Beam2Support Security

Content

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 Beam2Support connection software. Moreover, Beam2Support never sends session content in clear text, but encrypts all data using 256-bit AES encryption.
 **Website Encryption**	All Beam2Support 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 VeriSign/Thawte.
User Interface Security	
 **Session ID and Session Password**	The host can specify a 9-digit session ID or use a randomly generated 9-digit session ID to uniquely identify the session. A session password can be defined for additional security. Sessions can only be joined with the session ID and the session password if any.
 **Roles and Responsibilities**	There are several roles in a Beam2Support session: host, presenter and participant. The host needs a user name and password and is the only user who can start sessions. The presenter has the capability to share data. The presenter determines what is shared in a session and the level of access that the participant will have during a session. The presentation rights can be handed over. Before becoming the presenter, the participant has to explicitly agree to transmit their computer screen and to grant remote control rights. It is not possible to view or control the computer screen without the explicit consent of the presenter.
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.
 **No Session Data is stored**	Dynamic session content displayed during a Beam2Support session originates only from the presenter's machine. The participant sees only representations of this data. At the conclusion of a session, all such representations dissipate.

In Detail

BeamYourScreen provides innovative web collaboration solutions to companies around the world. These companies use the BeamYourScreen products for sales, marketing, training, project management and customer support. BeamYourScreen endeavors that its services meet the most stringent corporate security requirements. BeamYourScreen 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 Beam2Support 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 Beam2Support software communicates with the Beam2Support servers located in North America and Europe using proprietary protocols and data exchange methods. It is impossible to participate in a Beam2Support session without the close coordination between the Beam2Support software and the Beam2Support servers. The data in a Beam2Support session is shared using the software, which must establish a connection with a Beam2Support server. These security features are inherent throughout the session. Each session is dynamic and involves a handshake between the Beam2Support software and the Beam2Support server, and the communication between these components is by default compressed, encoded, and encrypted.

Firewall Compatibility

The Beam2Support software communicates with the Beam2Support servers to establish a reliable and secure connection. When a session is started, the Beam2Support software determines the best method for communication. The Beam2Support software connects to the Beam2Support servers using TCP or http/https protocols over port 80 or 443. In case TCP connections are blocked, the Beam2Support software will tunnel all communications using http/https. Regardless of the type of connection that is established when the session is started, firewalls do not have to be specially configured to enable Beam2Support sessions.

Content Security

Beam2Support provides several controls to prevent unwittingly sharing data during a session. The presenter can hide the screen at any time to browse through their own confidential files. The presenter can also hide the desktop's wallpaper, the desktop contents, and the task bar.

Data Compression and Encryption

All content that a presenter shares with the participant in a session is only a representation of the original data. In addition, 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 Beam2Support connection software. Moreover, Beam2Support never sends session content in clear text, but encrypts all data using 256-bit AES encryption (Advanced Encryption Standard).

Website SSL Encryption

Beam2Support 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 VeriSign/Thawte.

Digitally Signed Software

All software components provided by Beam2Support are digitally signed using VeriSign/Thawte certificates, the leading certificate authority.

User Interface Security

Beam2Support security is also enforced through a variety of mechanisms exposed through the Beam2Support user interface. The available options depend on the role a session participant assumes.

Roles and Responsibilities

There are several roles in a Beam2Support session: host, presenter and participant. The host needs a user name and password and is the only user who can start sessions. The participant can participate in a session. Both, host and participant can become presenter and show their screens.

Session Parameters

The host can specify a 9-digit session ID or use a randomly generated 9-digit session ID to uniquely identify the session. A session password can be defined for additional security. Sessions can be joined by either entering the session ID manually or by clicking on the join session URL in an email invitation or instant message. In either case, the host must explicitly inform the participant of the existence of the session either by phone or by email.

Host, Presenter and Participant Privileges

Only a host can start a Beam2Support session using a unique user name and strong password. The host has the first level of control in the session and can specify the initial viewing direction. The viewing direction can be switched by both the host and the respective presenter at any time during a Beam2Support session and requires the explicit consent of the participant. The presenter has the capability to share data. The presenter determines what is shared in a session and the level of access that the participant will have during a session.

The presenter may grant remote control permissions. At any point during such a session the presenter can immediately revoke the participant's remote control privileges by pressing Ctrl + F12 on the keyboard or by clicking on the S icon in the system tray and selecting Disable Remote Control. This allows full control over what can occur during a remote control session.

The host may actively request remote control privileges. The presenter always has to explicitly agree to grant remote control rights. It is not possible to control the computer without the explicit consent of the presenter. Both, host and presenter can switch the viewing direction. However, the participant first has to explicitly agree to become the presenter and to show their computer screen. After the participant has become the presenter for the first time during a session, the host can switch the viewing direction even

without the consent of the participant. However, when switching the viewing direction, the host always has to explicitly agree to become presenter. Both, host and presenter can end the session at any time.

Infrastructure Security

Beam2Support maintains a distributed network of high-speed switching servers. Session data originating from the presenter's machine and arriving at the participants' machines is switched – never stored – through the Beam2Support switching server network. No session data is stored on the Beam2Support servers.

There is no need to upload content to the Beam2Support servers prior to a session. Dynamic session content displayed during a Beam2Support session originates only from the presenter's machine. The participant sees only representations of this data. At the conclusion of a session, all such representations dissipate. All that remains of a Beam2Support session is ancillary information like billing records, not a record of the conversation itself.

BeamYourScreen 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.

Conclusion

BeamYourScreen pays careful attention to the incorporation of security principles and standards in the design and operation of the Beam2Support infrastructure and services. Data security will remain the highest priority at BeamYourScreen, enabling us to continue achieving the goal of providing efficient and secure online real-time communication services.