BrowserStack Security

Absolute security and compliance, guaranteed

BrowserStack

Executive Summary

This document is designed to give you an overview of our privacy and security processes, outlining how your data is kept safe and secure when you use BrowserStack.

In the document, we showcase our Security Compliance and Certifications such as our SOC2 compliance and GDPR compliance, as well as our default HTTPS implementation. In the Data Controls section, we cover our policies around third-party access to data, how data is secured during tests, security of physical devices, and data retention.

We then outline how our Identity Access Management policy monitors, grants, or restricts entry into BrowserStack's cloud infrastructure. We also explain how Local Testing works and how we ensure security while testing from your private networks on the BrowserStack Cloud.

The following section on Remote Testing revolves around subjects like privacy and device clean up after each test session, security and privacy of browsing data, virtual and physical devices. In addition, we also highlight our processes around secure storage of BrowserStack credentials, security of account information and usage logs, destruction of browsing data, and test history. Our best practices relating to server patch management and change management are also mentioned in this section.

Lastly, we summarize our policies around our Data Centers, Sub-processors, Penetration Tests, and our Business Continuity Plan in the rare case of a business disruption.

Overall, this document is meant to answer all your security-related queries. We are confident in the robustness of our comprehensive security policies, and we hope to reflect our security posture through this document.

We look forward to partnering with you and enabling you to create awesome customer experiences using our safe and secure infrastructure.

Security Compliance and Certification

BrowserStack has the following certifications to ensure that your data is secured as per international standards.

SOC2 Compliance

BrowserStack is SOC2 Type 2 compliant, and we are audited annually to check if your data is managed securely. Our SOC2 compliance also ensures that yours and your organization's privacy is protected. Our SOC2 compliance extends to all the products we provide.

- We comply with 3 Trust Service criteria that ensure the security, availability, and confidentiality of your data.
- Our certification ensures that we monitor unusual system activity, authorized and unauthorized configuration changes, and user access levels.
- In the rare event of a security incident, we have meticulous alerting procedures in place.

GDPR Compliance

BrowserStack's privacy policy is in compliance with the GDPR regulation. In accordance with the General Data Protection Regulation (EU) 2016/679, we guarantee the protection of your data.

- GDPR compliance requires Data Privacy Impact Assessment (DPIA), a process that helps in identifying and minimizing risks related to data processing.
- Employee training and policies are in place for data retention, personal data collecting and processing, notices, and consent.
- GDPR compliance covers all your account-related information and customer content.

HTTPS Implementation

To ensure that users run their tests more securely, we have implemented HTTPS by default. This means that every time you communicate with BrowserStack, you will be redirected through a secure connection using HTTPS. It uses Transport Layer Security (TLS 1.2 and greater), formerly known as Secure Sockets Layer (SSL), and makes the communication between your browser and BrowserStack servers more secure.

- Every time you communicate with us, you are redirected through secure TLS (Transport Layer Security).
- Our HTTPS implementation guarantees the protection of the privacy and integrity of your data in transit.
- HTTPS is a bidirectional encryption that prevents eavesdropping and tampering of any communication.

Data Controls

At BrowserStack, data is governed and managed in accordance with global benchmarks. This safeguards sensitive and important information against unauthorized access and use. BrowserStack may obtain technical data about customers' use of our services that is non-personally identifiable. This usage data may be used to analyze, improve, market, support, and operate our services.

Third-Party Access to Data

BrowserStack does not sell customer data, or provide third parties access to production systems.

- Access to data is restricted to authorized applications, and only through access control processes.
- No confidential customer-related data is stored on our network nor do BrowserStack employees or administrators have access to the testing data or any other data while customers are testing; except for system administration, investigation and debugging. Apps uploaded by customers are stored on cloud.

Security of Data in Testing

We recommend that our customers only use test data (sanitized data sets that protect personally identifiable information).

- BrowserStack has no access to customers' test data in test sessions created by customers, except for system administration, investigation and debugging.
- Customer data is encrypted at rest using AES 256 encryption, and with HTTPS (TLS 1.2 and greater) during transit.

Device Security

- All our Android and iOS mobile devices are real devices hosted in our data centers.
- The physical devices are stored in locations with top-rate security policies and procedures, with stringent access controls.
- Only authorized personnel are allowed to handle the devices, and that too for routine tasks such as maintenance and upkeep.

Data Retention

- Test session data such as logs, screenshots, etc. are saved to BrowserStack's databases and viewable via customers' dashboards.
- Test data logs are stored for 30 days.
- App data is stored for 60 days from last usage (as per the timestamp), before being automatically deleted.
- Other data on the device (downloads, cookies, etc.) is removed during the post-test teardown process.
- Users can also prematurely delete test session artifacts from our product dashboards OR via our REST APIs (Automate REST API documentation, App Automate REST API documentation).
- GDPR User deletion: Users can request for complete removal of their BrowserStack account information by emailing support@browserstack.com.

Single Sign On

We Provide SSO via SAML 2.0 as a part of our Enterprise Edition.

- Control access to BrowserStack via your IdP.
- Enable your users to be automatically signed-in to BrowserStack with their IdP accounts.
- Manage your accounts in one central location - the IdP.

Currently, you can setup connector with the following IdPs from your BrowserStack dashboard:
1. Azure AD (SAML) 2. ADFS (SAML) 3. Okta (SAML) 4. OneLogin (SAML)

Identity Access Management

BrowserStack's Identity Access Management systems log every entry into the cloud infrastructure.

- We provide a role-based administration system for all user accounts.
- There are 3 roles: owner, admin, and user; each with different permissions.
- The administrators of the account (owner and other admins) can control user activity at will, even to the extent of prohibiting team members from accessing BrowserStack products.

Local Testing

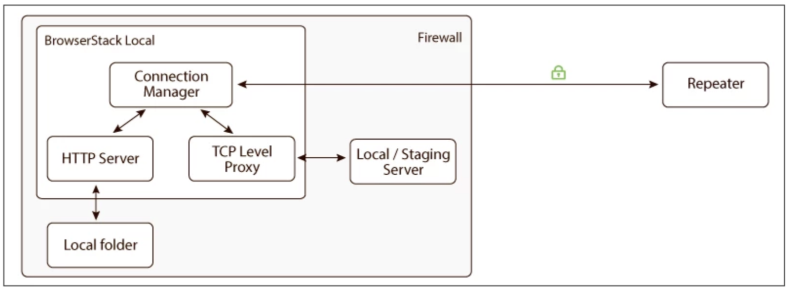
With Local Testing, you can test private servers - or web design folders hosted on private networks - using BrowserStack's cloud infrastructure. The feature lets you test work-in-progress web and mobile apps at scale without hosting them on public staging environments. We do this with our app, our binary, or our Chrome extension.

Our custom-designed Chrome extension with WSS (secure WebSockets) connects your machine to the cloud. WebSockets allows extensive interaction between the client browser and the servers and devices.

- When testing on a private server, we forge a connection between the server you have specified and our virtual machines or physical devices.
- To protect the privacy of transferred data during the testing session, we use WSS exclusively.
- WSS uses Secure Sockets Layer over port 443 for transport and therefore only transmits encrypted data
- The mechanism is set up to forward requests and responses back and forth, and nothing else.
- Similarly, for local folder testing, the BrowserStack Cloud only has access to the folder mentioned during the setup of the connection.
- Our infrastructure cannot access anything else on your filesystem.
- Local Testing supports HTTPS, and content served from multiple servers.
- The Local binary, which allows you to test development environments which are not publicly accessible on the Internet, automatically checks for the newest binary version available and self-updates on every restart.

- We regularly update binary release notes and bug fixes on our website.

Internal Architecture of BrowserStack Local



Learn more about Local Testing internals and security.

Remote Testing Sessions

Remote testing sessions establish a connection between your computer and the BrowserStack Cloud, allowing you to test your website on secure virtual machines and physical mobile devices. Each virtual machine is a fresh instance. This guarantees not only a tamper-proof environment but also a consistent baseline for test scenarios. Physical devices undergo a comprehensive clean up process after each testing session.

- To make testing as easy as possible, data is transferred from your machine to the server. This data is encrypted, so as not to be accessible whilst in transit.
- Also, all transactions take place from within the browser itself. This eliminates the need for any additional setup on the devices.
- In the event that you are testing from behind a firewall, BrowserStack does not require any special rules to operate successfully.
- We use HTTPS and WSS, both of which are standard web protocols, allowed universally by firewalls. Therefore, your existing security is left unaffected.

Privacy and Device Cleaning after each Session

We guarantee that every test runs on a tamper-proof real device. Each device is in a highly secure network, behind strong firewalls. Our users are not allowed to install programs on the devices, other than the ones intended for testing.

- Our devices are stored in locations with stringent security, where access is highly restricted.
- Only authorized personnel can handle the devices, and for maintenance and upkeep only.
- After every session, the devices undergo a thorough clean up process where apps installed, temporary file caches, browsing history, cookies, passwords, testing logs, and downloads are erased.

Browsing Data Security and Privacy Policy

BrowserStack does not have any mechanism to view or store user browsing data. All data is erased as soon as the session ends.

- Our restoration mechanisms for remote mobile and desktop browsers are stringent and extremely thorough, ensuring that all browsing data is effectively erased.
- This includes user-installed apps, the temporary cache of files, the browsing history, any cookies generated during the testing session, passwords and other form data, testing logs, and all downloads.

Virtual Machines Privacy and Security

Each time a new testing session is created, the BrowserStack Cloud assigns the user a virtual machine. After sessions, our machines are restored to their original states, which means their registry contents and caches are erased, cookies are deleted, and all running processes are killed.

At any given time, you have sole access to a virtual machine. Your testing session cannot be seen or accessed by other users, including BrowserStack administrators.

Once you release a virtual machine, it is taken off the grid and restored to its initial settings. All your data is erased in this process.

- Each time a test is run, the default settings are restored, providing an ideal test environment.
- Once the restoration process is complete, the virtual machine is then put through a series of validation checks, as a fail-safe mechanism. In the rare case that the virtual machine fails even a single check, it is taken off the infrastructure altogether.
- The machines themselves are in a secure network, and behind strong firewalls to present the safest environment possible.

Secure Hosting for Virtual Machines and Physical Devices

BrowserStack partners with only the best hosting providers across the globe, and our machines and devices are located in secure locations in the US, EU, India, and Australia. Our data centers are listed here. Our selection process is exacting, focussing on excellent service records and established security policies.

- Each service provider has implemented security with a view to protecting all those using their cloud.
- Many have had their security policies independently audited from an external authority, and have been certified under major compliance regulators. One of our providers is AWS.
- We ensure that the BrowserStack infrastructure is protected from the ground up.
- Starting from physical security, we constantly improve security policies as the threat landscape changes.
- Our priority is to protect the integrity of your data, and guard against any service interruptions.

Secure Storage of BrowserStack Credentials

- Your account information such as your username, logins, password, access keys, and account details, are stored in an encrypted format on our systems.
- We use SSL to transmit information back and forth from our servers.
- BrowserStack cannot view any of your credentials, so much so that if you lose your password, it must go through the reset procedure for your account to be accessible again.
- The same policies are applied to all payment details. We have partnered with the reputable credit card processor - Stripe.

Security of Account Information and Usage Logs

Your account information is encrypted before it is stored. We cannot view any of your credentials, even in the case of an emergency.

- Our data encryption and privacy policies apply to all payment details.
- Test history and log data are stored in a secure database on our cloud.
- A highly encrypted access mechanism grants data access to you and only you.

Destruction of Browsing Data

We guarantee that we have no way to view or store your browsing data. As soon as you end an active session, all user data is erased.

- Our restoration mechanism for remote mobile and desktop browsers is extremely thorough.
- We erase all browsing data as soon as a user’s session ends.
- The data erased include apps installed, temporary file caches, browsing history, cookies, passwords, testing logs, and downloads.

General Usage Logs and Test History

All BrowserStack products generate usage logs, which are used for analytical purposes. These usage logs do not contain any personal data about the user nor any browsing data generated during tests.

- Test history can be generated in the form of screenshots and log data.
- Test history is stored in a secure database on our cloud and is only accessible to you, via your BrowserStack account.

Server Patch Management

- BrowserStack ensures that all patches to network device/server operating systems are checked for stability and any availability issues, and tested before applying to the production environment.
- All the critical and security patches are applied on a priority basis.
- This ensures that your systems are not compromised due to vulnerabilities, if any, in our products.

Change Management

The Change Management process describes a methodical approach to handle the changes that are to be made to BrowserStack's systems. All the changes are subjected to a formal Change Management process.

- Change Management at BrowserStack covers system, IT infrastructure, network components, and production environment.
- All major changes are initiated by appropriate personnel, analyzed for impact, tested and approved before deployment.
- Post-implementation, performance is checked as part of the Change Management process.

Data Center

- Our real devices and machines used for testing website and mobile apps are hosted in the US, EU, India, and Australia. Our data centers are listed here.
- You are automatically directed to the nearest location based on your IP.
- Our application, processing, data collection, and other supporting servers are hosted in the US and EU.
- The servers are owned by reputable vendors that have stringent security policies.
- BrowserStack has obtained and reviewed a SOC2 Type 2 report from AWS, as well as SOC2 reports or ISO 27001 certificates from other data centers.

Sub-processors

BrowserStack engages with a number of third-party Sub-processors after conducting diligence to evaluate their security, privacy and confidentiality practices. In line with GDPR, our sub-processors comply with GDPR accountability obligations.

- A list of the categories of Sub-processors used by BrowserStack is maintained on BrowserStack's website.
- We notify customers of changes in our sub-processing arrangements, if any, by publishing details on our website. Customers then have a 10-day period to exercise their Right of Objection.
- In case of customer objection to our sub-processing arrangements, it must be brought to BrowserStack's notice immediately.
- Our subprocessors are listed here.

Penetration Tests

To ensure that we are up-to-date with our security policies, Penetration Tests on both - the network and the application - are conducted annually by a third party.

Business Continuity and Disaster Recovery

- BrowserStack's business continuity and disaster recovery plans, including restoration of backups, are tested annually.
- Backups are taken daily and stored on AWS's high availability Relational Database Service (Amazon RDS) platform and on Digital Ocean cloud.
- BrowserStack also has procedures for data restoration from backup files in place.
- Backups are stored in a geographically separated cloud.
- There is sufficient redundancy for data centers that provide machines for customer testing. If a data center (or a part of it) is down, the load shifts to other data centers automatically.

Incident Response

As BrowserStack is GDPR compliant, we have incident and risk management protocols in effect.

- When an incident is detected or reported, a defined incident response process is initiated by authorized personnel.
- Corrective actions are implemented in accordance with defined policies and procedures. BrowserStack production systems are monitored by BrowserStack.
- Any incident (outage, bug, security vulnerability, etc.) noticed or reported will trigger the Incident Response Process.
- As per GDPR guidelines, we have a 72-hour response window.

Closing note

Your data is safe and secure when you use BrowserStack. We guarantee this. You can read more about our Security Policy, Privacy Policy, Terms of Service, Cookie Policy, and Candidate Data Protection Policy.

Alternatively, you can get in touch with our Account Executives in case of further queries.

About us

BrowserStack is the world's leading software testing platform powering over two million tests every day across 15 global data centers. We help Tesco, Shell, NVIDIA, Discovery, Wells Fargo, and over 50,000 customers deliver quality software at speed by moving testing to our Cloud. Our platform provides instant access to 3,000+ real mobile devices and browsers on a highly reliable cloud infrastructure that effortlessly scales as testing needs grow. With BrowserStack, Dev and QA teams can move fast while delivering an amazing experience for every customer.

Founded in 2011, BrowserStack is a privately held company backed by Accel, BOND Capital, and Insight Partners with offices in San Francisco, New York, Mumbai, and Dublin. For more information, visit https://www.browserstack.com.

Trusted by global enterprises

Discovery TESCO RBS GE

AXA edmunds FT FINANCIAL TIMES match

BNP PARIBAS NVIDIA WELLS FARGO