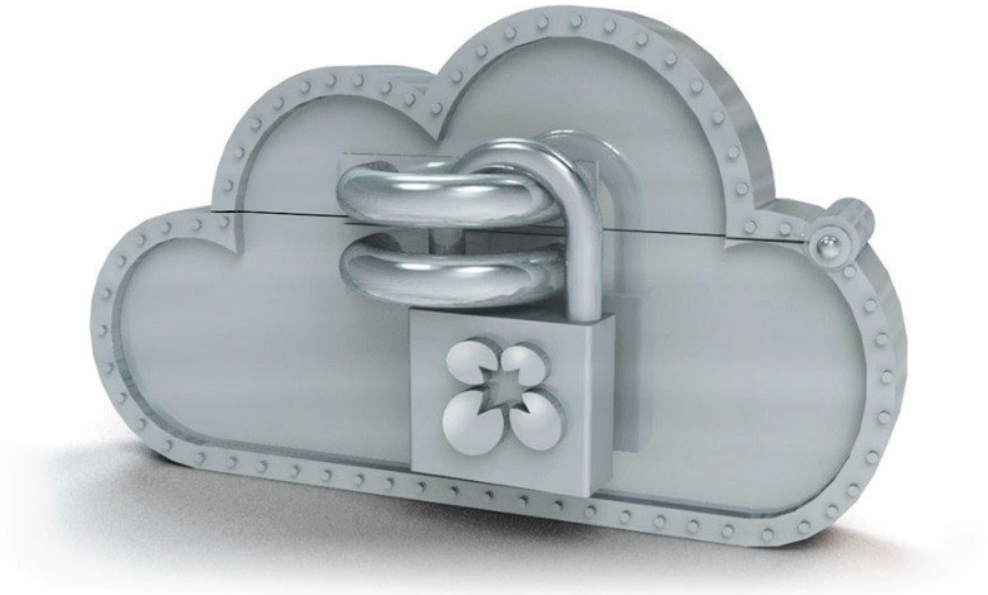


OmniJoin Datensicherheit

[Whitepaper]

IT-Sicherheit in der OmniJoin Cloud

Zertifizierter Datenschutz für Web- und Videokonferenzen

- OmniJoin Public Cloud: Sichere und flexible Nutzung der Brother Cloud ohne großen Aufwand.
- OmniJoin Hybrid Cloud: Meetinginhalte und Video-/Audio-Daten werden auf eigenen Servern gehostet (On-Premises).
- OmniJoin Private Cloud: Maßgeschneiderte Lösung, die komplett auf Ihrer IT-Infrastruktur betrieben wird.
- OmniJoin ist kompatibel mit nahezu jeder Hardware und unterstützt VMware- und Microsoft Hyper-V-Serverumgebungen.
- Der Einsatz von zusätzlicher Hardware ist optional. Auch ohne teure Hardware können Sie mit OmniJoin sichere Online Meetings durchführen.

OmniJoin wird in vielen datenschutzsensiblen Branchen mit hohem Bedarf an IT-Sicherheit genutzt, wie zum Beispiel im Gesundheitswesen oder in der Pharmabranche. Wenn Sie branchenspezifische Fragen zum Thema Datenschutz und Sicherheit haben, schreiben Sie uns eine E-Mail oder wenden Sie sich an unsere OmniJoin Hotline:

omnijoin@brother.de | 0800 100 87 56

Adminkontrolle – Public / Hybrid Cloud

Mehrschichtige, zuverlässige Sicherheitsinstanzen und umfangreiche Möglichkeiten zur Konfigurationskontrolle garantieren eine flexible Nutzung und maximalen Datenschutz in verschiedenen Serverumgebungen.

Service Provider Level: Kontrolle von top-down definierten Feature-Sets. Die Einstellungen werden auf Administratoren-Level und auf Userprofile angewendet.

Administrator: Einstellungsoptionen und Features werden vom Firmen-Admin verwaltet und können mithilfe von Gruppen- und User-Profilen einfach und schnell angepasst werden.

Meetingveranstalter: Userebene, auf der zu Online Meetings eingeladen werden und über Teilnehmer-Beschränkungen entschieden werden kann.

Teilnehmer: Ebene, auf der eingeladene Teilnehmer an einem Online Meeting partizipieren und sich via URL-Link mit den vom Admin festgelegten Einstellungen einloggen.

OmniJoin basiert auf der folgenden mehrschichtigen Sicherheitsstruktur:

- Die OmniJoin Cloud: Physischer Schutz und Sicherheit des Netzwerkzugangs
- Kommunikationssicherheit
- Endpunkt-Sicherheit
- Accountauthentifizierung (Active Directory – Single Sign On für Hybrid/Private Cloud)
- Konferenz- und Sessionsicherheit
- Datenschutz der Teilnehmer
- Firewall / Proxy Traversal
- Richtlinien zur Wahrung der Privatspähre

Zertifiziert für: ISO/IEC 27001:2013 Information Security Management System, Nummer der Zertifizierungslizenz: IS 639075

Physische / Netzwerk-Sicherheit – Public Cloud

Die OmniJoin Network Operations Center (NOC) und das OmniJoin Backend sind sichere und geschützte Rechenzentren, die SSAE 16 Type II zertifiziert sind (Bestimmungen für physischen und Remote-Zugang). Die OmniJoin Public Cloud nutzt virtualisierte Server mit Redundanz zu physisch entfernten Rechenzentren. Die entstehende Konfiguration verbessert die Verfügbarkeit von Ressourcen und ermöglicht bessere Möglichkeiten zur Softwarewartung.

Dezentrale Server-Architektur in der Public Cloud

Die dezentrale Server-Architektur bietet stets ideale Bedingungen für Ihre Web- und Videokonferenzen und reduziert die Videolatenz durch die Nutzung von dem geografisch nächstgelegenen Server. Auf Wunsch können alle Online Meetings über eine bestimmte Serverregion, zum Beispiel über den Deutschen Serverstandort, durchgeführt werden.

- Deutschland
- Skandinavien, Großbritannien
- Vereinigte Staaten von Amerika (Ost-, West-, Zentral-Amerika)
- Asien-Pazifik (Japan)

Sie haben die Wahl: Mit der optionalen Festlegung auf einen Serverstandort werden alle Meetinginhalte auf einem Server virtualisiert ohne systemseitige, automatische Serverauswahl. Entscheiden Sie sich für die komplette Server-Architektur wird der bestmögliche Server ausgewählt und dank Server-Failover die maximale Verfügbarkeit garantiert.

OmniJoin Public Cloud vs. Hybrid Cloud

OmniJoin Sicherheitsfunktionen:	Public Cloud	Hybrid Cloud
Durchgängige Ende-zu-Ende-Verschlüsselung	✓	✓
Passwort- und Teilnehmer-Kontrolle	✓	✓
IT-Security-Richtlinien, Firewall- und Proxy-Compliance	✓	✓
Keine unbeaufsichtigten oder remote Zugriffsfunktionen	✓	✓
Installierbar hinter der Firmen-Firewall		✓
Wählbarer Speicherort der Daten und Aufzeichnungen		✓
Zusätzlicher Passwortschutz für Accounts, die keinen Single-Sign-On (SSO) nutzen	✓	✓
Konferenzraum-Richtlinien per Default festlegen	✓	✓
Eigene Sicherheitszertifikate für zusätzliche Verschlüsselung verwenden		✓
Active Directory Synchronisation und SSO aktivieren		✓

Verschlüsselung und Kommunikations-Sicherheit

OmniJoin entspricht den folgenden NIST- & IETF-Anforderungen:

NIST 800-52 Transport Layer Security (TLS) Richtlinien

IETF RFC 5246 TLS/SSL Protokoll, Version 1.2

Alle OmniJoin Konferenzen, OmniJoin IM und Portalseiten-Sitzungen werden mit TLS 1.0, TLS 1.2 Protokollen verschlüsselt. Wenn eine sichere Verbindung nicht hergestellt werden kann, schlägt die Verbindung fehl.

- OmniJoin setzt eine Public-Key-Infrastruktur (PKI) und Drittanbieter-Zertifikate und Zertifizierungsstellen ein.
- OmniJoin verwaltet intern weder Schlüsselpaare noch werden proprietäre Verschlüsselungsmethoden verwendet.
- Dank RSA 256bit AE-Verschlüsselung sind die Verbindungen für alle Kontrollprotokolle und für den Medien-Payload gesichert.

Endpunkt-Sicherheit

Alle OmniJoin Clients verwenden Code Signing-Zertifikate, die mit den Entwickler-Richtlinien von Microsoft Windows, Apple OS X, Apple iOS, Google Store und Mozialle übereinstimmen. OmniJoin Browser-Loader verwenden Zertifikate mit erweiterter Überprüfung, die von den ausstellenden Organisationen (Microsoft, Apple, Google, Mozilla, soweit zutreffend) unterzeichnet werden.

Account-Authentifizierung

Alle OmniJoin Accounts erfordern eine Login-ID und ein Passwort, um sich anzumelden. Für die Login-ID ist eine E-Mail-Adresse erforderlich. Die Account-Passwortkomplexität und -gültigkeit können vom Administrator definiert werden.

Meetingsicherheit / Sicherheit des virutellen Konferenzraums

Alle Verbindungen sind verschlüsselt:

Alle OmniJoin Konferenz-, Instant Messenger- und Webportal-Sessions werden gesichert mit industrie- und branchenüblicher Verschlüsselung.

Für ein OmniJoin Meeting wird eine sichere TLS-Verbindung hergestellt und automatisch über den bestmöglichen virtuellen Konferenzserver (VCS) durchgeführt. Kunden können die automatische Festlegung auf einen VCS umgehen und eine bestimmte Serverregion für ihre Meetings festlegen.

OmniJoin setzt eine Public-Key-Infrastruktur (PKI) und Drittanbieter-Zertifikate und -Zertifizierungsstellen ein. OmniJoin verwaltet intern weder Schlüsselpaare noch werden proprietäre Verschlüsselungsmethoden verwendet.

Der Lizenzinhaber kann optional neben einem Konferenzraum-Passwort auch ein Passwort vergeben, mit welchem die Teilnehmer den Konferenzraum mit einer bestimmten Berechtigung betreten können.

In der rollenbasierten Sicherheitshierarchie sind neben dem Lizenzinhaber auch die Abstufungen „Veranstalter“, „Moderator“ und „Teilnehmer“ möglich. Der „Veranstalter” eines Meetings kann z. B. die Kontrolle über Audio- und Videosteuerung übernehmen und der „Moderator“ erhält die Möglichkeit Freigaben an die restlichen Teilnehmern zu präsentieren.

Ein Online Meeting wird, 15 Minuten nachdem der letzte Teilnehmer den Raum verlassen hat, automatisch „entvirtualisiert“ - nachdem entweder „Konferenz verlassen“/ „Konferenz beenden“ gewählt, keine Aktivität verzeichnet oder die vordefinierte Endzeit für die geplante Konferenz erreicht wurde.

Firewall- und Proxy-Traversal

OmniJoin wurde für Multisite-Netzwerke und NAT, sowie Firewall- und Proxy-Traversale entwickelt. OmniJoin nutzt TLS-Verbindungen auf den Ports 80, 443, 22, 23, 1270 und 37000 (sog. „legacy ports“). OmniJoin nutzt TCP und stellt keine UDP oder andere broadcastorientierte Verbindungen her. Alle Verbindungen werden vom Client außerhalb der Firewall aufgebaut – es gibt keine sog. „Inbound Connections“.

OmniJoin unterstützt Proxy-Authentifizierung-Standards inklusive WPAD, NTLM, Proxy-Autokonfiguration, Socks5 und manuelle Proxykonfigurationseinstellungen. OmniJoin Software beinhaltet herstellerspezifische Proxy-Optimierungen für z. B. Squid Web Proxy, Microsoft® Threat Management Gateway/ISA Server. OmniJoin bietet außerdem Ausweichmechanismen für Proxy-Server ohne installierten Proxy-Client.

Die OmniJoin Verbindungssequenz nutzt verschiedene Ports und Verbindungstypen. In der Regel wird ein höherer Datendurchsatz und direkte TCP-Verbindungen über Port 443 (wenn möglich) bevorzugt.

OmniJoin Meeting- und Collaboration-Kontrolle

OmniJoin bietet mehrere Optionen, um erweiterte Berechtigungen und Freigabetools zu ermöglichen. Diese Optionen sind zunächst nur für Veranstalter verfügbar, bis zu dem Zeitpunkt, an dem der Veranstalter einem Teilnehmer eine andere Berechtigungsstufe (z. B. Moderator) zuweist.

Folgende Funktionsberechtigungen können zugeteilt werden:

- Desktopfreigabe (per drag&drop auf mehrere Bildschirme verschieben)
- Anwendungsfreigabe
- Whiteboard-Freigabe
- Mediendatei-Freigabe
- Freigabe einer bestimmten Region
- Anmerkungsmodus/ Speichern und Drucken

Die Funktionsberechtigungen werden vorab definiert und umfassen, je nach Einstellung des Service Providers und/oder Administrators, unterschiedliche Funktionen und Möglichkeiten.

Meetingveranstalter: Die Veranstalter verfügen und kontrollieren ihren eigenen Online-Konferenzraum und können z. B. jede Datei-, Anwendungs- und Desktopfreigabe beliebig starten. Ist die Fernsteuerungsfunktion aktiviert, kann remote gemeinsam an Dateien gearbeitet werden.

Moderatoren: Je nach Einstellung können Moderatoren bestimmte Freigaben starten und zeigen.

Teilnehmer: Verfügen standardmäßig über keine Meetingkontrolle und können an dem Online Meeting teilnehmen, die gezeigten Freigaben sehen und die anderen Veranstalter und Teilnehmer sehen und hören.

OmniJoin Konferenzplanung

Mit dem intuitivem User Interface können Online Meetings einfach angesetzt werden, um Veranstalter und Teilnehmer schnell miteinander zu verbinden. Mit den offenen Schnittstellen (API) kann OmniJoin in bestehende Softwarestrukturen integriert werden.

Alle virtuellen Konferenzräume können gesperrt werden, sodass alle Teilnehmer in einen Wartebereich gelangen und eine entsprechende Nachricht erhalten. Wenn der Meetingveranstalter den Online-Konferenzraum wieder entsperrt, betreten alle Teilnehmer die Sitzung. OmniJoin unterstützt verschiedene Meetingkonfigurationen, die wie folgt definiert werden:

- Online Meeting mit Registrierung
- Geplantes Online Meeting
- Ad-hoc Meeting

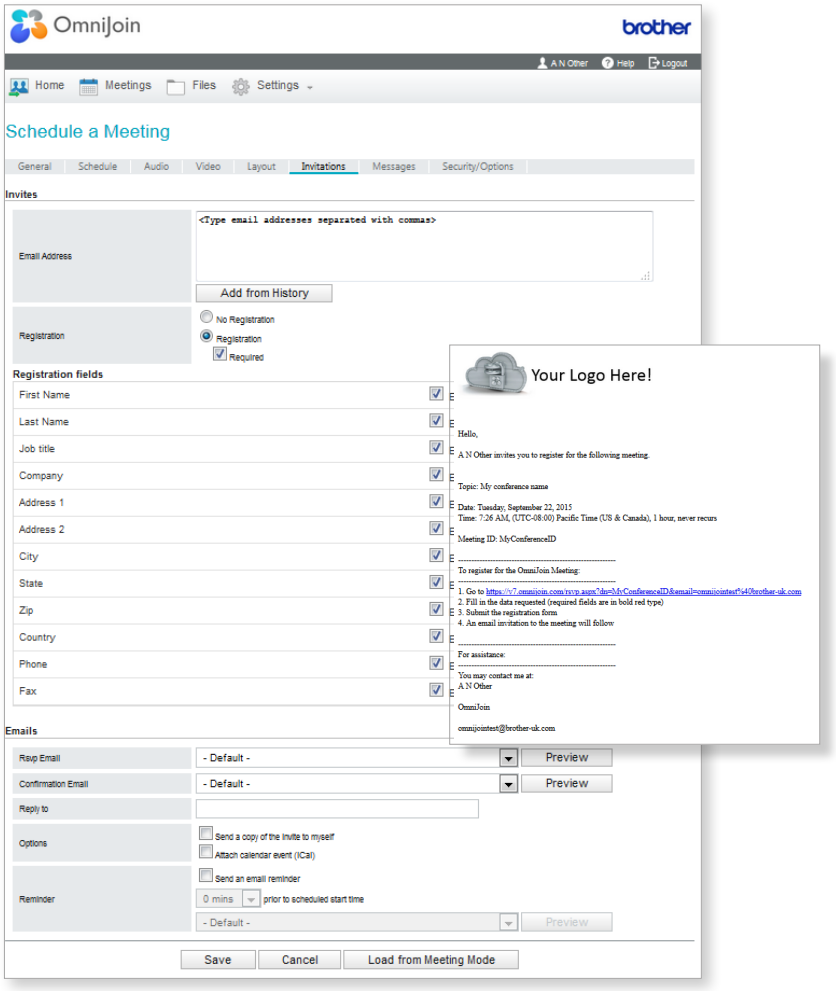
Online Meeting mit Registrierung

Dieses Online Meeting findet zu einer vordefinierten Zeit statt und erfordert von jedem Teilnehmer eine Registrierung, in der Informationen von dem User abgefragt werden. Die Fragen an die Teilnehmer können vorab festgelegt werden. Daraufhin wird eine E-Mail verschickt, in der dem Teilnehmer die Meeting-URL, das Datum und der Zeitpunkt des Meetings mitgeteilt werden.

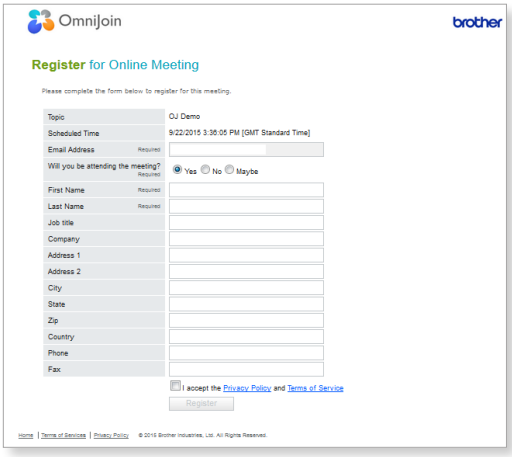
Beispiel: Registrierung

1. Einladungen für Ihr Online Meeting können über das OmniJoin Webportal erstellt werden. Klicken Sie hierfür auf „Zeitliche Planung einer Konferenz“ und nutzen Sie die Einladungs-Vorlage, um die Teilnehmer über das anstehende Online Meeting zu informieren.

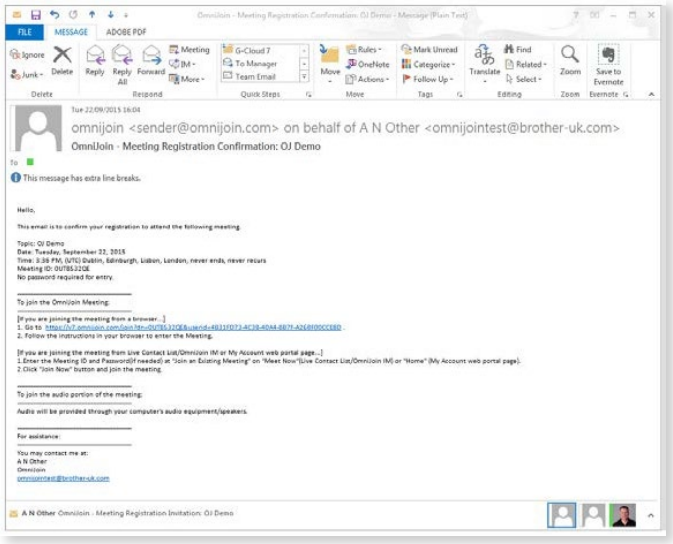
2. Wenn der Veranstalter eine Registrierung zu der Web-konferenz wünscht, kann er definieren, welche Infor-mationen der Teilnehmer angeben muss.



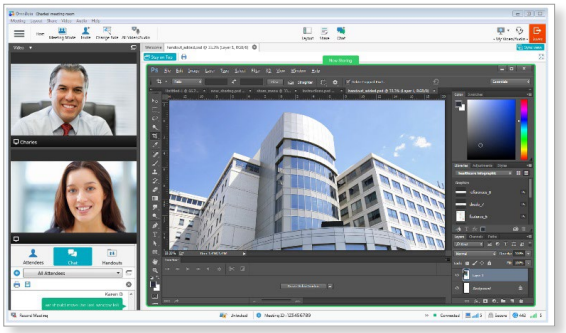
3. Der Teilnehmer erhält den Fragebogen und vervollständigt diesen.



4. Der Teilnehmer erhält die E-Mail-Einladung inklusive Link zum virtuellen Konferenzraumes und dem zugehörigen Passwort (wenn benötigt).



5. Die Teilnehmer klickt auf den Link und kann schnell und einfach, z. B. über seinen Webbrowser, am Online Meeting teilnehmen.



Geplantes Online Meeting

Datum und Zeit werden für diese Meetingart vorab festgelegt. E-Mail-Erinnerungen und Kalendereinträge (iCal) helfen dem Veranstalter bei der Organisation des geplanten Meetings.

Ad-hoc Meeting

Für spontane Videokonferenzen kann in wenigen Sekunden ein virtueller Konferenzraum aufgesetzt und genutzt werden. Auch hierfür können Einladungen via E-Mail verschickt werden und die Teilnehmer gelangen schnell über ihren Browser in den entsprechenden Online-Konferenzraum. Wenn alle Teilnehmer erschienen sind, kann der virtuelle Raum auf Wunsch gesperrt werden.

www.brother.de/OmniJoin