DATA SHEET

# Rainforest QA Security Overview

Rainforest QA is committed to providing secure, reliable crowdsourced testing to our customers. To ensure that all customer data stays protected before, during and after testing, we have taken measures to ensure that our platform, application, and tester network adhere to high standards for security. This document provides an overview of Rainforest QA security measures and our approach to protecting customer data.

## Rainforest Platform Security

Our main application, API, databases, etc. are powered by Google Cloud Platform (GCP). As a result, Rainforest inherits all of the benefits of Google Cloud's security model and world-scale infrastructure.

Rainforest has internal security policies around access control during development, specifying which developer role has access to which information. Customer information is only made available if it is necessary from a business perspective.

Read more about Google Cloud Platform security here.
Read more about Amazon Web Services here.

## Rainforest Application Security

Rainforest application security consists of several components, including:

- SSL protocol for industry-standard encryption of all network data
- DDoS protection provided by CloudFlare
- Single sign-on using Security Assertion Markup Language (SAML), which has security protocols built-in, or with Github authentication
- API access via rotating key authentication
- Customer data is stored encrypted-at-rest in our database
- Screenshots, videos and HAR logs are stored encrypted-at-rest in Amazon S3

## Rainforest Virtual Machines

All Rainforest tests are executed within our virtual machines (VMs) or on real iOS and Android mobile devices via Amazon Device Farm. Our virtual machines have been designed to provide a testing environment that is consistent and reliable for each and every test run. With that in mind, Rainforest takes multiple security measures to keep customer data secure within these VMs.

### Limited Interactions to Stop Data Leaks

Virtual machines do not allow users to use the copy & paste function outside of the VM itself. As a result, while testers can paste information into the VM and interact normally within the VM, they cannot copy out any information to use after the test has concluded.


### A Clean VM for Every Run

Because Rainforest testers interact with the webpage through our VMs, not directly from their own computers, we are able to monitor every interaction. A new, clean environment is spun up in our virtual machines for each individual test run. Once a test run is complete, the environment is destroyed and testers do not have access to any test data after the test has been completed. All testing data is logged for auditing and research purposes.

### IP Whitelisting

Rainforest uses a growing set of static IP addresses for all of our testing environments. This makes it easy for customers to whitelist our testing IPs. Having a set of static IP addresses ensures that access to our customers' environments are controlled by Rainforest, and all access is logged and traceable. This also prevents testers from starting a test or accessing a customer environment outside of the VM. When required, Single-IP is also available for added security.

### Virtual Private Networks (VPN)

Rainforest offers IPsec VPN and OpenVPN as an alternative to IP whitelisting for customers who wish to add an additional layer of security to their testing process.

View our list of static IP addresses here.
Our virtual machines run on servers provided by Hetzner Online GMbH. Read more about security at Hetzner here.

## HIPAA/ISO 27002 Compliance

Rainforest is HIPAA (Health Insurance Portability and Accountability Act) and ISO 27002 compliant, covering both Rainforest employees and our testing crowd. Only testers who have met our standards for compliance are able to execute tests for HIPAA-regulated Rainforest customers. See section on Rainforest Testers below for more information on our HIPAA compliance features.

## Rainforest Testers

Rainforest testers provide the human intelligence behind the Rainforest platform. We take tester training and management seriously, and hold our testers to high standards for both test quality and professionalism.

### Sourced and Trained Testing Professionals

Rainforest testers are sourced through Amazon Mechanical Turk (mTurk). Before any new tester can start running tests for Rainforest customers, they must both meet initial experience requirements, plus complete a rigorous Rainforest Tester Training School. This includes an expanding set of courses they must pass, including ones specifically dedicated to how they should interact with any customer data they engage with in the course of executing tests.

### Tester NDAs

All Rainforest testers must sign an NDA to ensure that they do not share any information that they learn about our customers' products. For customers with specific privacy needs, we offer custom NDAs, which require testers to adhere to your organization's standards for discretion before they can accept any work. Rainforest uses industry-standard HelloSign to collect e-signatures, which are required before testers receive your work.

### Using Machine Learning to Catch Unusual Activity

Testers only have access to your application during the test run. We use machine learning algorithms, statistics, and AI to ensure that each test run meets our standards for quality. Every tester action is monitored closely and recorded, and we take prompt actions to address any suspicious or unusual activity.

### Tester Malware Scans

Testers working on HIPAA-regulated customer accounts are required to submit regular malware scan logs. Customers who are not HIPAA-regulated may request that their tester pool is limited to testers who have submitted valid malware scan logs in the past 6 months.

### Tester Account 2-Factor Authentication

Testers have the option of securing their account with 2-factor authentication. Customers may require that only testers with this feature enabled have access to tests.

## Our Commitment to Continuous Quality

Rainforest is continually looking for ways to provide our users with a better QA testing experience. We constantly evaluate our security trends and upgrade our security technologies to provide the highest level of security for our customers.

To learn more about what we're doing to improve application security, read about our bug bounty program here.

## About Rainforest QA

Rainforest QA helps agile and continuous delivery engineering teams move faster with the industry's only AI-powered crowdtesting platform. Our platform leverages 60,000 qualified testers to deliver on-demand, comprehensive and machine learning-verified regression test results. Rainforest customers spend less time and money testing so they can ship better applications faster. For more information on Rainforest, visit https://www.rainforestqa.com.

Rainforest QA
2 Embarcadero Center Suite 2308-R
San Francisco, CA 94111 USA

www.rainforestqa.com
info@rainforestqa.com