Brosix Security

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

Table of Contents

Overview

Brosix provides a secure communication tool to businesses and thus help them improve their productivity. By using Brosix our customers are sure their data is protected and not exposed allowing them to focus on their business.

Brosix customers are spread all around the world. They use Brosix products for sales, marketing, training, project management, customer support, collaboration etc. Some of them are subject to regulations like SAS-70, HIPAA and using Brosix they have to meet regulation requirements. Brosix ensures 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: servers, communication channels, applications, end users, brosix staff, firewall compatibility, content security, user interface security, and infrastructure security.

Servers and Infrastructure

Brosix maintains a distributed network of high-speed IM servers. The high-performance servers are located in state of the art secured data centers that meet high security requirements standards.

No customer data is stored on Brosix servers. You can enable an option to track user activity. If Users Activity Log is enabled the data is stored on a secure dedicated server. This option is provided for customers who have to comply with regulations that require them to store records for all their employees' communication.

All servers are subjects to regular backups that are transferred to at least two different geo locations via a secured VPN connection.

Brosix operates a distributed and redundant system. If some server fails, the users are automatically redirected to another server so they can keep communicating securely. Only approved administrators have access to the servers.

Communication channels

Brosix provides several controls to prevent sensitive data exposure while users communicate.

Peer-to-Peer connections

All communication channels established between users are preferably peer-to-peer (directly between the users, not going through a server). If no direct connection can be made between the clients, the communication goes through a Brosix tunnel server. In this case the sender encrypts and the recipient decrypts the data and the tunnel server does not see the original data. The server does not process, nor store the data.

Data Compression and Encryption

All communication channels are compressed and encrypted with AES 256-bit. This compressed and encrypted content can be interpreted only by the authorized Brosix user.

Website SSL Encryption

Brosix secures all its sensitive 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.

Applications

Brosix software communicates with the Brosix servers using proprietary protocols and data exchange methods. It is impossible to log into 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 to authenticate the user. 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 compressed, encoded, and encrypted.

Application security

Brosix client applications are signed with a code signing certificate provided by COMODO which ensures the publisher identity and proves that the application files have not been tampered or changed by third party. They are thoroughly tested to ensure the software quality and stability.

End Users Authenticity

All users that want to use Brosix have to authenticate. Authentication process goes through Brosix secure servers and ensures the users are really who they pretend to be. IM network administrators have full control from their Web Control Panels to: create/delete user accounts, block user accounts, allow/block communication between users, enable/disable application features for users.

Brosix Staff

Brosix staff that has access to the servers is highly motivated, well trained, and aware of customer's security. All of them are highly educated and continue to raise their qualifications every day. Following strict security principles, they strive to provide excellent customers experience.

SAS-70, HIPAA, SSAE 16, HITECH

Since Brosix does not process our customers' financial information we are not subject to SAS-70. Brosix also does not process our customers' health information so we are also not subject to HIPAA.

Brosix provides secure communication channels that our customers use to transfer their information. During the transmission Brosix does not process, change, tamper or in any other way manipulate their data.

Brosix customers who are subjects to SAS-70, HIPAA, SSAE 16, HITECH or any other regulation, can easily meet their requirements.

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 providing efficient and secure instant communication services.