Current Security Policy Document for Synthetic Users Inc

---

1. Product Overview

Synthetic Users is a platform that helps you better understand your customers by replicating them as Synthetic Users and allowing you to run studies with them. Synthetic Users focuses on qualitative user experience (UX) research.

All your studies are automatically recorded and stored in the cloud. Studies remain in Synthetic Users' servers, where your UX team can watch, comment, and export them.

2. Personally identifiable information (PII)

By default, Synthetic Users collects two pieces of personally identifiable information (PII) from participants: email address, and IP address. This information is collected to assist users in managing their studies and to aid in debugging and service improvement. Synthetic Users primarily focuses on generating synthetic interviews and reports.

3. Security and privacy policy

Our security policy is aligned with the SOC 2 standard.

- • SOC 2 Compliance

The policy encompasses various aspects such as human resources, physical security, access control, acceptable use, software development, incident management, device security, and compliance with laws and regulations. It is approved by management, communicated to the staff, and reviewed annually by our security team.

To ensure security and privacy, we have implemented the following controls:

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

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 is granted based on the principle of least privilege. 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 Synthetic Users.

Before hiring new employees, we perform a background check for criminal records (to the extent permitted by applicable law) and an identity verification check.

5. Networks

Network Security

Our organization leverages the built-in software firewalls provided by AWS and Render to protect our network infrastructure.

AWS Firewalls

- **Security Groups and NACLs:** We utilize AWS Security Groups and Network Access Control Lists (NACLs) to control inbound and outbound traffic to our EC2 instances and subnets. These act as virtual firewalls, allowing us to define granular rules for network traffic.
- **Configuration Management:** Our team configures and manages these security groups and NACLs to align with our security policies and the principle of least privilege.
- **Regular Reviews:** Firewall rules are reviewed quarterly or whenever significant changes are made to our infrastructure to ensure they remain effective and up-to-date.

Render Firewalls

- **Managed Security:** Since Render manages the underlying infrastructure, including network security, we rely on their built-in software firewalls and security practices to protect our applications.
- **Isolation and Protection:** Render provides network isolation and enforces security boundaries between applications using software-defined networking and firewalls.

Firewall Policy Review

- **Quarterly Reviews:** We perform quarterly reviews of our firewall configurations and rules within AWS to ensure they comply with our security requirements.
- **Change Management:** Any changes to firewall settings follow our documented change management process, including necessary approvals and testing.
- **Monitoring and Logging:** We monitor firewall logs and network traffic to detect any unusual activity, with alerts configured for critical events.

All traffic between Synthetic Users systems and client-accessible services is encrypted using TLS 1.2 or higher.

Wireless Network Security

Synthetic Users maintains a dedicated wireless network at its office in Portugal.

- **Security Protocol:** WPA2 Personal
- **Network Standard:** 802.11ac (Wi-Fi 5)
- **Network Isolation:** The office network is dedicated to Synthetic Users and is not shared with other organizations.
- **Access Control:** Network access requires a pre-shared key, distributed only to authorized employees.
- **Data Protection:** All application data transmitted over the wireless network is additionally encrypted via TLS 1.2+ at the application layer, providing defense in depth regardless of the underlying network.

The majority of employees work remotely. Remote employees connect to cloud-hosted services over their own networks; all remote access is secured via SSO with MFA and

TLS 1.2+ encryption, ensuring data protection regardless of the underlying network infrastructure.

6. Servers

Synthetic Users servers run on AWS, Render, and Vercel. 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, disable SSH access, set up log forwarding to a centralized logging system, scan for known vulnerabilities, and prevent the applications from spawning additional processes.

7. Data and Storage

Where we store the data

We store all sensitive data in the client's own region to ensure compliance with local data residency requirements.

- **UK clients:** Data is stored within the United Kingdom.
- **EU clients:** Data is stored within the European Union.
- **US clients:** Data is stored within the United States.
- **Canadian clients:** Data is stored within Canada.

Our infrastructure runs on AWS, using S3 and EC2 instances in the respective regional data centers (for example, Ireland for the EU, London for the UK, Virginia for the US, and Montreal for Canada). Database management is handled by a third-party service (Postgres), but all underlying data remains within the same regional AWS environment.

Names and emails of Synthetic Users account holders (i.e., platform users, not participants) are processed by HubSpot, which operates from the US. User inputs that form part of study generation may be securely transmitted to our AI subprocessors (OpenAI, Anthropic, Google, Meta, and Mistral) in the US for processing.

IP addresses may also be transmitted to our logging systems located in the US for security and monitoring purposes.

What we capture

When someone generates a study with Synthetic Users, we capture and store:

- Audience data
- Goals, pains, and problems
- All gestures/touches (or mouse movements and clicks) performed on the device
- Solution input data in the form of text and images
- IP address

Encryption during sessions

For study streaming, we encrypt data using the industry-standard AES-128 algorithm.

Encryption at rest

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

Data segregation

You view your data using our web app. It uses app-level logic to determine who can see what data. Data is tied to a workspace, and if you are not a member of a workspace, you cannot see any of the workspace'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, including authentication, privileged system calls, and data access. Logs are sent to a centralized environment with limited access and are regularly reviewed. Sensitive logs are encrypted, protected from modification, and stored for 12 months. Log events that are outside of the ordinary result in notifications for a human to inspect.

9. Administrative access

Synthetic Users servers run on Linux without any ways to log in to the server (SSH is disabled).

Personnel with access to accounts at third-party providers such as AWS or Render have individual user accounts with 2FA. We have processes in place to audit and revoke access to the systems within 24 hours of someone leaving their position at Synthetic Users.

10. Clients

Workstations at Synthetic Users are registered and monitored centrally. They are configured according to a standard that includes full disk encryption, 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 shortly after being released.

Security staff follow mailing lists to stay 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. Antivirus Policy

To safeguard against malware and other malicious software, Synthetic Users has implemented a comprehensive antivirus policy across all systems and devices.

Antivirus Software Deployment

- **Comprehensive Coverage:** All servers, workstations, and portable devices used within Synthetic Users are equipped with industry-leading antivirus and anti-malware software.
- **Centralized Management:** Antivirus software is centrally managed to ensure consistent configuration, updates, and policy enforcement across all devices.

Regular Updates and Patching

- **Automatic Updates:** Antivirus definitions and software are updated automatically on a daily basis to protect against the latest threats.
- **Timely Patching:** Systems are regularly patched to address vulnerabilities, with critical patches applied within 24 hours of release.

Scanning and Monitoring

- **Real-Time Protection:** Real-time scanning is enabled on all devices to detect and prevent malware infections proactively.
- **Scheduled Scans:** Full system scans are scheduled weekly to ensure thorough coverage and detection of any latent threats.
- **Threat Monitoring:** Any detected threats are automatically quarantined and reported to the security team for immediate analysis.

Incident Response

- **Immediate Isolation:** In the event of a malware detection, the affected system is immediately isolated from the network to prevent the spread of malware.
- **Notification Protocols:** The incident response team is promptly notified to initiate remediation procedures.
- **Forensic Analysis:** A thorough investigation is conducted to determine the source and extent of the infection.
- **Remediation Actions:** Remediation steps are taken promptly, including cleaning or rebuilding affected systems, and affected users are notified as necessary.

User Awareness and Training

- **Employee Training:** Employees receive regular training on recognizing and avoiding malware threats, such as phishing emails and suspicious downloads.
- **Acceptable Use Policies:** Policies prohibit the installation of unauthorized software or the use of personal devices without explicit approval.
- **Reporting Procedures:** Clear procedures are in place for employees to report suspected malware infections or security incidents.

Access Control and Least Privilege

- **Least Privilege Principle:** Users operate with the least privilege necessary to perform their duties, reducing the risk of malware installation and propagation.
- **Executable Controls:** Executable files received via email or downloaded from the internet are blocked or subject to additional scrutiny and approval processes.

Audit and Compliance

- **Regular Audits:** Periodic audits are conducted to ensure compliance with the antivirus policy and to identify areas for improvement.
- **Policy Review:** The antivirus policy is reviewed annually or after any significant changes to ensure it remains effective and up to date with current threats.

12. Development

Development is performed through a process that involves planning, coordination, implementation, review, testing, and follow-up after deployment.

The planning and coordination steps involve stakeholders from different departments, including security. Complex systems or complex changes are implemented by more than one developer and/or reviewed by senior developers. Security-related changes are always reviewed.

We do a range of testing depending on the size and complexity of the changes. It involves automated tests and may also involve testing in an isolated testing environment, as well as internal and external user research/beta testing.

All code is kept in a secure version management system.

13. Technical security testing

To ensure our systems are secure, we have scheduled to 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.

14. Your use of Synthetic Users

Your Synthetic Users user account

If you log in with a username and password (i.e., not using SAML), your password is hashed with SHA-256 on the client and sent over HTTPS to our servers where it's hashed with bcrypt before it's stored or compared with the value in the database.

Passwords must be at least 12 characters and must not have appeared in any previous password leaks (You cannot set your own password policy when logging in with your email and password, but if you use SAML, you are free to set your own requirements). We do not force rotation of passwords.

We rate-limit login attempts to prevent brute-force attacks.

User roles

Workspace

- **Owner**:
  - Add and remove members
  - Manage subscription
- **Member**:
  - Limited permissions (can't add/remove members or manage subscription)

Project

- **Admin**:
  - Add and remove people from projects (if already on the workspace)
  - Request addition of new members to workspace (requires workspace owner approval)
  - Generate studies
  - Run interviews

- **Editor**:
  - Generate studies
  - Run interviews
  - Cannot invite anyone to projects

14.1 Dynamic Code Testing

Synthetic Users incorporates dynamic code testing practices throughout its development and deployment workflows to proactively identify and mitigate potential security vulnerabilities and performance issues in real time.

Runtime Safeguards and Testing

• **Sandboxed Execution**: All code generated or executed dynamically as part of Synthetic User simulations runs in fully isolated environments using containerization and serverless technologies. This eliminates the risk of affecting the host systems or other users.

• **Runtime Monitoring**: Code executions are instrumented with telemetry to track runtime behavior, performance bottlenecks, memory usage, and any unexpected exceptions or behaviors. Alerts are triggered for anomalous patterns.

• **Time and Resource Limits**: To mitigate abuse and prevent denial-of-service (DoS) conditions, Synthetic Users enforces strict CPU, memory, and execution time quotas on all dynamically executed code blocks.

Automated and Manual Review

• **Automated Testing**: All code contributions go through automated tests covering unit, integration, and end-to-end scenarios. Special emphasis is placed on code paths that affect data parsing, transformation, and AI output handling.

• **Static + Dynamic Scanning**: Every deployment is scanned for known security vulnerabilities using both static analysis tools (e.g., semgrep, ESLint security plugins) and dynamic application security testing (DAST) tools.

• **Manual QA Review**: For sensitive changes (e.g., updates to AI agents' behavior or data pipelines), senior engineers conduct peer reviews and occasionally pen-test the interactions manually.

Security Focus Areas

• **Input Sanitization**: All user and system inputs to AI agents or scripting environments are sanitized and validated using strict allowlists and schema validators.

• **Escaping and Output Encoding**: Outputs generated from code or AI suggestions are carefully encoded or escaped to prevent code injection or script execution in rendered environments.

• **Audit Logging**: Every code execution—whether from a test, a simulation, or production—is logged with detailed metadata (timestamp, user ID, input/output hashes), enabling forensic tracking and rollback if needed.

15. Enterprise Plan Security Features

The following security features are only available in the Enterprise plan from May 2024:

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 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 obtain our `Metadata.xml`, our certificate, and see the current field definitions.

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 penetration testing reports upon request.

Customizable data retention rules

By default, studies are stored on Synthetic Users servers until one of your researchers deletes 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, notes, and comments. Reach out to our support for further information.

Compliance with your additional security requests

Missing something? Let us know, and we may be able to accommodate your request.

16. Additional Questions

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

For additional questions, reach us at support@syntheticusers.com

Version History: Jan 23 2026, v1.1