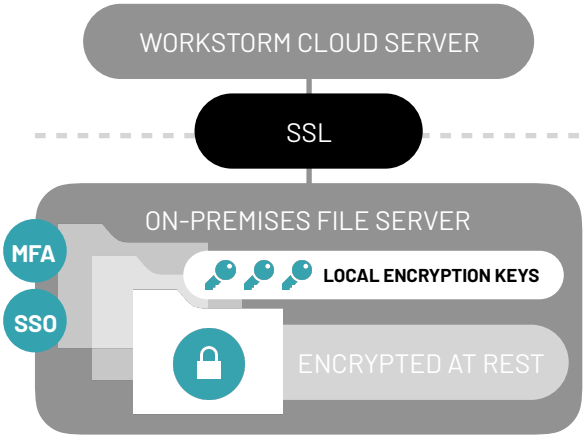


Fully encrypted message and file sharing

Files and messages are encrypted at rest with AES256 bit encryption, with an additional layer of encryption using your locally stored RSA 2048 bit encryption key. Communication in transit between servers and clients is encrypted with SSL TSL 1.2 protocol. All messages are stored on the on-premises server.

Secure file storage

Files are saved within the on-premises SFTP storage system. These files are encrypted at rest with your own encryption keys, so the contents remain hidden from Workstorm and everyone other than the intended recipients.

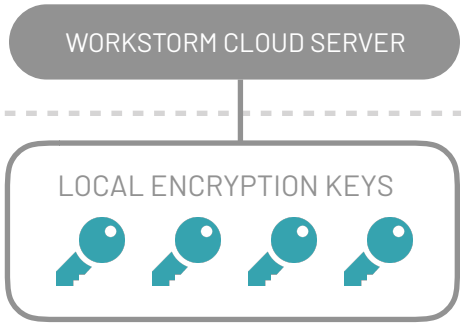


Search securely

With Workstorm, your data stays your data. Unlike other collaboration providers, we never store a temporary index on our servers or hand off your local encryption keys to any service or application. Thus, in the event of a cloud server security breach, your valuable data has zero risk of exposure because it is never there.

Gain control without losing performance

Some collaboration solutions require you to provide your encryption keys to access certain features. With Workstorm, you can access all the tools you need to collaborate – like persistent messaging, videoconferencing and project management – without sharing your key and putting data at risk.



Robust data controls

Built for the needs of highly regulated industries, Workstorm offers features like multi-factor authentication, single sign-on, mobile device management, configurable data retention settings and eDiscovery integrations, and complies with SOC 2 standards for secure software development.

- CUSTOM DATA RETENTION
- SOC 2 COMPLIANT
- EDISCOVERY INTEGRATIONS

Don't settle for subpar security

Maintain control of your data while keeping collaboration free-flowing – the way it should be. To explore on-premises deployment for your own firm, schedule a consultation today at workstorm.com

WORKSTORM