convene

Security features
An overview

At Convene we believe that your trust in our security is an integral part of the user experience.

Our award winning solution was developed in response to private and public service companies that require high level data protection, access control and application security. Built with strong encryption mechanisms, Convene's secure portal allows your meeting administrators to centrally manage your accounts, system policies, file access rights as well as monitor user activities.

Security and Confidentiality
"Full Ownership of Data on Convene. The concern was that if the cloud was hacked, all data could be instantly accessible, so the issue was that we didn't have control.
We are able to control our own architecture, but we would not necessarily know if Convene was ever hacked.
The normal cloud set up involves a lot of different accounts, with 10 computers using the same cloud.
Convene overcame this issue by offering segregated clouds, with master passwords for our IT team. This meant that we could take full ownership of the cloud and take any action if required.."
Kye Pearson - Company Secretary at London Metal Exchange

scroll down for the full report

APPLICATION SECURITY

Convene grants its users full system ownership, from managing user roles and devices to setting system and security preferences. Whether used on a mobile device, tablet or desktop, Convene and all meeting processes are secure from any threats or vulnerabilities.

USER ACCOUNTS AND SYSTEM SECURITY PREFERENCES

Account Management

Easily add and/or remove users from the system, assign them as General Users or System Administrators and divide them into groups for easier meeting set-up and granting of access controls.

Role-based access control

User Roles

Configure system settings, customise access rights and manage user accounts based on User Roles (General User or System Administrator).

Meeting Roles

Define and limit what meeting participants can do during Live Meetings and with the board material by assigning Meeting Roles.

Authenticated Voting

Verify the identity of voters in Meetings and Resolutions on Convene through the use of additional authentication during the voting process.

User Logs and Activities

Track application and Admin Portal activity such as logins, document access, meeting changes, profile updates, etc. System Administrators can also generate usage reports through Convene's Audit Trail.

Offline Logins

Offline logins to Convene are tracked and reported in the Convene Admin Portal.

Password Policies

Ensure account security with customised password policies and password expiration periods.

Password Blacklist

Specify a list of banned passwords to prevent users from using commonly used and vulnerable passwords for their Convene accounts.

Session Timeout and Sign-in Retries
Set session timeouts and limit sign-in retries to prevent unauthorised access to Convene.

Automated Security Alerts
Automatically notify users or System Administrators of an attempted breach in the case where an account has been locked due to an excessing number of invalid login attempts.

DOCUMENT SECURITY & DIGITAL RIGHTS MANAGEMENT (DRM)

Copy Restrictions
Prevent the copying of document content to other applications so as to minimise exposure of user data.

Document Access
Document Library
Limit who can view, download or edit individual files or folders in the Document Library.

Meetings
Assign Meeting Roles to limit who can view, download, forward, export and print specific meeting agenda items and/or documents from meetings with advanced permission settings.

Secure Agenda Contribution
Meeting participants and organisers can be restricted from viewing classified or sensitive agenda items within a meeting.

Scheduled Archival and Disposal
Schedule the archival and/or disposal of documents after a certain time has lapsed to avoid unauthorised access of files in specific Meetings, Review Rooms or Resolutions. Meetings and Resolutions that are marked as closed become read-only.

Watermarks
Selectively add customisable watermarks to Meetings, Review Rooms and Resolutions documents to discourage misuse of sensitive material and to highlight key information such as author, version, and date created or produced. Additionally, automatically add watermarks to documents downloaded (based on user permissions) from the Document Library.

Secure Document Signing

Signing Documents
Securely store and edit a freehand signature in Convene to easily sign documents and other meeting material.

"Enterprise-Grade Security Features Convene's security features also won us over. Information security is very important because we deal with members and their personal data, so we must be vigilant. Everybody has got their own passwords, and as a system admin on Convene, I have fine-grained access control so I can block certain users whenever required. We only use iPads which are required to have a security lock on, so everybody has their own user codes."
Community Trade Union
Anthony Ansar, IT Manager

Authenticated E-Signatures
To prevent signature fraud, Convene requires users to provide their credentials before signing with an E-Signature.

Timestamped E-Signatures
Convene can be set to automatically timestamp E-Signatures, recording the exact moment a document was signed to eliminate the possibility of clerical errors. Furthermore, these timestamps cannot be edited or changed, preventing any inaccuracies caused by tampering.

Multi-Level Encryption
Data stored on Convene is protected with multi-level encryption whether at rest or in transit. *See data right:*

DATA AT REST
_ AES 256-bit encryption

DATA IN TRANSIT
_ RSA 2048-bit Transport Layer Security (TLS)

DEVICE SECURITY

For a more secure mobile experience, Convene has features that protect user data from any vulnerabilities or threats.

On-the-Fly Decryption Model
When a user needs to access encrypted files on storage, only the needed parts are decrypted into memory.

Measures to Secure Lost or Stolen Devices

Remote Data Wipe and Automatic Purge
Remotely delete stored offline data downloaded to a device in case it is lost or stolen. Automatic purging of data can be set when users sign out of Convene or have been offline for a specific number of days, or when password guessing is detected.

Re-Authentication
In the case of lost or stolen devices, session timeouts render data inaccessible unless the device is re-authenticated.

Jailbreak and Root Detection
Convene is able to detect whether a mobile device has been jailbroken or rooted and will not run on these devices. This reduces the risk of bypassing security measures and the exposure of sensitive information.

Additional Protection of Encryption Keys
System Administrators can apply an additional layer of protection for the encryption keys used by the Convene App on specific untrusted devices (e.g. BYOD devices). These devices will require a persistent online connection to Convene to view documents.

Application Masking
Convene is masked when in the background, serving users with a generic screen. This prevents sensitive information or documents from being accidentally disclosed through everyday use (e.g. switching between applications).

SECURE USER AUTHENTICATION

Convene is widely compatible with several authentication methods to suit clients' specific security needs.

User ID and Password
Convene only allows members with registered user accounts to log in to the system using their own unique password.

Biometric Authentication
Do away with the inconvenience of typing login information with Touch ID or Face ID (iOS) or fingerprint scanning (Android) for mobile devices.

Active Directory Integration
Through Active Directory (AD) integration, users no longer have to remember another set of credentials, while organisations can ensure that only registered users have access to Convene. This can be done though Lightweight Access Directory Protocol (LDAP) or Active Directory Federation Services (ADFS).

Single Sign-On (SSO)

SAML SSO
Eliminate the need to repeatedly type in passwords per login through a streamlined single sign-on process using SAML 2.0.

Multi-Factor Authentication

SMS One-Time Pin (SMS OTP)
Receive and enter a one-time verification code—which is securely and instantly delivered to your registered mobile number—before logging in to Convene. Integration with AWS' secure SMS gateway (AWS SNS) is supported.

Device Registration
Selectively restrict access to Convene to previously registered devices and/or browsers.

Time-Based One-Time Password (TOTP)
Use the authenticator application of your choice to secure your Convene account. Authenticator applications supported include Google Authenticator, Microsoft Authenticator and many others.

"Convene works well for us as far as remote working is concerned. Due to COVID-19, forced home working has resulted in people becoming keener to embrace new technology. This has been one benefit that has arisen as a result of this current crisis. Technology is being more readily adopted out of necessity."
Jonathan Jenkins, Chief Executive at London's Air Ambulance

CLOUD INFRASTRUCTURE & NETWORK SECURITY

Enterprise-Grade Cloud Hosting

Convene has partnered up with the leading provider of cloud services in the industry, Amazon Web Services (AWS), to guarantee that client data is protected on all levels.

Amazon Web Services (AWS)

_ Capable of analysing billions of events and continuous streams of meta-data to detect, prevent and defer any form of cyber-attacks regardless of size

_ Ranks highly on platform configuration options, monitoring and policy features, security and reliability

_ Preferred choice of government institutions and multinational companies worldwide

Convene cloud global infrastructure is located in ISO-certified (ISO 9001, 27001, 27017 and 27018) and AICPA (SOC 1/2/3) compliant hosting facilities worldwide which are audited under the SSAE-18 standards. *See data right:*

HOSTING FACILITIES

_ Asia, Singapore
_ Australia, Sydney
_ U.S., North Virginia
_ Canada, Montreal
_ Europe, Ireland

Each physical hosting facility is protected and monitored 24/7 by professional security staff, video surveillance, intrusion detection systems, two-factor authentication, and many more. At the same time, access to the cloud infrastructure is limited to a dedicated access network that requires VPN access and two-factor authentication. Only authorised personnel are provided access to the dedicated access network.

Client data is protected by an additional security layer with AWS' EBS Encryption and is also segmented and stored separately from each other to ensure that data does not leak or overlap. Convene also benefits from the protection of AWS Shield Standard, receiving protection against all currently known infrastructure attacks.

Cloud Data Segregation

Each Convene client has its own single-tenanted environment—with its own set of data schemas that are protected with individual authentication credentials and completely unique keys—to ensure that the client's data is separated from other organisations'. All client environments are protected by security firewalls, with only specific ports and addresses allowed.

Cloud Data Availability

With AWS Cloud Hosting, Convene is able to store client data on multiple availability zones. Each availability zone is composed of at least one data centre with independent power and internet sources to make certain that there is no single point of failure and to provide high availability and durability at all times.

24/7 Intrusion Detection System (IDS)

The 24/7 Intrusion Detection System (IDS) monitors access logs for common malicious attack patterns and notifies the System Team of any suspicious activity.

24/7 Intrusion Prevention System (IPS)

The Convene cloud infrastructure is protected with an Intrusion Prevention System (IPS) that scans traffic and blocks any suspicious activity, including uploads containing malware. Uploaded files are automatically scanned by services provided by Trend Micro.

Backup and Recovery

Daily automated backups are done to ensure data integrity, while unused or obsolete archives are destroyed and replaced to prevent unauthorised retrieval.

SECURITY GOVERNANCE

Defined Security Policies

Documented security policies and procedures are in place to ensure the confidentiality, availability and integrity of the system.

Designated Security Team

Convene's Security Team ensures staff compliance with security policies and procedures, protection of customer data and the regular review of the effectiveness of current security policies and procedures.

Data Processing

Convene's data processing procedures are compliant with the GDPR and are overseen by a Data Protection Officer.

Business Continuity Measures

Convene's Business Continuity Plan ensures that support services operate continuously in order to serve all customers at all times.

Daily Automated Backups*

Customer data is automatically backed up daily to ensure system integrity.

Availability Zones and Data Redundancy*

Convene leverages AWS' (Amazon Web Services) availability zones in its cloud infrastructure to restore services during disaster situations, ensuring high reliability and availability. These data backups are copied to another AWS location within the same region and remain encrypted. The data is stored using Amazon Web Services S3 (Simple Storage Service).

Disaster Recovery*

The Convene System Team conducts annual Disaster Recovery drills to test and improve the Disaster Recovery plan so that the Recovery Time Objectives (RTO) and Recovery Point Objective (RPO) are met.

Incident Management*

Monitored 24/7, Convene's detection mechanism alerts the Support Team to any incidents that are then forwarded to the System Team for immediate resolution. Users can also report any incidents via chat, email or phone.

Vulnerability Management

Convene's servers regularly undergo several security tests and are hardened following security benchmarks from the *Center for Internet Security.*

Internal Security Testing and External Penetration Testing*

The Convene infrastructure is regularly tested and scanned for vulnerabilities by the Convene System Team, and is subjected to external penetration testing by independent third parties. Customers may also request for a copy of the results or perform their own security testing and pass their findings to Convene.

Application Development

Convene was designed, developed, and tested for vulnerabilities against the *Open Web Application Security Project* (OWASP) Top 10 and *Common Vulnerabilities and Exposures program*. Convene's System Team works with the Security Team to perform scans immediately after every major release and implement patch management procedures for critical vulnerabilities (Example: Spectre 2018).

AWS Vulnerability Scans*

AWS performs regular vulnerability scans on the host operating system, web application and databases in the AWS environment. The AWS Security Teams subscribes to news feeds for applicable vendor flaws and proactively monitor the vendor's website and other relevant outlets for new patches.

"We were searching for a tool that was intuitive for our Executive members to use. It was important for our members to be able to access information easily and to share important documents during meetings. It was essential for this to be done securely, so security was a key issue for us."
Xristina Giannopoulou, Piraeus Bank

Personnel Security

All Convene employees are subject to criminal background checks and are bound by an agreement to uphold the company's privacy policy and protect the confidentiality of customer data.

Security Awareness Training

New staff members are required to undergo a security awareness training that discusses common security attacks, social engineering tactics, detection and prevention of attacks and procedures for reporting.

Role-Specific Security Training

Convene developers and system engineers regularly undergo training so that they are updated on industry-standard security practices.

**Security Measures are for Convene Cloud Environments only.*

"What excited me most about Convene was the way it encrypts data on a device. We looked at similar products that did this, but meeting collaboration wasn't their primary function. Yes, we did have a business need that revolved around security but what worked out well for us, when it came to the procurement of Convene, were the add-ons such as digital collaboration, remote meetings, and a meeting pack archive."

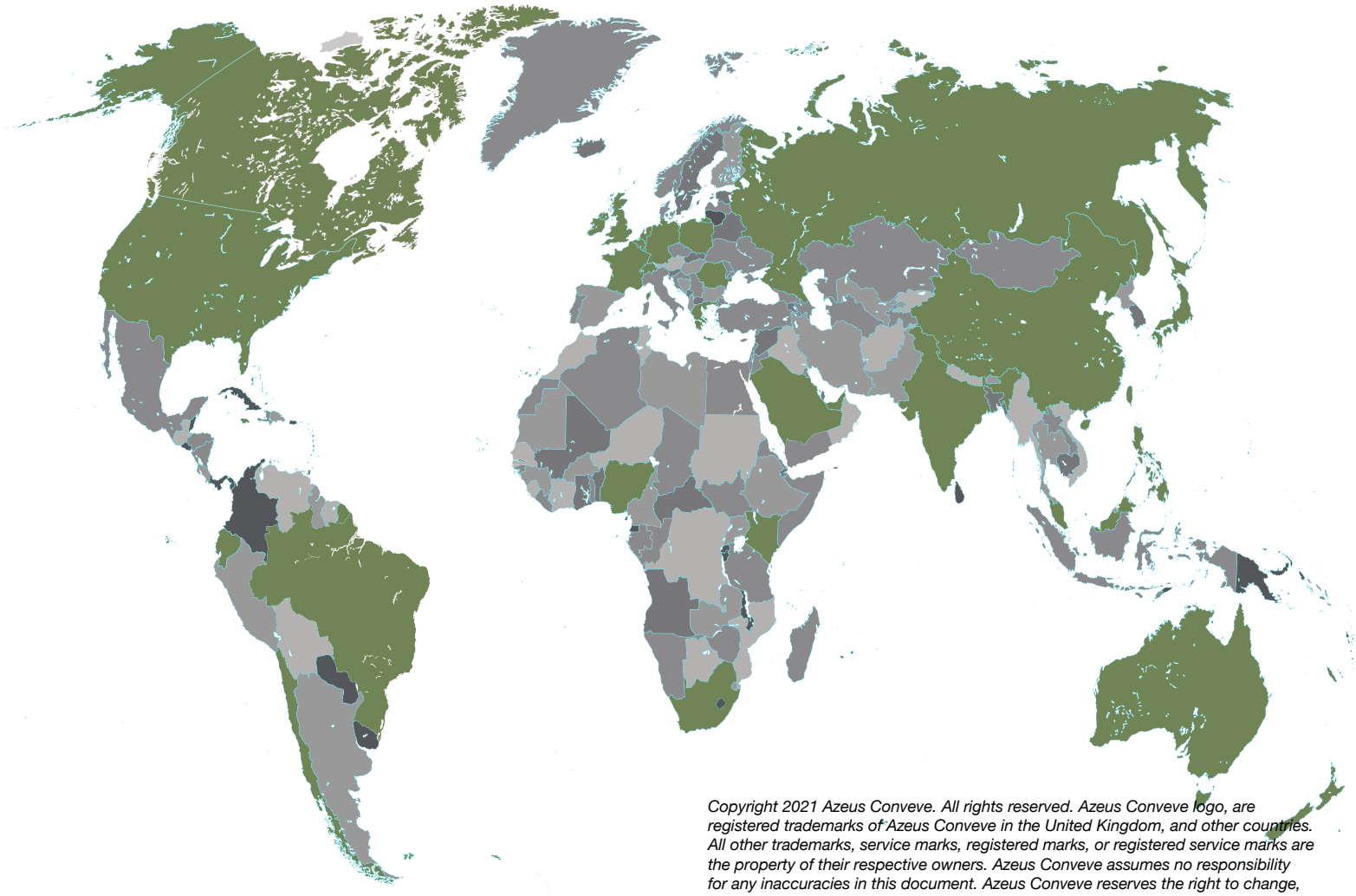
Special Olympics Ireland
Niall Callaghan, IT Manager

Contact:
UK +44 (0)20 3743 2515

sales@azeusconvene.co.uk
azeusconvene.co.uk

Support:

EMEA		APAC		AMERICA	
UAE:	+971 42482947	Australia:	1 800 789 564	United States:	1 800 638 0246
United Kingdom:	0 800 088 5517	China	+86 010-5283 2591	Canada:	1 800 638 0246
France:	+33 01 8626 2736	Egypt	+20 101 466 1004		
Greece:	+30 2111988980	New Zealand:	+64 4830 3496		
Kenya:	+254 20 3892298	India:	000 800 1006 862		
South Africa:	0 800 999 371	Hong Kong:	+852 2152 3666		
Turkey	+90 546 283 93 87	Singapore:	800 852 3335		
		Malaysia:	1 800 817 240		
		Philippines:	+63921 316 0339		
		Nigeria	+234 812 417 9126		
		Zimbabwe	+263 779 080 703		
sales@azeusconvene.co.uk azeusconvene.co.uk		sales@azeusconvene.com azeusconvene.com		sales@azeusconvene.com azeusconvene.com	



convene

Don’t just meet – Convene