Privacy and Security of Teamwire

Intro

Teamwire is a secure and completely encrypted enterprise messaging solution. As a German company, Teamwire fully complies with strong data protection needs. The solution can be managed for the whole organization and deployed on-premise or in the cloud. This whitepaper outlines all privacy and security features of the service.

COMPLETE ENCRYPTION

Encrypted Messaging

All messages and digital content get automatically encrypted by the sender, and only after the transmission decrypted by the receiver (AES 256-bit and other secure algorithms).

Encrypted Meta Data

To protect against eavesdropping and man-in-the-middle attacks, the meta data together with the encrypted messages get encrypted before the transmission (AES 256-bit). Only the app and the servers can decrypt these data packages.

Encrypted Transmission

In addition, to protect the connection between the app and the servers, all communications are securely transmitted and encrypted via high-grade HTTPS (SSL 256-bit with Perfect Forward Secrecy).

Encrypted Storage

Teamwire uses state-of-the-art technology for secure data storage. All messages, digital content and user data on the servers are stored encrypted with the Advanced Encryption Standard (AES 256-bit).

STRONG PRIVACY PROTECTION

Anonymized User Data

We value your privacy and treat your data absolutely confidential. Teamwire anonymizes personal data as far as possible.

One-way Encrypted Passwords

All IDs, telephone numbers, email addresses and passwords are hashed and salted before they are stored on the servers (SHA-256 and other secure algorithms).

Multi-factor Authentication

Teamwire users need to verify their email address and phone number, before they can access their company domain and can communicate with colleagues and teams. Multiple factors are permanently validated to authenticate a user.

Privacy Built-in System

Teamwire has been made for messaging and sharing privately with your colleagues and teams. The app is a dedicated tool for the internal communication only. Everything is private, and there is no way to share publicly.

No Complicated Privacy Settings

There are no complicated privacy settings for the user to understand or to configure: The user chooses recipients for a message. Then the message is sent exclusively to these recipients. It doesn't get easier than that.

No Address Book Storage

Teamwire does NOT store or know your address book. Before we find your colleagues, the required data gets converted to anonymized values (SHA-256). Afterwards this data is immediately deleted from the servers.

SECURE INFRASTRUCTURE

Private Cloud or On-Premise Deployment

No matter if an enterprise pursues a cloud or on-premise strategy for its IT infrastructure, Teamwire is the perfect solution: Customers can choose between a public cloud, private cloud (with dedicated servers) and an on-premise deployment.

ISO-27001 Certified Data Centers

All data centers of Teamwire are ISO-27001 certified. The data centers offer excellent network connection, employ 24/7 security personnel and video surveillance, enforce strict physical access policies and controls, and are even fully equipped for emergencies (e.g. a power outage).

Comprehensive Network Protection

The Teamwire network is constantly monitored (24/7) and undergoes frequent threat assessments to ensure data protection. The servers reside behind robust firewalls that selectively grant access to resources.

99,9% Uptime Guarantee

Teamwire employs multiple servers in multiple locations to guarantee high availability and low latency. Teamwire is operational and available at least 99.9% of the time in any

calendar month and year.

Strict Security Policies

Teamwire treats data absolutely confidential and enforces strict company-wide security policies in order to limit and prevent access to its infrastructure, data centers and systems.

Internal and External Audits

Teamwire regularly runs audits including vulnerability scans and penetration tests. We also work with third-party firms, security associations and hackers for in-depth security reviews.

FULL DATA PROTECTION

Data Stored on Servers in Germany

Teamwire completely fulfils the data protection needs of European companies. All user data and messaging content are stored on servers in Germany only. (Other server locations are available upon request.)

German Data Protection Laws

Teamwire is a product of a company based in Munich, Germany, and fully complies with strong German and European data protection laws.

Data Economy and Reduction

Teamwire uses as little data as possible to operate, and personal data is only accessed if it is absolutely required for administrative and security reasons.

Secure Backup of Data

All data is written synchronously to multiple servers, backed up regularly, and stored encrypted in multiple locations.

Deletion of Older Content

Possibly confidential information is not stored longer than needed. If requested by the customer, delivered messages and older content are deleted regularly from the servers.

Secure Storage on Device

The user data and messages are stored encrypted on the device, in order to protect and separate corporate data.

Secure Integrations

Teamwire made all provided integrations, connectors and APIs to third party solutions by itself. Teamwire fully controls the data transmitted to these third party solutions and there are no uncontrolled data leaks.

PROFESSIONAL IT ADMINISTRATION

Administrator Portal

All users of an enterprise can be managed by IT via an administrator portal. IT can easily invite and administer all users, pre-configure the app, set general communication rules for the company, and monitor the service.

Active Directory and LDAP Support

Since Teamwire offers comprehensive Active Directory and LDAP integrations, users and groups can be smoothly imported from these directories. In addition, changes in these directories can be automatically synced to Teamwire.

White Listing of Users

IT can white list users, teams or units in order to be in full control of the deployment and ensure that only authorised employees get Teamwire access.

Pooling of Users

If required by compliance, users can be pooled in closed circles (e.g. research & development, accounting, investment banking, etc.) to restrict the distribution of confidential content and prevent information leaks.

Pre-Configured Groups

IT can easily define groups for its users with the administrator portal. These groups (e.g. project teams, units, departments) are then available in the Teamwire app, and also lead to a faster on-boarding of users.

Custom Archiving

IT can archive the messages and content of its enterprise for audit-proof via the administrator portal. Depending on the documentation requirements, IT can archive the messaging for specific time spans and user groups.

Multi-Domain Support

Teamwire supports enterprises that use multiple domains. Employees or organizations with different email domains can be directed to the same server of an enterprise. (This works for cloud and on-premise deployments.)

Multi-Tenancy Capability

Teamwire offers an advanced multi-tenancy capability. IT is able to set up and manage individual tenants for different organizations and subsidiaries. Besides an enterprise can appoint super-administrators, who have the rights to manage all their tenants.

MOBILE APPLICATION MANAGEMENT

Blocking Access of Users

IT can easily block the access of a user via the administrator portal, in case an employee leaves the company or a device gets compromised.

Remotely Deleting Content

In data loss prevention scenarios where a device gets lost or stolen, Teamwire allows IT to remotely delete all the content and data of the app.

Company-Wide Policies

IT can set global policies for its users in order to prevent sharing of messages via copy&paste or sending certain digital content (e.g. photo sharing, location sharing, etc.).

Enforcing Passcodes

IT can enforce PIN passcodes for the Teamwire app for all its users in order to implement an additional security layer.

Secure App Tunneling

Teamwire supports secure app tunneling in order to control access and protect the network. This prevents access from unauthorized devices and is often important in BYOD environments.

Registration Token

IT can set a registration token for its devices in order to restrict the access and prevent usage of Teamwire on unmanaged devices.

Enterprise Mobility Management Integration

Teamwire seamlessly integrates in leading enterprise mobility management solutions (e.g. MobileIron and Airwatch). Thus the app can be easily configured, authorized and managed for the whole enterprise, and ensures company-wide IT compliance.

About Teamwire:

Teamwire is a fast, easy to use and secure enterprise messaging app. Teamwire improves the internal communication with colleagues and teams, and increases the productivity of businesses and large corporations. Users can send 1:1 and group messages, post status updates, exchange video and voice messages, and share calendar dates, files and much more. Teamwire fully complies with strong German and European data protection needs and is a completely encrypted solution. The service can be easily managed for the whole organization and ensures company-wide compliance. Teamwire is available for all mobile and desktop platforms as a private cloud or an on-premise solution.

More information: www.teamwire.eu