Privacy and Security of Teamwire

Intro

Teamwire is a secure and completely encrypted enterprise messaging app. As a German company, Teamwire fully complies with strong privacy and data protection needs (incl. GDPR). The service can be easily managed for the whole organization and ensures company-wide compliance. Teamwire is available as a German cloud, private cloud or an on-premise solution. This whitepaper outlines all our privacy and security features.

COMPLETE ENCRYPTION

Encrypted Transmission

To protect the connection between the app and the servers, all communications are securely transmitted and encrypted via high-grade HTTPS (TLS 1.0-1.2 with Perfect Forward Secrecy). The app and the servers negotiate temporary random keys. An attacker who has captured the network traffic will not be able to decrypt it in hindsight.

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). Therefore Teamwire does a Diffie-Hellman key exchange during the registration, based on a secure elliptic curve (Secp256k1). Only the app and the servers can decrypt these data packages.

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). For each chatroom a unique key is generated. These keys are under the control of the customer, in order to enable archiving, multi-device scenarios, big data analytics, API integrations, security functions and similar requirements of enterprises.

Encrypted Storage

In addition, Teamwire uses state-of-the-art technology for secure data storage. All messages, digital content and user data on the servers (private cloud or on-premise) are stored encrypted with an individual key of the customer (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 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 By Design and No Metadata Analysis

Teamwire has been made for messaging and sharing privately with your colleagues and teams. Everything is private, and there are no hidden analysis of the metadata, the users or the communication.

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.

Scalable and Reliable Solution

Teamwire provides redundant cluster setups, that ensure scalability and reliability for enterprises of any size. Teamwire is even suitable for large enterprises and corporations.

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 (incl. GDPR and ePrivacy).

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 (AES 256-bit), 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.

Disabling the Message Preview in Notifications

If an enterprise wants to prevent, that a message preview is transmitted with push notifications of Apple, Google or Microsoft, the organization can deactivate the preview with a company-wide policy for all its users.

Order Data Processing incl. Agreement

Teamwire provides order data processing conformable to law, that is required by enterprises to process personal data of employees, customers and partners. Teamwire offers a comprehensive agreement for order data processing as part of the terms.

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 and user activity.

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.

Multi-Domain Support

Teamwire supports enterprises that use multiple domains. Different email domains can be directed to the same server of an enterprise. Multiple domains can be easily managed in single or grouped views.

Multi-Tenancy Capability

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

Two-Factor Authentication for Administrators

Teamwire offers a two-factor authentication mechanism to access the administrator portal. An IT administrator needs to enter a password and an app-based second factor to access the administrator portal and confidential enterprise data.

Customization of Email Templates

All email templates for the invitation, registration and confirmation can be completely customized. Teamwire provides an easy to use email editor for all email templates in order to localize and change the content and information.

Filtering and Bulk Operations

Administrators often need to perform specific operations for multiple users at once. Teamwire features advanced filtering mechanisms to easily allow transparency and analysis. Moreover Teamwire provides bulk operations for the most relevant user management tasks of administrators.

Usage Statistics

For enterprises it is important to monitor the messaging service and understand user activity. Teamwire provides detailed usage statistics like e.g. activity by hour, monthly active users and messages sent.

MOBILE APPLICATION MANAGEMENT

Blocking Access of Users

IT can easily block the access of a user or a single device 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.

Automatic Roll-out and Registration

The complete roll-out and registration process of the app on devices can be fully automated. That means the whole registration and configuration of the application can be carried out without any user action in order to reduce support and accelerate the roll-out.

Policies for Data Retention Duration

IT can configure global policies for the duration of data retention on the devices of users. All messages and data that are older than the defined duration are then automatically

deleted from the devices. This ensures that confidential communications and sensitive data are not stored on devices longer than required.

Enterprise Mobility Management Integration

Teamwire seamlessly integrates in leading enterprise mobility management solutions (e.g. Teamwire is a partner of MobileIron and Airwatch) and is compatible with many others (e.g. Citrix Xenmobile, IBM MAAS360, Soti). Thus the app can be easily configured, authorized and managed for the whole enterprise, and ensures company-wide IT compliance.

AUDIT-PROOF MESSAGING

Custom Archiving

An enterprise can archive its messages and content for audit-proof and documentation via the administrator portal. An enterprise can archive the messaging for specific time spans and user groups. The archive is only accessible by authorized personnel and is searchable.

Audit Logs

Teamwire provides professional audit logs that give a chronological record of all activities and operations that are relevant for the security, data protection, compliance and administration of an enterprise.

Revisor Access

Teamwire provides a revisor access to its administrator portal. Dedicated auditors, controllers and revisors can get access in order to ensure data protection, labour law and regulatory compliance, but without being able to make changes.

About Teamwire:

Teamwire is a fast, intuitive and secure enterprise messaging app. Teamwire solves the Whatsapp problem of businesses, increases productivity and improves team communication in the messaging era. Users can send 1:1 and group messages, post status updates, exchange video and voice messages, and share photos, locations, calendar dates, files and much more. Teamwire fully complies with strong European data protection and the GDPR, and is a completely encrypted solution. The service can be easily managed for the whole enterprise and ensures company-wide compliance. Teamwire is available for all mobile and desktop platforms as a cloud, private cloud or on-premise solution.

More information: www.teamwire.eu