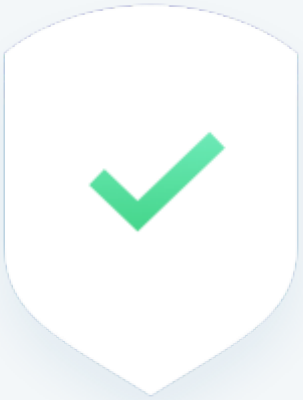
lookback



Cloud Security Whitepaper

Sep, 2018

1. Product Overview

Lookback is a platform that helps you understand your customers. Lookback focuses on qualitative user experience (UX) research. It's used by thousands of companies including Facebook, Netflix, Spotify, Dropbox, eBay and SAP.

Lookback lets you talk to your users anywhere in the world. You see their face and what they see on their screen, hear their voice, and see visualizations of where they interact on the screen ("touch icons") while they use an app, website or prototype. Your users (we call them "participants") can be using mobile or desktop devices.

All real-time sessions are automatically recorded and stored in the cloud. However, if you don't have time to interview in real time, you can send out tasks to participants. Recordings from participants completing those tasks will then be uploaded to Lookback's servers, where your UX team can watch, comment and export them.

Participants only use Lookback with consent. Sessions cannot be started automatically, and participants always have to explicitly enable screen sharing, camera sharing, and microphone sharing before a session can start.

2. Personally identifiable information (PII)

Lookback only collects two pieces of PII from participants: their full name and their e-mail address. We do that to help your researchers separate recordings from one another, and to allow them to easily contact the participants in case a submission was not fully completed or contained errors.

However, since Lookback's primary content type is videos from a device's screen and camera, anything could be captured in a recording. Including credit cards, passwords, etc. It all depends on what your participants do and what your researchers instruct them to do.

Using Lookback without saving any PII

If you do not wish to capture any PII within Lookback, here are some tips:

- Test with prototypes rather than real websites, to limit what can be inserted into certain fields. Avoid password fields and credit card fields.
- Instruct participants to not enter full names and emails when prompted by Lookback. The fields aren't required, and participant emails are never validated or reused.
- Avoid asking questions or writing instructions to participants that may make them reveal any PII.

3. Security and privacy policy

We have a security policy based on ISO 27001 and can be audited against the standard. It covers security in human resources, physical security, access control, acceptable use, software development, incident management, device security, and compliance with laws and regulations. It's approved by management and communicated to the staff. We have an ISM who's responsible for the policy. The policy is reviewed at least yearly by the security team.

As part of our security and privacy policy we maintain the following controls:

- An external policy available to our customers, detailing how we protect their data.
- Written internal policies for safe handling and protection of data.
- Yearly internal audits of the security and privacy policy.
- Yearly third party audits of the security and privacy policy.
- A training program for the staff to ensure they are familiar with the security and privacy policy.
- Background screening of employees.
- Applying the principle of least privilege for sensitive data and systems.
- Protected access logs for sensitive data and systems.
- A process to ensure third parties are capable of protecting sensitive data.
- Processes to identify and address security and privacy incidents in a timely fashion.
- A change management process with reviews for networks and systems.
- A risk assessment program where we regularly review the threats to the company and how they can be addressed.

4. Personnel security

All employees undergo training on security and privacy. This training includes device security, password and 2FA management, physical security, malware protection, network security, incident reports and acceptable use.

All access to systems are granted on a need-to-know basis. We have processes to revoke access when it's no longer needed, be it because of new assignments or because the person is no longer working with Lookback.

Before hiring new employees we perform an identity verification, verify references and do a criminal record check.

5. Networks

Service network

Lookback runs the production systems in a segregated network in a AWS VPC. The network is divided in public and private subnets. Services that have to be exposed to the public internet are running in a DMZ and everything else is on our internal networks. Ports that are not required to operate the Lookback service are closed and administrative access to the servers is only possible from our corporate network.

All traffic between Lookback's systems and client accessible services, like web apps and applications for recording, is encrypted using TLS 1.2. Traffic between Lookback's internal services is also encrypted.

Corporate network

The corporate network is protecting our internal resources like monitoring tools, dashboards, deployment systems, server access, etc. It's accessible via an encrypted VPN tunnel that requires two-factor authentication. The VPN also serves as an additional layer of security where we monitor traffic and block malicious traffic to and from our workstations. Only registered devices with the required security measures installed are allowed to access the corporate network.

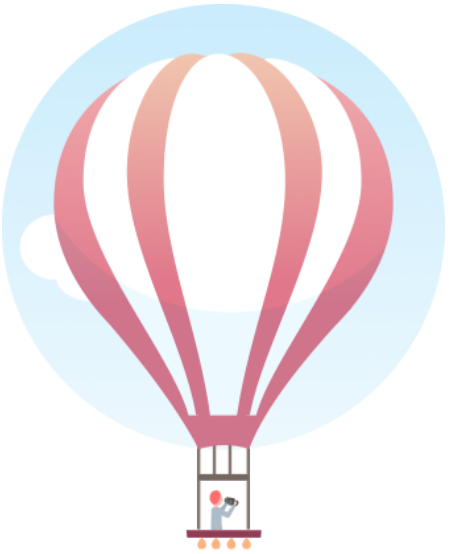
6. Servers

Lookback's servers run on AWS EC2. They are built and hardened using a standard build program. As part of the hardening we remove and disable all non-essential services, disable default accounts and passwords, disable password based authentication, setup log forwarding to a centralized logging system, install antivirus and install vulnerability scanners.

We run vulnerability and malware scans daily and can roll out patches for critical vulnerabilities outside of our regular patching schedule. Patches can be tested in isolated testing and staging environments before being rolled out to production. Our employees are also signed up to mailing lists informing us of security issues.

7. Data and Storage

Where we store the data



We store all sensitive data on AWS on Ireland, using S3 and EC2. Our database management is handled by a third party (MongoDB) but the data is also stored on AWS Ireland.

What we capture

When someone records with Lookback, we capture and store:

- a video of the device's screen,
- audio from the device's microphone
- all gestures/touches (or mouse movements and clicks) performed on the device,
- optionally the front facing camera (capturing the user's face)
- participant's first name, last name and email address
- metadata about the device used to record with (model, OS version, etc.)

Data segregation

You view your data using our webapp. It uses app level logic to determine who can see what data. Data is tied to an organization and if you are not a member of an organization you cannot see any of the organization's data.

Backups

The database is backed up by MongoDB. Files are backed up by AWS. We do not keep any backups of our own.

8. Logging

We log events on our servers and workstations, including authentication, privileged system calls and data access. Logs are sent to a centralized environment with limited access and are regularly reviewed. Sensitive access logs are encrypted, protected from modification and stored at least a year.

9. Administrative access

Lookback servers run on Linux and are connected to a central directory for managing access. Personnel with server access have individual accounts and use sudo where privileges are necessary. We have process in place to audit and revoke access to the servers. Access logs are regularly reviewed.

10. Clients

Workstations at Lookback are registered and monitored centrally. They are configured according to a standard that includes full disk encryption, secure configuration of VPN, network logging, anti malware programs that are centrally managed, secure administrative passwords and screen locking that activates within a few minutes of inactivity.

Updates are installed automatically by the built in patching mechanism in the OS. Security staff follow mailing lists to be up to date on vulnerabilities and when necessary we take action to protect our systems in case patches for new vulnerabilities haven't been released yet.

11. Technical security testing

To ensure our systems are secure we contract third party security firms to perform penetration tests on a yearly basis. It's a white box test covering applications, systems and networks, including both manual and automatic testing. Any findings are tracked and resolved by the security team.

Our last major review was in February 2018, when an independent security group performed a thorough, two week test of our entire system.

12. Enterprise Plan Security Features

The following security features are only available in the Enterprise plan:

Single Sign On (SSO)

We support SAML 2.0 and provide a simple interface for organization owners to configure it in our web dashboard. There are four primary settings you need to interact with:

- *SAML Validation URL:* Input this into your server's SAML configuration.
- *SAML SSO URL:* The SAML 2.0 endpoint that our servers should redirect to to authenticate the request.
- *Identity Provider Issuer:* An identifier/name for your Identity Provider (IdP), usually a url like https://yourdomain.com.
- *Public Certificate:* Your IdP's public certificate.

Further, we support the following options:

- Sign AuthnRequest
- Encrypt Assertion

You can get a copy of our Metadata.xml, our certificate and see the current field definitions.

Encryption at rest

Your data is encrypted at rest using the industry-standard AES-256 algorithm.

Security audits

We allow Enterprise Plan customers to audit our data processing procedures and documentation once a year, with reasonable notice, in order to assess our compliance with the security agreements between your company and ours. We also give access to recent penetration testing reports upon request.

Compliance with your additional security requests

We're happy to discuss any additional requests such and, upon request, may be able to include your specific needs as a Data Protection Addendum to the Lookback Enterprise Service Contract.

On-Premise installation

We offer the ability to install the entire Lookback platform on internal servers to select customers, under certain circumstances. This installation runs everything, including storage, the dashboard, and session processing, on your internal CentOS machines or private AWS installation. If you are interested, reach out to us to see if you qualify and to get more information.

Make all projects private *(Coming soon)*

We're building a feature to let Enterprise Plan organization owners require that all newly created projects are made private per default.

Currently, it is up to the creator of the project to choose whether to make it visible to the entire organization or just those with access. This new features gives owners more control over who can see what within the organization.

Customizable data retention rules *(Coming soon)*

Per default, recordings are stored on Lookback's servers until one of your researchers delete them, or until you stop being a customer. With the Enterprise Plan, you can set a custom time period that decides how long we'll store your recordings, participant information, notes and comments.

7. Additional Questions

To learn more, see our Privacy Policy or Terms of Use.

For additional questions, reach us at security@lookback.io or contact Carl directly:

Carl Littke
Chief Security Officer
carl@lookback.io

🇺🇸 +1 (415) 530-0665
🇸🇪 +46 70-27 23 655

Happy researching!

The Lookback team