CoScreen Security Whitepaper

Secure collaboration for enterprise teams

1. Security at CoScreen

This document outlines the security best practices and frameworks upon which the CoScreen collaboration platform is developed and maintained to keep its customers and their data safe.

2. Infrastructure Security

2.1. Security Standard Compliance

CoScreen does not operate any own physical infrastructure for customer-facing purposes.

CoScreen leverages the fully managed web application platforms Google Firebase and AWS (Amazon Web Services). For further information about Firebase security processes and how they comply with information security standards, please refer to their Privacy and Security in Firebase document and specifically the ISO and SOC-compliance section.

CoScreen also uses the Jitsi-as-a-Service platform by the ISO 27001, FISMA, NIST-compliant, and HIPAA-compatible vendor 8x8. It provides enterprise-grade SFU (Selective Forwarding Unit) video relay infrastructure for multi-point conferences. For further information regarding 8x8's security processes and the enterprise-readiness of their platform, please refer to 8x8 Security and Compliance.

2.1.1. ISO 27001

Firebase fulfills the ISO 27001 standard (Firebase ISO 27001 certificate) which is a security management standard that specifies best practices and comprehensive security controls. AWS also fulfills this standard: AWS ISO 27001 Compliance FAQs. 8x8 is also ISO 27001-compliant (8x8 Security and Compliance).

2.1.2. GDPR

Firebase/Google follows the EU General Data Protection Regulation and acts as a GDPR data processor - more information can be found under Privacy and Security in Firebase. All AWS services are also GDPR-ready. 8x8 is also GDPR-compliant, details can be found in the 8x8

GDPR FAQ. CoScreen has also appointed a Data Protection Officer to oversee the compliance and data protection efforts.

CoScreen's AWS services employ encrypted storage for all user data and supports data export and removal on request.

2.1.3. Additional Certifications (HIPAA, FISMA, NIST)

8x8, which handles the infrastructure used to transmit shared content of CoScreen users in some scenarios, is also HIPAA-compatible (Health Insurance Portability and Accountability Act) and FISMA-compliant (Federal Information Security Management Act). Details can be found in the 8x8 Security FAQ.

2.2. Infrastructure Server Locations

CoScreen's Firebase account is located in the region us-central.

CoScreen's AWS account leverages the region us-west-2 for backup video servers and us-east-2 for analytics databases, and production and development clusters that are used for adjacent services like the CoScreen integration APIs.

2.3. Incident Response

Security incidents can be brought to the attention by sending an email to security@coscreen.co.

CoScreen has implemented a formal Business Continuity Plan and Disaster Recovery process to implement the policies, tools, and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a business disruption that might be, but does not have to be, related to security incidents.

The status of the CoScreen infrastructure and services as well as customer-facing incidents are published on https://coscreen.statuspage.io/.

CoScreen runs business continuity tests on a regular basis.

2.4. Monitoring

CoScreen's infrastructure is monitored automatically using AWS CloudTrail and an alerting system is set up to ensure that the CoScreen team is able to swiftly react to incidents.

System uptime is monitored through Google Cloud Platform for Firebase and CloudWatch for AWS systems.

System status and service quality of 8x8 JaaS is monitored using Callstats and TestRTC Monitoring.

2.5. Sensitive Customer Data

CoScreen does not store any customer data, shared window data, or remote control input. It only captures encrypted session metadata for purposes like billing and product quality. Access to session metadata is limited to employees and systems that require access.

2.5.1. Personally Identifiable Information (PII)

CoScreen does **not** record or store any shared window content, remote control input, audio or video chat data. CoScreen captures email addresses of end-users as identifiers and for internal session management and to coordinate activities between end-users (e.g. invites), but uses anonymized IDs in connected systems whenever possible (e.g. for error logging).

For more details please see the CoScreen Privacy Policy.

2.5.2. Customer Credentials and Access Tokens

Credentials and access tokens used for customer systems and third-party systems are stored securely in a service such as AWS Secrets Manager and are never transmitted via emails, chat, or similar. If credentials are exposed by accident, they are revoked and reissued.

Employees do not store credentials in their development environments.

2.6. Development Infrastructure

2.6.1. Environments

CoScreen operates in two distinct environments: development, and production.

Access controls are in place between those environments, with changes to access levels continuously managed and reviewed by authorized personnel.

The purpose of the environments are as follows:

- Development: local development using non-production data.
- Production: live production environment.

All code is statically analyzed for security flaws on every merge request using SonarQube:

- Security Vulnerabilities.
- OWASP Top 10 (the most critical security risks to web applications).
- Security Hotspots (security-sensitive code and secure coding practices).

All merge requests affecting production code are reviewed by a second pair of eyes with security in mind.

2.6.2. Access Control

To minimize the potential harm of an incident, all servers, applications, and users are granted the minimal set of privileges possible for the task they perform. This includes but is not limited to firewall rules, AWS API permissions, and database privileges.

All user roles in critical systems are only accessible via multi-factor authentication, using a physical device or the Google Authenticator app.

Select access control measures:

- The firewall rules of a service using a database should only open the ports necessary for the service to open connections to the database, and the database is only accessible behind a secure VPC.
- When a service only reads from a database, it should not have write access.
- Services should not have administrative rights, such as the right to drop databases - these rights are reserved for administrators.
- When a service is allowed to access specific objects in Firebase, or S3, the service must be restricted to the most specific access possible, and only the actions it needs.
- Services using Firebase cloud functions, or AWS APIs are only allowed to use the specific actions they need, and only the resources they need.
- Services and applications running in the development environment are in a separate VPC and do not have access to the production environment, and vice versa.
- Services leverage roles, versus static credentials whenever possible to ensure keys are ephemeral and expire often.

- Access logs of critical infrastructure are reviewed on a regular basis.

2.6.3. Open Web Application Security Project (OWASP)

All application development is managed in accordance with the best practices outlined by the Open Web Application Security Project ("OWASP") Top 10 in terms of developer and web application security.

OWASP and other common vulnerabilities are continuously tested with every merge request.

2.6.4. System Updates and Security Scanning

CoScreen infrastructure is continuously kept up-to-date in terms of security updates and regularly scanned in terms of security, reliability, and maintainability matters using AWS Inspector and Google Cloud Monitoring.

In addition, port scans are done regularly to ensure systems are configured securely.

2.6.5. HTTPS/TLS

All traffic from and between CoScreen applications and services is encrypted and transmitted over HTTPS/TLS. Certificates are managed through the AWS Certificate Manager whenever possible, and Let's Encrypt/certbot otherwise. Certificates expire after XXX and are set to auto-renew.

2.7. Supplier Risk Management

CoScreen has a formal Supplier Risk Management Policy in place to ensure that suppliers, vendors, and their sub-contractors are being held to the highest standards.

3. Network Security

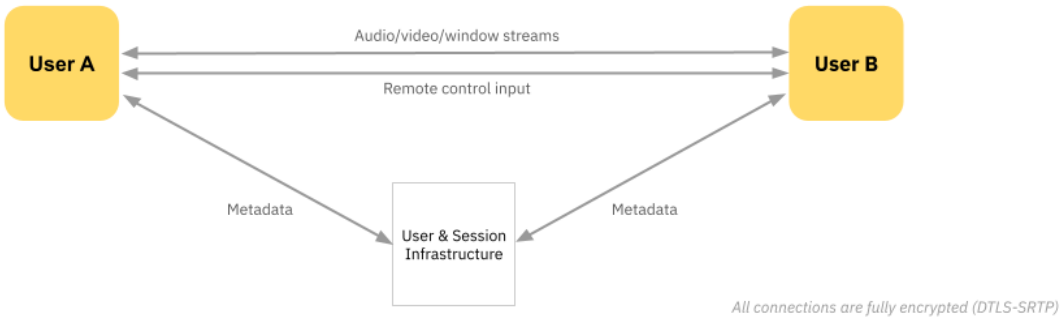
3.1. Encrypted Data Transmission

Data exchanged between end-users and CoScreen servers is always transmitted over encrypted connections.

Any windows which are shared between CoScreen customers, as well as their audio and video chat traffic, are encrypted and transmitted using DTLS-SRTP (IETF memo), the enterprise-grade standard for secured WebRTC connections (more on WebRTC security).

CoScreen does not record or store any shared window content, remote control input, audio or video chat data.

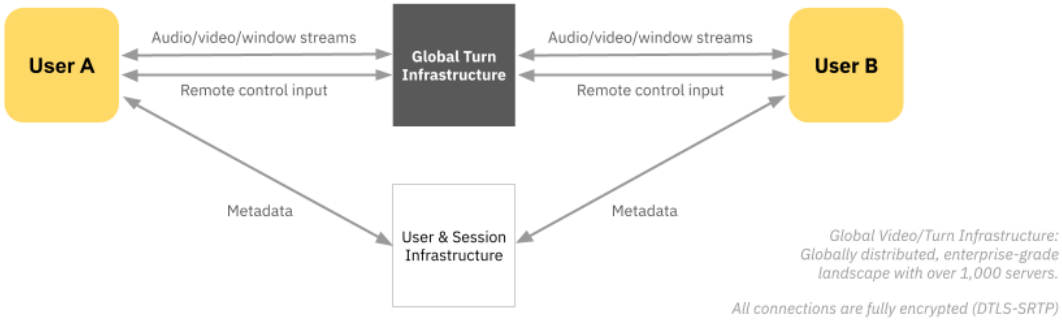
3.2. P2P (Peer-to-Peer)



CoScreen P2P Network Scenario - Two users, direct connection possible

Whenever two collaborators can establish a direct connection between them (P2P/Peer-to-Peer, NAT Traversal), shared content is transmitted directly between them and is end-to-end encrypted, without touching any CoScreen infrastructure.

3.3. TURN

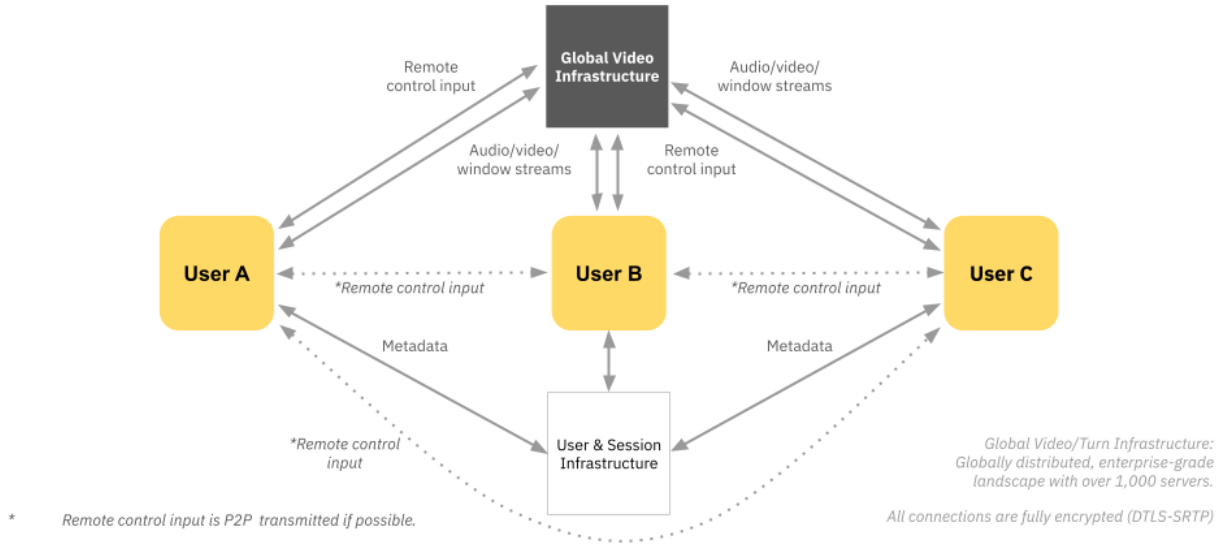


CoScreen TURN Network Scenario: Two users, only indirect connection can be established

When two collaborators cannot establish a direct connection between themselves, e.g. due to corporate firewalls and VPNs, shared content is encrypted and transmitted over a secured TURN (Traversal Using Relays around NAT) infrastructure so that customers can connect under any network condition.

Shared content is always encrypted during transmission. The global TURN infrastructure is managed by CoScreen's HIPAA-compatible partner 8x8 (compliance details: Security Standard Compliance), which offers the enterprise-grade platform using the highest levels of security and compliance policies and procedures (more in the section on Security Standard Compliance).

3.4. Bridged



CoScreen Bridged Network Scenario: More than two users connecting

Because P2P connections do not scale performantly for more than two participants (details here), CoScreen sessions with more than two collaborators will be handled via the globally distributed video bridge infrastructure by our partner 8x8.

Shared content is always encrypted during transmission. The global video bridge infrastructure is managed by CoScreen's HIPAA-compatible partner 8x8, which offers this enterprise-grade platform using the highest levels of security and compliance policies and procedures (more in

the section on Security Standard Compliance). No customer video/audio/screen/control data passes through CoScreen infrastructure

The video infrastructure relies on the mature open-source framework Jitsi (learn more: Jitsi Meet Security & Privacy). CoScreen can support end-to-end encryption as part of an Enterprise service plan. For large scale-deployments, the local deployment of the video infrastructure as on-premise/in-house installation can be explored.

4. End-User Security

4.1. Authentication

End users can register and authenticate with CoScreen using a Google Account or by entering an email address that has to be confirmed by CoScreen through an email verification flow.

Strong password requirements are enforced and must contain the following:

- Eight or more characters.
- At least one uppercase character.
- At least one lowercase character.
- At least one number.

4.2. Screen-sharing and Remote Control

CoScreen enables end-users to share windows individually and keep the rest of their desktop private. This reduces the chances for them to share information accidentally.

Windows that are shared are transmitted as encrypted video streams and not recorded, stored, or accessed by CoScreen personnel and infrastructure.

If users only share individual windows, their collaborators can only control individual shared windows and their child windows, not the entire operating system unlike in other remote collaboration solutions.

4.3. Privacy

See the CoScreen Privacy Policy.

5. Organizational Information Security

5.1.1. Critical Systems

Access to critical systems is restricted at the individual level based on role and responsibilities. Examples of access restrictions include superuser access (Admins only), production, environment access, and AWS IAM policy groups limiting resources.

Shell access for administrative tasks uses SSH. Only public key-based authentication is allowed, using unique keys for each user.

All critical systems leverage encrypted storage.

Centralized logging is in place for all critical AWS infrastructure to enable traceability in the event of an incident.

Examples of event logging include:

- Failed access attempts and logins.
- Deployments of new code.
- Adjustments to Route53.

5.1.2. Personal Computers

Employee personal computers fulfill the following requirements:

- Full disk encryption of all hard drives.
- Passwords must be required to log in.
- Password entry is required after a brief period of inactivity.
- No automatic login at computer boot/wakeup is allowed.
- Antivirus is installed and enabled.
- All systems are equipped with Sophos Endpoint Protection/Monitoring and continually monitored for security issues by the in-house IT administrator.

5.1.3. Passwords

5.1.3.1. Password Managers

It is mandatory for all CoScreen employees to use a password manager for all work-related passwords.

5.1.3.2. Other Passwords

All work-related passwords managed by the password manager must be generated using a password recipe following these minimal guidelines.

- At least 20 characters long.
- Containing at least 2 digits.
- Containing at least 2 symbols.

Employees are highly encouraged to utilize the strongest password recipe possible for all services.

5.1.4. Multi-Factor Authentication

MFA (also known as Two Factor Authentication or Two-Step Authentication) must be enabled for the following services and should be used for any service that provides it.

- AWS Console.
- Firebase console.
- GitLab.
- Slack.
- Google Workspace console.

5.1.5. Software Development and Change Management

Software development at CoScreen is done according to industry best practices: formal code reviews, pair programming, automated and manual testing, continuous deployment, production logging and alerts, and regular quality and performance benchmarking.

CoScreen has also put in place a formal Configuration and Change Management policy and established a process for provisioning, hardening, securing, and locking down all system components prior to full deployment to production. This process helps ensure that standardized methods and procedures are used for efficient and prompt handling of all changes, in order to minimize the impact of change-related incidents upon service quality, and consequently improve the day-to-day operations of the organization.

5.1.6. Security Education and Policy Trainings

Employees are required to complete information security policy, security awareness, and incident response training upon hire. Employees also review security policies and best practices on an ongoing basis. In addition, engineers are required to take Secure Coding Training.

5.1.7. Policy Review

The security officer or their deputy performs a bi-monthly review to make sure that employees follows the policies in this section.

5.1.8. End of Employment / Access Revocation

At the end of employment, either by resignation or termination, the security officer or their deputy will revoke access to any critical systems, email accounts, and all other systems.

The employee is bound by law and/or employment contract depending on jurisdiction to erase all data and other immaterial property rights from any medium, including physical copies and printouts at the end of employment.

5.2. Employee Non-Disclosure and Confidentiality

All CoScreen employees are required to sign a confidentiality clause included in their employment contract, restricting employees from sharing customer information with any third party unless required by law.

Any external subcontractors that may come in contact with sensitive information are also required to sign a non-disclosure agreement (NDA).

Contact for questions or concerns: security@coscreen.co