convene
Smart. Simple. Secure.

System Security Features

convene
Smart. Simple. Secure.

Overview

Azeus Convene provides excellent user experience in holding meetings, as well as reviewing, sharing, and collaborating on documents—without compromising security. By using Convene, users can securely access documents, organize meetings, and conduct presentations with mobile devices in both online and offline mode.

Convene is designed and developed with an emphasis on responding to the challenges of enterprises and public services that require data protection, control, availability, and application security. Built with strong encryption mechanisms throughout the system, Convene's web portal allows user administrators to centrally manage user accounts, system policies, and file access rights, and to also monitor system user activities.

At a Glance

- SOC1 (SSAE16 / ISAE3402 / SAS70), SOC2, SOC3, ISO27001, ISO27017, ISO27018 certified cloud hosting.
- SOC2-compliant
- 2048-bit TLS
- AES-256 network and document encryption
- Multiple-factor authentication by device registration
- On-the-fly decryption
- Fine-grained access control
- Automatic purge for lost devices

Infrastructure Security

- Hosting facilities in the United States, Canada, Europe (Ireland), Singapore, and Australia are SOC1 (SSAE16 / ISAE3402 / SAS70), SOC2, SOC3, ISO27001, ISO27017, ISO27018 certified.
- The system is SOC2-compliant.
- Convene is unaffected by the Heartbleed Bug vulnerability (a serious bug found in the open-source OpenSSL cryptography library — CVE-2014-0160).
- Daily automated backups ensure data integrity. Unused or obsolete backups are destroyed and replaced to prevent unauthorized data retrieval.
- Our staff closely and continuously monitors servers in real time to ensure optimum system performance and to protect against any attempted network attacks.
- Convene servers undergo operating system hardening. Login is secured by strict access controls and encrypted access. Administrative access is restricted to authorized personnel only.
- Proxy server support is provided.

Network & Document Encryption

- Wireless network transmissions between Convene and its web portal are encrypted via 2048-bit Transport Layer Security (TLS).
- Documents are always encrypted with AES-256 when stored in Convene's local storage and web portal.

Secured Decryption on Mobile Devices

- Convene uses a secure, on-the-fly decryption model. When the user needs to access encrypted files on storage, only the needed parts are decrypted into memory. In contrast, common encryption software decrypts the whole document and stores its decrypted form on temporary file storage which hackers can access.
- Convene uses automatically-purged local storage for its temporary files. Files are never backed up to iTunes and iCloud.

Key Management

- Data is protected by three-tier key management with random document key, user key, and system key.
- User keys are protected which ensures that even restoring a cloned application image to another device cannot decrypt the user key.
- System administrators only need to keep and manage the system key to control overall security.

User Authentication, Password and Login Session

- Users can log in to both Convene and its web portal with a single user account.
- Strong password policy and password expiration period are enforced.
- Multiple-factor authentication ensures only your registered devices can sign in to Convene to prevent anyone else from accessing your account with an unregistered device.
- Password is encrypted using AES-256.
- Meetings can be protected through the attendee list.
- The system automatically signs out users on session timeout.

Access Right Control

- Access rights can be granted to an individual user or user group.
- Automatic access right inheritance from parent to subfolders and files is applied to ensure proper access right control while minimizing administrative effort.
- User administrators can set individual password protection for specific files and folders.
- User administrators can grant read-only and read-write permissions.
- Access right control includes role-based access permissions to files in the portal and meetings.

Security for Lost Devices

- Authentication prevents unauthorized access to data on a lost device.
- Multi-level encryption keys and key management reinforce key protection, which is important especially when a device gets lost.
- Data on a lost device is automatically purged when password-guessing is detected. When password-guessing is detected, the system automatically locks the dubious user account and wipes out offline data/cache.

Audit Trail

- All login attempts, file uploads and downloads, and file permissions granted to users and user groups are tracked and recorded.

Physical Security

- Physical security of hosting facilities provided 24x7 encompasses all computer and network communication systems.

Information Security

- Information security controls are governed by strict internal access policy involving provisioning and change control. All employees are trained on data security requirements.

Security Testing

- Application and infrastructure penetration testing are performed regularly.