OmniJoin®
meet smarter.

Public Cloud Datasheet

Public Cloud Security

Military-Grade, Secure Web Conferencing

Our cloud-based online service only allows secure connections, and it is constantly monitored. If a secure conference connection cannot be established, the connection fails. This is a major advantage over traditional, hardware-based video conferencing installations whose configuration settings can be changed by remote employees without system monitoring, allowing sensitive information to be sent unprotected over the Internet.

OmniJoin® conferencing transmits all live sharing, voice over the Internet (VoIP), and video over secure, encrypted connections. This is a marked improvement over some solutions that encrypt live sharing, but send VoIP and video data over separate, unencrypted protocols putting your communications as risk.

Worry-Free Online Meetings

- OmniJoin® cloud-based resources are located in secure facilities with restricted physical access.
- End-to-end encryption provides transmission security and all online meeting hosts are authenticated.
- Additional access, user, and feature controls are provided in the OmniJoin® administrative console such as requiring meeting passwords, disabling remote control, and more.

Online Meeting Passwords & Host Controls

Online meeting hosts can select conference passwords, and make them required for conference room entry. In

One cloud-based service.

Two deployment models.

NO special hardware.

OmniJoin® web conferencing from Brother delivers high-quality, highly-secure voice, video and collaboration through web meetings, in our public cloud or your own private cloud. www.omnijoin.com.

Brother International Corporation is one of the premier providers of products for the home, home office and office.

Public Cloud Security

addition to password authentication and other technical measures, conference hosts can control all video, and personally verify each meeting attendee by sight and role call the attendee list. Attendees may be expelled by the host at any time during an OmniJoin® session.

The meeting host can select passwords meeting-wide (typical); or be more specific, and set separate passwords for the host, presenters, and participants. The latter is useful for more formal meetings such as webinars where there are multiple presenters and a large number of participants. Passwords may also be required to download shared documents and recorded meetings when distributed from the OmniJoin® cloud.

IT Security Policy, Firewall & Proxy Compliance

OmniJoin® conferencing uses industry standard ports 80 and 443 for web services and provides proxy and firewall traversal in accordance with most IT security policies. All OmniJoin™ conference connections are initiated by the user from behind his/her own firewall. The service does not attempt any inbound connections. OmniJoin® conferencing operates over secure TCP/IP connections, via the physical, NAT, and proxy routing specified by each user's respective network.

No Unattended Remote Access Features

In scenarios where OmniJoin® remote control features may be used — e.g., with live desktop, application and region sharing — the user is always prompted with a dialog box requesting remote control.