UPSCOPE

Security Doc

1. OVERVIEW

From the infrastructure to the features of Upscope, security is always at the forefront. State of the art data centers ensure your information is safe and secure and data is encrypted by SSL.

Ask for user's permission

Optionally enable a popup asking for your user's permission before screen sharing is initiated.

Remote control limited to the browser

Unlike other screen sharing systems where the user has to install software or at very least an extension, Upscope allows your agents to control the user's browser (limited to clicks and scrolls).

No installs are required, making the experience safer and smoother for both agent and user.

Hide sensitive parts of the page

Easily hide sensitive parts of the page or specific form fields (such as SSN or credit card information) by selecting the element to hide in our dashboard. Portions of the page hidden with.

State of the art data center

Our website is hosted in secure data centers operated by AWS and located in the North Virginia region.

Remote log out

You can easily log out of other browsers, and as an administrator you can remotely log out other team members of all their sessions.

SSL everywhere

Your connection with Upscope is protected by SSL everywhere. All access cookies are HTTPS-only, to guarantee no man-in-the-middle or third party library can get hold of them.

Sandboxing

While we load remote HTML in your agent's browser to show them what your user is seeing, we do so in a sandboxed iframe so that no javascript can be executed. We also proxy all remote assets to ensure they are served over HTTPS.

Protected database access

Only key employees are able to access our database (which only holds account information and user metadata in any case). Access is only possible through a secure VPN connection, and it is always logged.

Secure by design

We secure your data by avoiding storing it at all. In case of a complete data breach, an attacker would only be able to access your user metadata and your account information.

On-premise

Complete on-premise deployment of our technology is available on our enterprise plan.

Secure office building

Our office is located in the middle of London and is equipped with CCTV and 24/7 security personnel and access control.

Background checked employees

All our employees are background checked to the PCI DSS standard.

ISO 27001 compliant facilities

Our office is fully ISO 27001 compliant and all our employees are trained on data security regularly.

All actions logged

All actions performed by our employees on your account (such as updating information, viewing your users when you request it for testing, etc.) are monitored and logged.

2. DATA

Never sent to Upscope:

The below data never leaves your visitors browser, and is never touched by Upscope.

Client's Screen Content	We never store the content of the clients screen and the data is only transmitted during a session.
Information masking	If there is any information you don't want to pass through the session, hide it with our data masking. The information will never touch our servers and won't be visible to agent
Cookies and Browser Storage Content	We don't store your clients cookies or browser storage
Console	Built into Upscope is a console, here you can see errors with the page, however, the content of the console isn't recorded until the session begins. (If console access is disabled, the data does not leave the visitor's browser even while screen sharing)

Sent to Upscope for Processing:

The data below us sent through Upscope's servers but is not stored or even logged

Client's Screen Content	The HTML of the client's screen is transmitted whilst a session is active, once the session has terminated the HTML stops passing through our servers.
Agent Actions	Any interaction the agent has with the client's page is processed until the session is terminated. Actions such as clicking, scrolling and highlighting.
User information	If integrated into Intercom, Upscope automatically pulls the client's name, email address, and location. This is displayed on the list of users on the main Upscope application.
Live chat content	E.g. With Intercom and Drift live chat, the client's side of the chat is visible during a session.

Cached for 24hrs:

This data is stored by Upscope for up to 24 hours for performance improvement purposes.

Publicly available assets	Stylesheets, images, fonts etc

Stored by Upscope for 7 days:

This data is stored by Upscope for 7 days after it is collected if we enable debugging for your account to troubleshoot problems.

List of events	Events to and from the user's browser will be stored, excluding the content of the event. e.g. we might store a "sent page content" event without the content

Stored by Upscope for 30 days:

This data is stored by Upscope for 30 days after the last time the visitor is seen by Upscope, until you delete the data or until you delete your account.

IP address	The IP of the visitor, this is used to determine the location of the client on the list of online users.
Last page viewed and when	The timestamp and URL of the last page viewed by the visitor.
Location	Taken from the IP address, the city and country of the visitor.
Device information	Device information such as what kind of device the visitor was on (desktop, phone, tablet etc) and which browser.
Visitor ID	Provided by you or a live chat integration, the ID or their name and email address is stored.

Stored by Upscope until account is deleted:

This data is stored until you decide to delete your entire Upscope account.

Session log	When a session occurred and who was involved, length of the session, the visitor ID
Visitor information	IP address, unique ID, and list of identities of your visitors. Optionally, you can delete individual visitor's information in your Settings.
Payment details	The card you use to purchase Upscope

Stored for one year after account termination

This data is stored for a year after your account is deleted or when you send us a request.

Agent information	Agent names, email addresses, phone numbers, IP addresses and all changes to their accounts. If the agent is part of multiple teams, the data will be retained as part of the other team.
Session history	Timestamps, visitor IDs, visitor unique IDs are stored, however if the unique ID appears to be an email, this is deleted. No session content is ever stored.
Setting changes	Setting alterations are logged.

Stored indefinitely

This data will be retained by Upscope indefinitely unless required to be deleted by law.

Billing history and details	All payments made, invoices
Communication exchanges	Chat and Email correspondences

3. LOGGING

3a. Activity Log

Changes to the Upscope account and basic record of screen shares are displayed in the audit log.

Each log item contains a hash of the previous entry to prove no item is changed or removed.

Activities recorded include:

- Any agents added or removed
- When an agent logs in
- Any co-browsing sessions initiated
- Any co-browsing sessions joined with another agent
- Personal detail changes

- Agent accesses given/revoked
- General Setting changes
- When passwords are enabled

3b. Session log

Screen share logs contain information about the session but never the content.

Information shown is:

- The agent and the client involved in the screen share
- When it started
- When it ended
- How long it lasted
- Which features were used

4. TEAM MANAGEMENT

4a. Restrict Access

You can restrict specific agents from certain areas of the application, these include:

- Viewing the list of online users
- Being able to co-browse with clients
- Accessing General Settings tab

- Accessing Team Members tab
- Being able to delete client data
- Billing page access
- Viewing audit and session log
- Viewing Reporting
- Client browser console access

4b. Managing who can join the team

Admins and anyone given access to the “Team Members tab” can add, remove and manage access. Anyone with the same email domain as the team account can sign up to Upscope and is automatically added to the team.

ie. If Fred James from Acmetechnologies was the first person to sign up to Upscope with f.james@acmetechnologies.net, he would own the acmetechnologies.net team account.

If anyone else joined after Fred, say Jane with the email address j.carver@acmetechnologies.net, she’d automatically be added to Fred’s team as an agent.

You can restrict anyone from joining so that if someone else tries to sign up with the same email domain, they wouldn’t be able to unless they contact you.

5. GDPR COMPLIANT

Upscope acts as both a data controller with regards to data about our own customers, and as a data processor with regards to data about your end users.

Your end user’s data

By installing Upscope on your website, we collect some information about your end users. This is limited to metadata such as their IP address, page url, and timestamps.

The data is automatically deleted permanently after 30 days of inactivity, or whenever you ask us to delete it through a dedicated page.

What personal information do we store?

Upscope has no core need to store any personally identifiable information (PII) for the long term. We store your end user's IP address, last activity timestamp, last visited url, and (optionally) user id and any identity information (such as name or email) for 30 days after they last visit your website. You can delete this data manually at any point.

By going to the delete visitor datapage. If you have REST API access you can also delete data from the API.

In your activity log we store the user id of the users you screen share with indefinitely. If the user ID you provide looks like an email address we mask it in your activity log.

ℹ️ Hiding specific page content

With Upscope, you have the ability to hide portions of the page. By doing this you can ensure that no PII ever touches our servers. You can apply this to form fields (such as a credit card number input), or to entire portions of the

page. When you enable this feature, the hidden portions are never touched by Upscope.

⚠️ Data stored indefinitely

As part of your activity log, we store everything that happens with your account indefinitely. This includes the user unique ID you provide of your end users, therefore it is essential you do not send us PII through the unique ID.

Where is data stored, how is it processed?

Metadata is stored in a secure AWS data centre in North Virginia.

When screen sharing is initiated, Upscope transmits the content of the page the end user is on and sends it to the agent's browser for rendering. Upscope never stores page content, and our servers only act as proxy.

After screen sharing ends, no additional data is sent from the user's browser to our servers.

Do we share information with 3rd party data processors?

We don't share your end user's data with 3rd party data processors. The data and our servers are hosted by AWS and MongoDB, Inc.

Our customers' data

By creating an Upscope account or visiting our website, we collect data about you, your company and your computer. This data is used for access control, marketing and business intelligence purposes.

What personal information do we store?

When you create an account, we store information such as your name, email address, phone number in our data center.

The same data is also collected for all the team members you invite to your Upscope account. All your activity on Upscope is stored indefinitely within your Audit Log.

This can only be deleted by contacting our team.

Where is data stored, how is it processed?

All our customers' data in a secure AWS data centre in North Virginia.

Do we share information with 3rd party data processors?

Our customer's data will be shared for processing with the following companies:

Intercom, Inc. (https://intercom.com/)

AWS, Inc. (https://aws.amazon.com/)

Stripe, Inc. (https://stripe.com/)

Xero Ltd (https://xero.com/)

ChartMogul Ltd (https://chartmogul.com)

Sentry, Inc. (https://sentry.io)

Information might also be collected by:

Google, Inc (https://google.com/)

New Relic, Inc (https://newrelic.com/)

Privacy policy, DPO and breaches

We've updated our privacy policy including assigning a data protection officer and the procedure for notifying customers of any breach. We'll notify customers of any major changes to the privacy policy.

You can find our terms and conditions and privacy policy here https://upscope.io/legal/

6.HIPAA COMPLIANT

Overview

Upscope is HIPAA compliant and ISO27001 certified.

Upscope co-browsing is the modern secure form of screen sharing giving you complete control over which user data is passed through servers and displayed to support agents.

In addition, you only see the user's browser tab containing your own website and no other 3rd party tabs or confidential desktop folders.

Signed BAAs

We meet all the key physical, technical and administrative requirements of HIPAA including having signed BAAs with all key 3rd party providers.

Data storage and transmission

Upscope's servers are run via AWS in their secure North Virginia data centre.

You only transmit data only while screen sharing. We only store metadata about your users such as their location, IP address, last activity timestamp, and optionally their identity. No page content is ever sent to our server unless screen sharing is initiated.

Hide sensitive parts of the page

Easily hide sensitive parts of the page or specific form fields (such as SSN or credit card information) by selecting the element to hide in our dashboard. Portions of the page hidden with Upscope never leave the user's browser.

Remote control limited to the browser

Unlike other screen sharing systems where the user has to install software or at the very least an extension, Upscope allows your agents to control the user's browser (limited to clicks and scrolls) with no installs required, making the experience safer and smoother for both agent and user.

Enforced SSL: All your user's data is only transmitted via secure SSL connections.

Immutable Audit logs: Every action your team takes on Upscope (except for screen sharing session details) is recorded and accessible in the admin

console. Each log item contains a hash of the previous entry to prove no item is changed or removed.

Access Controls

Upscope provides role based access controls for restricting which personnel can conduct screen

sharing sessions with users.

Further information

You can find more information on security including data storage and options on white labelling / on premise solutions on our security page here.

7. ON-PREMISE SOLUTION

If your company has stringent data protection policies and you can't allow customer data to leave your infrastructure, you have the option of deploying Upscope on premise.

On-premise architecture

Our on premise solution is designed to maximize security while reducing the amount of components needed to run the service.

Data service on premise + Upscope cloud

Upscope's data service is designed to handle all user data including keeping track of who is online

and allowing screen sharing between visitor and agent.

Due to it being the only component which touches user data, it is the only one you'll need to run in

your own infrastructure to maintain a high standard of security.

With our on premise + cloud solution, you can ensure no user data touches our system while still benefiting from our dashboard which includes agent authentication, live chat integrations, SSO, agent management and more.

Data service on premise + Upscope API

Our middle ground solution allows you to host all user data in your own infrastructure and make use of our API to authenticate agents. This enables you to allow user-to-user screen sharing.

Using this solution has the advantage of still being able to use our dashboard to manage your account.

Data service on premise only

Our data component is completely independent from the rest of our system, therefore you are able to host the component in your private cloud and authenticate agents through a JWT. This solution enables you complete control over authentication and user data.

Deployment

To run our data service on premise, you will need to be able to run a docker image. If you have a large number of visitors (i.e. 5000 + concurrent), you

might need to run multiple servers behind a load balancer and connect them with a Redis instance or cluster.

Installation and Updates

We publish an update to the application every 4 weeks, and support the last 2 versions. Security updates are provided in a timely manner. An update command is included in the package. Downtime for updates is typically less than 5 seconds and does not interrupt active co-browsing sessions.

Pricing

Please get in touch with our team for our on-premise pricing.