Brosix Security

Data security is the highest priority at Brosix, enabling us to continue achieving the goal of providing efficient and secure online real-time communication services.

Table of Contents

The Most Important Facts in a Nutshell 2

Content Security 2

User Interface Security 2

Infrastructure Security 2

In Detail 3

Application 3

Firewall Compatibility 3

Content Security 4

Data Compression and Encryption 4

Website SSL Encryption 4

Digitally Signed Software 4

Infrastructure Security 4

Conclusion 4

The Most Important Facts in a Nutshell

Content Security	
Data Compression and Encryption	All content that is shared with the participant in the session is compressed with proprietary compression algorithms. This compressed content can be interpreted only by the appropriate Brosix connection software. Moreover, Brosix never sends data in clear text, but encrypts all data using 256-bit AES encryption.
Website Encryption	All Brosix websites are secured with 128-bit encryption using Secure Sockets Layer (SSL), which is the most widely used Internet standard for securing sensitive web data communications. SSL web server certificates are provided and signed by GeoTrust, Inc.
User Interface Security	
User authentication	Each user has to authenticate upon logon, and the communication between the users and servers is by default compressed, encoded, and encrypted.
Infrastructure Security	
Third Party Access Prevention	We employ state of the art firewalls, network monitoring, and intrusion detection tools. Strict change management is employed and additional internal security policies and procedures are enforced.

In Detail

Brosix provides innovative IM collaboration solutions to companies around the world. These companies use the Brosix products for sales, marketing, training, project management and customer support. Brosix endeavors that its services meet the most stringent corporate security requirements. Brosix assigns data security the highest priority in the design, deployment and maintenance of its network, platform and services. The purpose of this document is to provide information on the data security features and functions that are available in Brosix and inherent in the underlying communication infrastructure. We discuss the following items in this document: application, firewall compatibility, content security, user interface security, and infrastructure security.

Application

The Brosix software communicates with the Brosix servers located in North America using proprietary protocols and data exchange methods. It is impossible to log in a Brosix IM network without the close coordination between the Brosix software and the Brosix servers. The data in a Brosix IM network is transferred using the software, which must establish a connection with a Brosix server. These security features are inherent throughout the private IM network. Each user has to authenticate upon logon, and the communication between the users and servers is by default compressed, encoded, and encrypted.

Firewall Compatibility

The Brosix software communicates with the Brosix servers to establish a reliable and secure connection. When a session is started, the Brosix software determines the best method for communication. The Brosix software connects to the Brosix servers using TCP or http/https protocols over port 80 or 443. In case peer-to-peer connections are blocked, the Brosix software will tunnel all communications. Regardless of the type of connection that is established when the session is started, firewalls do not have to be specially configured to enable Brosix sessions.

Content Security

Brosix provides several controls to prevent sensitive data expose.

Data Compression and Encryption

All content that is shared with the users in the contact list is compressed with proprietary compression algorithms. This compressed content can be interpreted only by the authorized Brosix user. Moreover, Brosix never sends content in clear text, but encrypts all data using 256-bit AES encryption (Advanced Encryption Standard).

Website SSL Encryption

Brosix secures all its websites with 128-bit encryption using Secure Sockets Layer (SSL), which is the most widely used Internet standard for securing sensitive web data communications. SSL web server certificates are provided and signed by Geo Trust, Inc.

Digitally Signed Software

All software components provided by Brosix are digitally signed using COMODO code signing certificates, the leading certificate authority. This ensures the software you run is delivered by Brosix and was not modified by third party.

Infrastructure Security

Brosix maintains a distributed network of high-speed servers. Brosix invests a lot of time and energy into developing, deploying and maintaining a secure environment for our services. We employ state of the art firewalls, network monitoring and intrusion detection tools. Strict change management is employed and additional internal security policies and procedures are enforced.

Brosix servers are located in SAS 70 Type II certified datacenters.

Conclusion

Brosix pays careful attention to the incorporation of security principles and standards in the design and operation of the Brosix infrastructure and services. Data security will remain the highest priority at Brosix, enabling us to continue achieving the goal of providing efficient and secure online real-time communication services.