TestingBot

SECURITY & COMPLIANCE

Security whitepaper.

An overview of the security processes, technology and compliance measures that protect TestingBot customers and their data.

Version 2026.07 · July 2026

EU only	99.99%	2012
HOSTING & DATA RESIDENCY	UPTIME SLA	OPERATING SINCE

CONTENTS

Table of contents

01 Executive summary 3

02 Compliance & certifications 4

03 Platform architecture & isolation 5

04 Data protection & encryption 7

05 Test assets & data retention 8

06 TestingBot Tunnel 9

07 Access & identity 11

08 AI features & data handling 12

09 Organizational security 13

10 Network & software security 14

11 Datacenter security, continuity & incident response 15

12 Subprocessors 16

13 Data we collect, and data we don't 17

14 Responsible disclosure 17

15 Conclusion & contact 18

SECTION 01

Executive summary

TestingBot is a cloud testing platform for running automated and manual tests on real browsers and real mobile devices, operated entirely from the European Union.

TestingBot provides an online grid of browsers running on Virtual Machines (VMs), together with physical iOS and Android devices, hosted on our own cloud infrastructure. Companies connect to this grid to run automated tests, live manual tests and visual tests against their websites and mobile apps, across the browsers, operating systems and devices we provide.

The service is operated by TestingBot, a company based in Belgium, and has been running since 2012. Our entire infrastructure runs on **dedicated hardware in EU datacenters**. Because we operate our own private cloud rather than reselling shared public-cloud capacity, we control and optimize the security of the service end to end, from the network layer up.

What this means for your data

- **EU-only data residency:** test logs, videos, screenshots and artefacts are stored and processed in EU datacenters.
- **Encrypted everywhere:** AES-256 at rest, TLS 1.2+ in transit with modern ciphers.
- **Isolated by design:** every automated test runs on a fresh, single-use VM that is destroyed afterwards.
- **Minimal data footprint:** we do not collect end-user PII, source code or passwords.

This document provides an overview of TestingBot's services, explains how we secure data in transit and at rest, and describes the security policies and procedures we operate. It is intended for security, procurement and compliance teams evaluating TestingBot as a vendor.

> The live, always-current version of the information in this document is published at trust.testingbot.com, together with our DPA, TOMs, CAIQ and other compliance documents.

SECTION 02

Compliance & certifications

Our control set is aligned with ISO 27001 and SOC 2 practices, our datacenters are ISO 27001 certified, and our security posture is independently rated.

CSA

CSA STAR Level 1

Registered in the Cloud Security Alliance STAR registry

GDPR

GDPR compliant

EU-based processing, DPA with SCCs available

CCPA

CCPA compliant

California consumer privacy rights honored

ISO

ISO 27001 datacenters

Certified facilities; internal controls aligned with ISO 27001

SOC 2

SOC 2 aligned

Internal controls follow SOC 2 Type II practices

DORA

DORA ready

Aligned with EU digital operational resilience requirements

BIT

Bitsight rated

Independent, continuous external security rating

AA

WCAG 2.1 AA

Accessibility conformance target for our web properties

Information security management

TestingBot operates a documented Information Security Management Program that is reviewed and updated annually. Policies cover access control, asset management, change management, incident response, business continuity and vendor management. The control set is aligned with ISO 27001 and SOC 2 practices.

Privacy & data protection

As an EU company processing data exclusively in EU datacenters, GDPR compliance is built into how the service operates rather than added on top. A Data Processing Addendum incorporating the EU Standard Contractual Clauses is available, and subprocessor changes are announced through a public change log with an objection window.

> Compliance evidence (CAIQ, datacenter ISO 27001 certificate, Bitsight report, DPA and TOMs) can be downloaded from trust.testingbot.com.

SECTION 03

Platform architecture & isolation

Every test runs in its own isolated, single-use environment. Nothing is shared between customers, and nothing survives the end of a session.

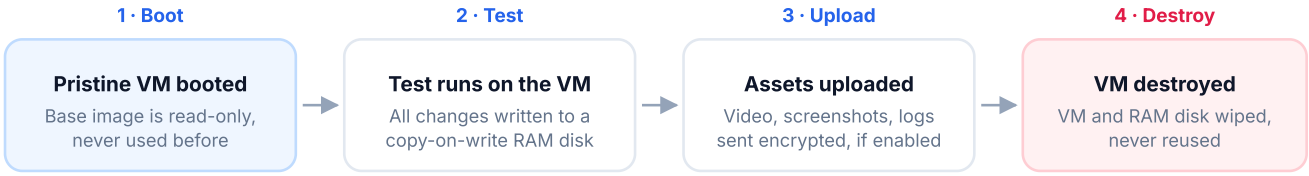
Virtual machines

The TestingBot cloud platform is a grid of Virtual Machines with browsers installed, covering the most popular operating systems: Windows, macOS, Linux, iOS (simulators) and Android (emulators).

For every test a user runs, the system allocates a **brand new, freshly booted VM**. Running each test on a pristine, single-use VM is the only way to guarantee that:

- No data from a previous test remains on the VM.
- No other customer could have installed any kind of program on the VM.

Securing shared VMs in a multi-tenant environment is notoriously difficult: you can never be certain a VM used by a previous customer was effectively cleaned. TestingBot avoids the problem entirely. Each test runs on a VM that has never been used before and will never be used again after the test completes.



Lifecycle of a TestingBot VM: one test, one VM, then gone.

Physical devices

TestingBot provides access to physical iOS and Android devices, located in our own EU datacenter. Customers can test on devices in a public pool, or on private, dedicated devices.

Devices in the public pool are used by multiple customers, one at a time. After every session, TestingBot runs automated cleaning: apps installed during the session are removed, accounts and settings are reset, and session data is wiped before the device returns to the pool.

For customers with stricter requirements we recommend **private devices**: dedicated hardware on which only your own tests run. With private devices you are guaranteed that no other customer's tests touch the device and no other data resides on it.

Public device pool

- Shared across customers, one session at a time
- Automated wipe and reset after every session
- Apps, accounts and data removed before reuse

Private devices

- Dedicated hardware, reserved for your account
- Only your tests ever run on the device
- Best fit for regulated or sensitive workloads

Per-session firewall

Every VM is configured with its own firewall. This firewall does not allow any inbound connection, other than from your test runner or manual test session. Each test runs on its own isolated virtual machine.

If you use the TestingBot Tunnel to reach your internal network during testing (see section 06), the VM's firewall is modified to allow only that connection, for the duration of the session.

Network segmentation

The production network is segmented: hypervisors, device hosts, storage and management systems live in separate network zones with firewalling between them. Systems that do not need to be reachable from the internet are not.

SECTION 04

Data protection & encryption

Customer data is encrypted at rest and in transit, and never leaves the European Union.

Encryption in transit

All connections to TestingBot services, including the website, API, test grid and asset downloads, are encrypted with **TLS 1.2 or higher** using modern cipher suites. Traffic to private networks flows through the encrypted TestingBot Tunnel over SSH.

Encryption at rest

Test artefacts, account data and backups are stored with **AES-256** encryption at rest, in EU datacenters. Backups are encrypted and monitored.

EU-only data residency

Every byte of your test data stays in Europe. TestingBot operates exclusively from EU datacenters, giving you GDPR compliance and data sovereignty by default:

- **Test logs & reports:** all test execution logs and reports are stored in EU datacenters.
- **Video recordings:** test session videos are recorded and stored within Europe.
- **Screenshots & artefacts:** all test artefacts are hosted on EU infrastructure.
- **Test execution:** tests run on browser and device fleets located in EU datacenters.

Key management & production access

Production systems use unique authentication per system, and multi-factor authentication is enforced on administrative access. Access to production data follows least privilege: only the people and systems that need access to operate the service are granted it.

> Some supporting services (for example payment processing and customer support) are provided by vetted subprocessors, a small number of which operate from the United States. The full list, including what data each one processes, is in section 12.

SECTION 05

Test assets & data retention

You decide what gets recorded, and everything that is recorded expires automatically.

What we record

For every test session, TestingBot can optionally:

- Record a video of the test, so you can watch afterwards what happened during the test.
- Take screenshots of the pages or screens under test.
- Collect log output from the automation framework (for example Selenium or Appium), our orchestrator and the browser.

Recording is on by default because it is what most teams want for debugging. If you don't want it, a single capability at the start of your test **disables recording completely**: no video, no screenshots, no logs.

How assets are stored

Assets are uploaded over TLS to protected, encrypted storage in the EU. Every asset is stored in private mode: nothing is reachable from the public internet. When you view a test in our dashboard, we generate **signed URLs that expire after 30 minutes**.

Retention

DATA	DEFAULT RETENTION	YOUR CONTROL
Test logs, video, screenshots	Deleted automatically after 30 days	Delete any test immediately via the dashboard or API
Enterprise plans	Configurable retention window	Custom retention or immediate deletion after each test
Account data	Lifetime of the account	Deleted when the account is closed

When you delete a test through our website or API, the test's assets are destroyed immediately.

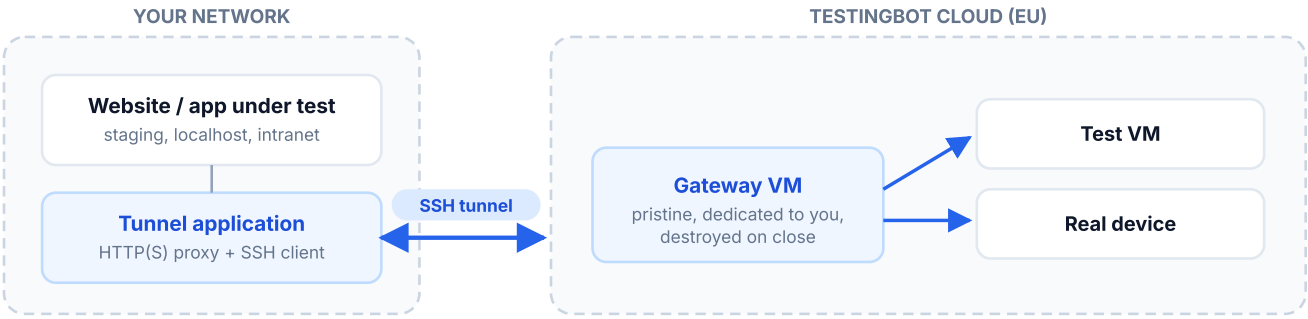
SECTION 06

TestingBot Tunnel

Test websites and apps that are not reachable from the public internet, through an encrypted tunnel that you control.

The TestingBot Tunnel allows customers to run tests against websites and apps on their own computer, staging environment or internal network. It consists of three components:

1. A **tunnel application** that runs on your computer or in your network: a Java-based application containing an HTTP(S) proxy and an SSH client.
2. A **gateway VM** on TestingBot's side: a pristine VM, accessible only to you and your team members.
3. A **TestingBot VM or device** for each of your tests, connecting to your network exclusively through the gateway VM.



All tunnel traffic travels through an SSH tunnel between your machine and your dedicated gateway VM.

The tunnel application is **open source**: its code is available at github.com/testingbot/Testingbot-Tunnel, so your security team can audit exactly what runs inside your network.

Gateway VM

Tunnel gateway VMs run an HTTP(S) proxy that caches commonly accessed images and scripts to minimize the traffic going through the tunnel. These cached assets are destroyed, together with the gateway VM itself, as soon as you close the tunnel.

Gateway VMs only accept connections from your computer. On the TestingBot side, only the VMs running your tests can reach your gateway; no other VM can access it.

Test VM behavior

During a tunnel session, the VM configures the browser under test to use the tunnel as its proxy. This is how the VM reaches the website or app running on your computer or network.

All VMs and devices on TestingBot are configured with our own CA certificate. By default, the tunnel re-signs TLS traffic originating from the tunnel with this CA certificate, to prevent issues when testing against services that use self-signed or otherwise invalid certificates. This behavior can be disabled with the `--nobump` option if you prefer end-to-end certificates.

Security properties

- All tunnel traffic is sent and received through an **SSH tunnel** between your computer and the gateway VM.
- The access the tunnel has to your network is **completely within your control**. We recommend running it in a firewalled DMZ that can reach only the resources required for testing.
- You can supply an upstream proxy, exclude domains that should not be proxied, and set a custom DNS server.
- The gateway VM is single-tenant and destroyed when the tunnel closes, including all cached data.

> Full tunnel documentation, including all hardening options, is available at testingbot.com/support/other/tunnel.

SECTION 07

Access & identity

Enterprise-grade authentication for your team, and scoped credentials for your test automation.

User authentication

Users sign in to the TestingBot website with email and password, and can protect their account with **two-factor authentication (2FA)**. Passwords are stored using modern, salted password hashing; plaintext passwords are never stored or logged.

Team-wide controls

SAML 2.0 single sign-on

Enterprise plans can enforce sign-in through your identity provider: Okta, Azure AD (Entra ID), OneLogin or any SAML 2.0 compatible IdP.

Organization-wide 2FA enforcement

Team owners on enterprise plans can require 2FA for every member of the organization; members without it must enroll before continuing.

IAM & RBAC roles

On enterprise plans, every team member holds two independent roles: an **IAM role** (Owner, Admin or User) governing administrative authority over the account, members, billing and team-wide settings, and an **RBAC role** (Admin, User or Viewer, plus custom roles) governing product capability, such as running, managing or deleting tests. Someone can have broad product access without being an account administrator. Removing a member immediately revokes their access to the team's tests and assets.

Audit logs

Audit logs record team activity across the organization: sign-ins and failed sign-in attempts, member and role changes, credential resets, 2FA changes and setting changes. Logs can be filtered by date range, event type or team member, are visible only to organization administrators, and are retained for up to 60 days.

API credentials & service accounts

Automated tests authenticate against the TestingBot grid and API with a per-account **key and secret** pair, available in the member dashboard. Credentials can be rotated at any time; rotating them immediately invalidates the old pair.

For CI/CD pipelines and other non-human contexts, **service accounts** provide API-only identities with their own key and secret; they cannot sign in to the dashboard, and their credentials can be rotated or revoked independently of any person's access.

Details at testingbot.com/support/team: rbac · service-accounts · audit-logs · enforce-2fa

SECTION 08

AI features & data handling

TestingBot offers optional AI-powered features. They are off until you turn them on, and they are built to share as little of your data as possible.

Three product features use AI: **AI Insights** (explains why a test failed and suggests fixes), **codeless AI testing** (turns plain-language intent into automated test steps) and **AI/MCP integrations** (connect TestingBot to AI agents through our MCP server).

Our AI data guarantees

- **Opt-in only.** AI features are off until the account owner explicitly enables them, and can be turned off at any time.
- **No model training.** Our AI subprocessors do not use data sent through their commercial APIs to train their models.
- **Minimized and masked.** Only a small, text-only slice of the test is sent. Detectable secrets and PII, such as API keys, tokens, passwords, authorization and cookie headers, private keys, email addresses and card-shaped values, are masked before anything leaves our servers.
- **Short retention.** The provider deletes inputs and outputs within 30 days; the generated analysis is pruned together with the test on our side.
- **Named subprocessors.** Anthropic and OpenAI (United States), under their Data Processing Addenda with EU Standard Contractual Clauses.

No video, screenshots or binary artefacts are ever sent to AI providers; the payload is text-only. Masking happens on TestingBot infrastructure, before any data leaves the EU.

> A detailed description of what AI Insights sends and stores is published at testingbot.com/support/ai/insights. Subprocessor additions for AI features are announced in the public change log with prior notice.

SECTION 09

Organizational security

Security is embedded in how the team works: least privilege by default, from hiring to offboarding.

Access control

- **Role-based, least-privilege access:** employees and systems only receive access to the specific micro-services and data they need for their role.
- **Access lifecycle:** access is granted at onboarding and removed at offboarding, following a documented checklist.
- **MFA on administrative access:** administrative access to production systems requires multi-factor authentication.

People

All TestingBot employees are required to sign a non-disclosure agreement, protecting the confidentiality of our code and our customers' data. The team receives security awareness training, and strict password policies and guidelines apply to all internal accounts.

Assets & change management

We maintain an inventory of hardware and software assets. All changes to our software are tracked in version control; we keep a record of every change, who made it and when. Access to the codebase is governed by the same least-privilege policies as production access.

Vendor management

Subprocessors are vetted before onboarding, with an EU-first selection policy: where an EU-based supplier can deliver the capability, we prefer it. The current subprocessor list, including what data each vendor processes, is published on our Trust Center and reproduced in section 12. Changes are announced through a public change log, which serves as the prior notice required by our DPA.

SECTION 10

Network & software security

A hardened, minimal production platform, continuously scanned and independently tested.

Server platform

TestingBot runs its service on **Ubuntu LTS**, chosen for its long-term support track record with security patches and upgrades. Servers are kept up to date with security patches.

Servers are accessible only via SSH, and employees authenticate with their own private key; password-based SSH login is not used. Servers acting as hypervisors for the VMs are not connected to or accessible from the public internet; they can only be reached by TestingBot employees over SSH.

Vulnerability management

- **Vulnerability scanning:** we regularly scan our websites and services for SQL injection, cross-site scripting and other classes of vulnerabilities.
- **Dependency monitoring:** third-party libraries and dependencies are monitored for known vulnerabilities and updated when advisories are published.
- **Penetration testing:** we periodically engage third parties to perform penetration testing against our services.
- **Independent rating:** our external security posture is continuously rated by Bitsight.

Secure development

TestingBot follows software security best practices, including template escaping against XSS, parameterized database access, and the use of vetted, maintained libraries. Changes are reviewed before deployment and tracked in version control.

> Found a vulnerability? We operate a responsible disclosure program; see section 14.

SECTION 11

Datacenter security, continuity & incident response

Datacenter security

Our primary datacenter is located in Brussels, Belgium and is **ISO 9001 and ISO 27001 certified**; additional capacity runs in EU datacenters in Finland, Germany and Switzerland. All servers and devices are located in secure, restricted areas, accessible only to a select number of TestingBot employees. The facilities provide 24/7 on-site security and monitoring, engineering personnel and access controls, with redundant fiber, power and cooling systems.

Business continuity & disaster recovery

We perform nightly backups of our system software to a SAN, replicated to an AWS EU region. Backups are encrypted, monitored and tested regularly. A documented business continuity and disaster recovery plan describes how we recover data and resume service after a major system failure in the least amount of time.

Monitoring & incident response

- **24/7 monitoring:** an extensive monitoring system watches infrastructure and application health around the clock and alerts engineers when incidents occur.
- **On-call rotation:** engineers are on an on-call schedule and are responsible for addressing any issue impacting the service.
- **Documented process:** incidents are handled through a documented incident response process covering triage, containment, remediation and post-incident review.
- **Transparent communication:** customers are informed of system incidents via our public status page at status.testingbot.com, which also publishes historical uptime.

> TestingBot commits to a **99.99% uptime SLA**. Live and historical availability is public at status.testingbot.com.

SECTION 12

Subprocessors

The third parties TestingBot uses to deliver the service, selected with an EU-first policy.

GENERAL SUBPROCESSORS

VENDOR	PURPOSE & DATA PROCESSED	LOCATION
Sentry	Error tracking Application error reports; may include an account email or IP address in stack-trace context. No test artefacts.	Europe
Cloudflare	CDN, security and storage Request metadata and IP addresses for CDN and WAF; cached static assets.	USA
Unix-Solutions	Hosting (Belgium) Hosts our EU infrastructure; account and test data at rest, encrypted.	Europe
Hetzner	Hosting (Germany) Hosts our EU infrastructure; account and test data at rest, encrypted.	Europe
Amazon Web Services	Storage Encrypted test artefacts (video, screenshots, logs) stored in the EU region.	Europe
Google Cloud	Geolocation testing + AI testing Geolocation test routing; for AI features, masked text-only test logs. No model training.	Europe and USA
Stripe	Payment processing Billing contact and card handled by Stripe; we store the last 4 digits only, never the full card.	USA
ActiveCampaign	Email delivery Account name and email address for transactional and product emails.	USA
Intercom	Customer support Name, email address and the content of support conversations.	USA

FEATURE-SPECIFIC SUBPROCESSORS

VENDOR	PURPOSE & DATA PROCESSED	LOCATION
OpenAI	AI testing Masked, text-only test context for codeless AI test generation. Opt-in. No model training.	USA
Anthropic	AI test failure analysis (AI Insights) Masked, text-only failing-test logs for failure analysis. Opt-in. No model training; deleted within 30 days.	USA

Subprocessor changes are announced at testingbot.com/sub-processor-updates, where you can also subscribe to update notifications. The change log serves as the prior notice defined in our DPA.

SECTION 13

Data we collect, and data we don't

We keep the data footprint as small as possible. This is the explicit list.

✓ **Employee business-card information**
Name, email, phone. Used to manage your account.

✗ **End-user personally identifiable information**
We do not collect end-user PII from your tests.

✗ **Credit card information**
Processed directly by Stripe. We never see your card; only the last 4 digits are stored.

✗ **Personal health information**
Out of scope. We are not a healthcare service.

✗ **Source code**
Not collected. Your test code stays in your CI/CD.

✗ **End-user passwords**
Not collected, not logged, not transcribed.

A Data Processing Addendum incorporating the EU Standard Contractual Clauses is available for download on our Trust Center, together with our Technical & Organizational Measures (TOMs).

SECTION 14

Responsible disclosure

We welcome reports from security researchers. If you believe you have found a vulnerability in a TestingBot product or web property:

- Report it to info@testingbot.com; our machine-readable policy is published in `security.txt` on our domain.
- Our security team responds within **one business day**.
- We do not operate a paid bug bounty, but with your permission we credit researchers in our hall of fame.
- Please act in good faith: no service disruption, no access to other customers' data, and give us reasonable time to remediate before public disclosure.

TestingBot

Secure testing, built in Europe.

TestingBot provides a secure computing cloud for teams that run automated and manual tests on real browsers, real devices and real platforms. Our service removes the cost and effort of running an internal test grid or device lab, without giving up control over where your data lives or how it is protected.

We take security seriously at every layer: single-use test environments, EU-only encrypted storage, least-privilege operations and independent verification of our posture.

TRUST.TESTINGBOT.COM

Questions for our security team?

Contact us at testingbot.com/contact/new or info@testingbot.com.

TestingBot
Vlinderhof 18, 9180 Moerbeke-Waas, Belgium
+1 (855) 410-0024

Version 2026.07 · This document is reviewed and updated periodically. The most recent version is always available at trust.testingbot.com.