WHITE PAPER

AN OVERVIEW OF SAUCE LABS SECURITY PROCESSES

UPDATED MAY, 2019

Enterprises large and small trust Sauce Labs to provide a secure platform for testing their web and mobile applications. Helping to protect our customers' data is of the utmost importance to us, as is maintaining customer trust and confidence. This document is an overview of the technology, processes and security operations that govern the Sauce Labs Continuous Testing Platform.

SAUCELABS

TABLE OF CONTENTS

3 Executive Summary

3 Compliance Statement

3 Data Privacy

4 E.U. GDPR / Data Residency

5 SSAE 16 / ISAE 3402 / SOC Type 2

5 Data Controls

5 3rd Party Access to Data

5 Security of Data in Testing

5 Production Access Security

5 Device Security

6 Data Retention

6 Sauce Labs Architecture

6 Cross Browser Web Testing

6 Mobile App Testing

7 Headless Testing

8 Connectivity Options

8 Sauce Connect Proxy

9 IPSEC VPN

10 Datacenter Security

10 Datacenter Offerings

11 Access Controls

11 Application Access

11 Change and Patch Management

12 Testing and Scanning

12 Disaster Recovery/Data Backup

12 Business Continuity

12 Testing and Validating Disaster Recovery

13 Incident Response

13 Additional Resources

EXECUTIVE SUMMARY

This document provides an overview of the technology, software development, and service management practices used to deliver the Sauce Labs Continuous Testing Cloud. Sauce Labs provides a secure and scalable cloud computing platform for testing web and mobile apps using both virtual and real devices.

This paper is intended for prospective customers and technology professionals focused on cloud security looking to leverage Sauce Labs as a hosted digital lab. Sauce Labs provides both a real device cloud (RDC) and a virtual device cloud (VDC) for testing digital applications. Both the RDC and VDC are multi-tenant public clouds deployed across multiple data centers globally. Global support is provided by a 24x7 operations and customer support team.

COMPLIANCE STATEMENT

Sauce Labs is a cloud-based testing lab which does not require the use of customer PII, PHI, or other sensitive data. The use of sanitized or synthetic data for testing is, in fact, considered a best practice. With the passing of the 2018 EU General Data Protection Law (GDPR), Sauce Labs classifies itself as a data processor with respect to its customers' Test Data and as a data controller with respect to its customers' Account Data (as such terms are discussed in Section 1 below). Sauce Labs continues to mature its governance program to support the evolving regulatory landscape and is pursuing a SOC2 audit and attestation. For the short term, Sauce Labs will continue to share the SOC2 reports from its data center partners upon request.

DATA PRIVACY

In providing its continuous testing cloud service, Sauce Labs receives two categories of data from its customers. The first category consists of data about our customers' access to and use of our service, and includes information about the specific customer employees or contractors that use our service. We refer to this data as "Account Data." The second category consists of the data that our customers upload to our service or that is otherwise accessed by our service in the course of testing customer applications, and the reports, logs, and other artifacts of such testing that are generated by our service. Our service operates by processing what a user's computer or device would process when accessing and using a web or native mobile application, which typically includes the customer's compiled web application rendered in a browser or executable native mobile application installed in a real or virtual device, and the test script or commands and data

inputs to manipulate the browser or application that is being tested, to mimic user behavior. Our service also generates artifacts from tests that are run, including images and videos of the application as the test is conducted, and reports, logs and analysis of the test results, We refer to this data as "Test Data." In general, Test Data need not and should not include any sensitive or personal data regarding customer personnel, customers or end users.

The Sauce Labs service is a test execution environment and is not intended as a production environment or "system of record" for any customer data (beyond data related to the tests themselves). All test logs, images and videos of applications being tested, and related reports and analysis, are automatically deleted from our service 30 days after they are generated by default, and our customers have access to and the ability to manually delete any or all such data at any time.

Sauce Labs has implemented and maintains a data privacy compliance program intended to comply with applicable requirements of the GDPR. Among other things, we:

- Maintain policies, procedures and protocols to ensure that we only process personal data lawfully, fairly, transparently, and in accordance with other privacy standards set forth in the GDPR;
- Select vendors that have implemented robust data protection measures and execute data processing and sub-processing agreements with them as appropriate;
- Offer assistance to customers to give effect to data subject rights and comply with relevant requirements under the GDPR as appropriate;
- Design our services and internal systems with data privacy principles in mind; and,
- Implement and maintain reasonable and appropriate technical, physical and organizational security measures to protect the data that we process.

We can provide additional information about our data privacy practices on request.

E.U. GDPR / Data Residency

Adhering to the GDPR, Sauce Labs works with customers to ensure that an appropriate mechanism is implemented to legitimate transfers of personal data outside of the European Union. Sauce Labs offers EU customers service

from data centers and storage infrastructure located in Europe, which avoids the need to transfer customers' raw Test Data (including any personal data therein) outside of the EU.

All deployments are supported by a global support team based in the U.S., and customer Account Data is also generally transferred to the U.S.

SSAE 16 / ISAE 3402 / SOC Type 2

Sauce Labs currently does not have its own SOC 2 report but we continue to pursue readiness. For the short term, Sauce Labs will continue to provide attestation reports for its various colocation partners.

DATA CONTROLS

For data in flight, customers may choose to access Sauce Labs via Sauce Connect (SSL Proxy) or IPSec VPN. Both options support secure connectivity using TLS 1.2 or above.

For data at rest, all data is encrypted using AES 256.

3rd Party Access to Data

Sauce Labs does not share customer data or provide 3rd parties access to production systems. Contractual agreements are in place with specific vendors/partners who provide support services to Sauce Labs (e.g., hosting and code repositories). All such agreements are reviewed at least annually by the Sauce Labs legal team.

Security of Data in Testing

Sauce Labs encourages customers to test using only non-sensitive or sanitized datasets. Sauce Labs considers all data as sensitive and therefore encrypts data at rest (AES256) and in motion (TLS 1.2) using Sauce Connect Proxy or IPSec VPN.

Production Access Security

Production access is limited to dedicated VLANs, systems, and admin privileges using multi-factor authentication. All activity is logged and reviewed on an ongoing basis. Any abnormal activity may trigger an incident to be reviewed by Security Operations.

Device Security

Devices in the real device cloud (RDC) are deployed in a multitenant environment. "Public" devices are shared and assigned on a per use basis

to users. Public pool devices are reset after test sessions using automated scripts. See Real Devices and Security

Virtual device cloud (VDC) is also deployed in a multitenant environment. Browser/OS combinations or emulator/simulator devices are provisioned on demand in virtual machines and destroyed at the end of every test execution.

Data Retention

Sauce Labs collects test data assets from individual tests that are being run on our platform. These assets include Selenium/Appium logs, screenshots, a video of the test, and metadata.

All test execution reports are available from the Sauce Labs user interface. Test execution reports and other Test Data assets are stored for 30 days and then automatically deleted. Customers who require longer data retention periods are encouraged to download their data directly.

SAUCE LABS ARCHITECTURE

Sauce Labs ensures that customer websites and mobile apps work flawlessly on every browser, OS and device. The company's Continuous Testing Cloud helps organizations accelerate software development cycles, improve application quality, and deploy with confidence across hundreds of browser / OS platforms, including Windows, Linux, iOS, Android & Mac OS X. Optimized for Continuous Integration (CI), Continuous Delivery (CD), and DevOps, the Sauce Labs platform is designed to ensure the highest level of security. Figure 1 below illustrates the data flow across the Sauce Labs solution in relation to a customer application.

Cross Browser Web Testing

Sauce Labs gives users the ability to run manual and automated functional tests written with Selenium and Appium across more than 800 browser and OS combinations. The platform eliminates the need to build and maintain an on-premise test grid, and provides the ability to run cross-browser tests in parallel, significantly reducing the time it takes to execute these tests. Results can be analyzed using videos, screenshots, log files and Test Analytics to quickly identify test patterns and resolve defects, enabling faster release cycles.

Mobile App Testing

Sauce Labs users can test mobile native, hybrid and web apps across real devices as well as hundreds of iOS simulators and Android emulators. Mobile

app tests can be conducted manually ("live" testing) to spot check issues, or automated using the Appium, Espresso or XCUITest test frameworks. Mobile tests can be run on a public real device cloud across thousands of devices, or on a private cloud, with unique devices dedicated to individual customers.

Headless Testing

Cross-browser testing on virtual machines is useful for uncovering unexpected behaviors for specific browser and operating system combinations. Headless testing, however, is run without the browser's graphical user interface and is more useful for (a) testing specific application components, (b) obtaining rapid test feedback, or (c) when you want to quickly and efficiently scale the number of tests you are running. Sauce Labs uses a container-based architecture to host our headless browsers, resulting in fast spin up times and low network communications latency.

All database access is managed through an object relational and service application model. Users are assigned a unique ID and access key. Data access is limited to data associated with a specific account.

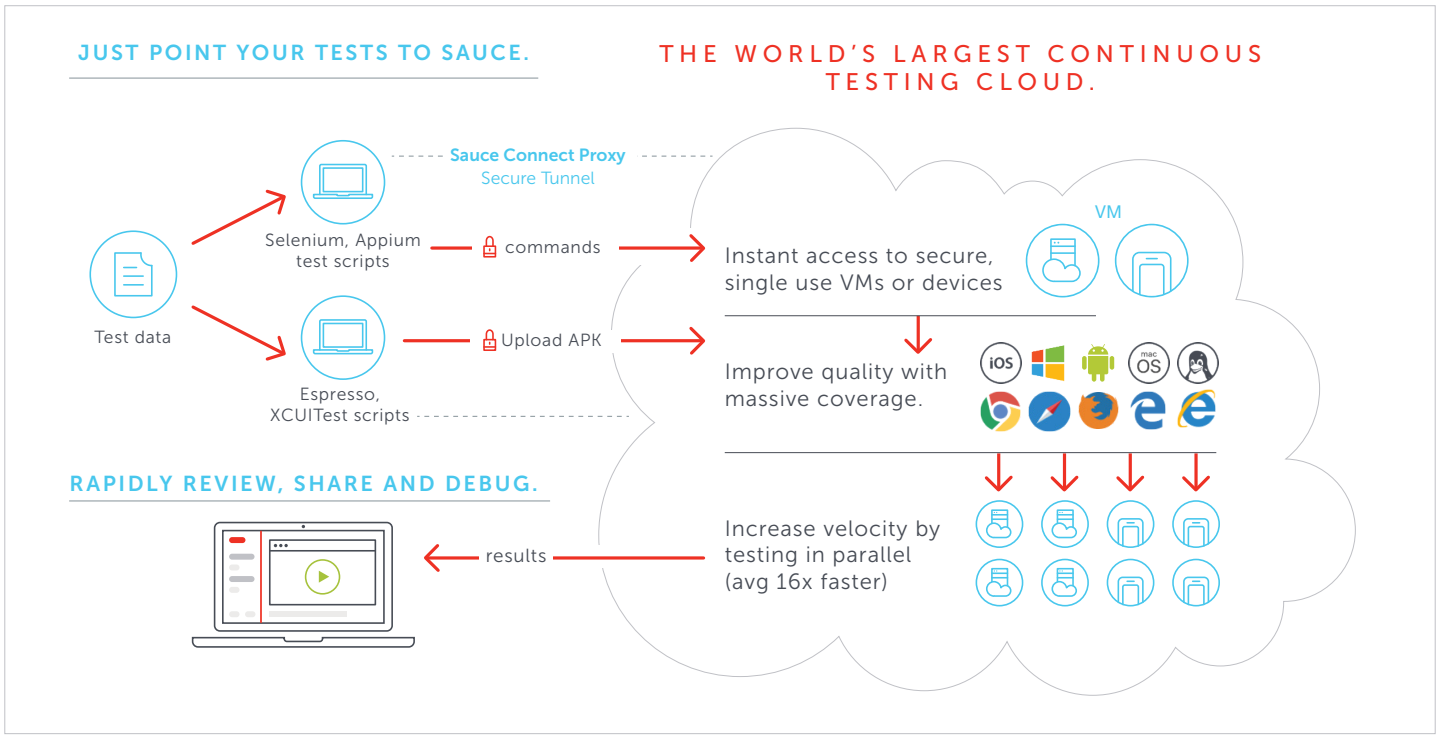

Figure 1: High Level Data Flow

CONNECTIVITY OPTIONS

Sauce Labs supports two connection options - IPSec VPN or TLS-protected proxy connections using Sauce Connect local client. The following sections provide a brief overview.

Sauce Connect Proxy and IPSec VPN solve the same problem, which is to establish a secure connection between applications hosted on an internal server and the Sauce Labs virtual machines or real devices that are used for testing. The difference is that IPSec VPN is based on an industry standard, while Sauce Connect Proxy is based on a proprietary protocol that runs over TLS. Sauce Connect Proxy is available for use by any Sauce Labs account, while IPSec VPN is a feature that requires an additional fee.

Sauce Connect Proxy

Sauce Connect Proxy™ is a proxy server that opens a secure connection between a Sauce Labs virtual machine running your browser tests, and an application or website you want to test that's on your local machine or behind a corporate firewall. Figure 2 below illustrates the architecture of the solution. Sauce Connect is not required to run tests with Sauce Labs, but only in situations where the website or application you want to test is not publicly accessible. It is strongly recommended that you work with a network engineer to install Sauce Connect, as network architectures can be complex.

In addition to providing a means for Sauce Labs to access your application or website, Sauce Connect has some other uses in your testing network architecture:

- As an alternative to whitelisting;
- As a means of monitoring upstream traffic through a proxy like BrowserMob;
- As a way to stabilize network connections (for instance, detecting/re-sending dropped packets).

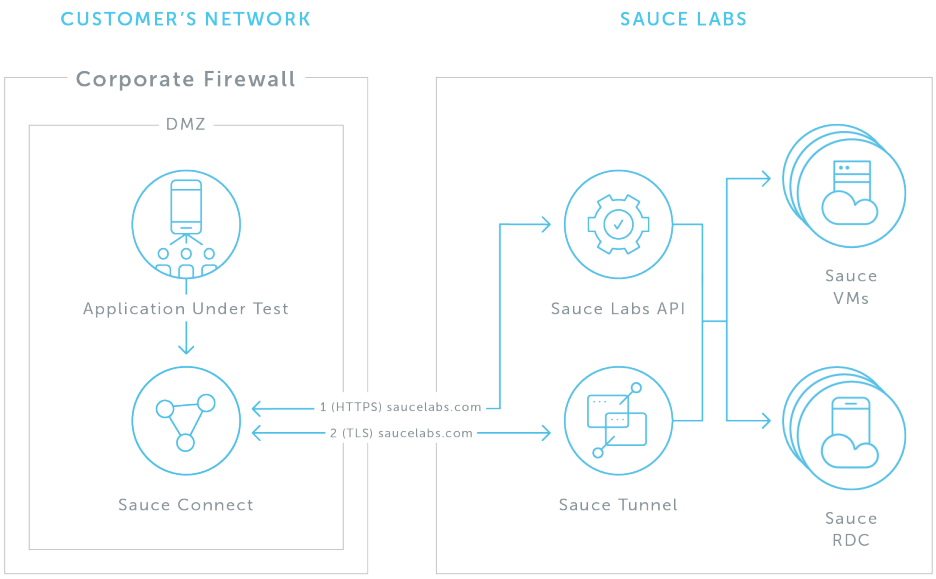

Figure 2: Sauce Connect Data Flow

IPSEC VPN

IPSec VPN allows test virtual machines in the Sauce Labs network to access application servers in customer's private network. However, IPSec VPN doesn't allow application servers to access Sauce test VMs. Figure 3 illustrates the architecture of IPSec VPN solution. The solution consists of two components, a VPN connection between two IPSec gateways, and a tunnel gateway.

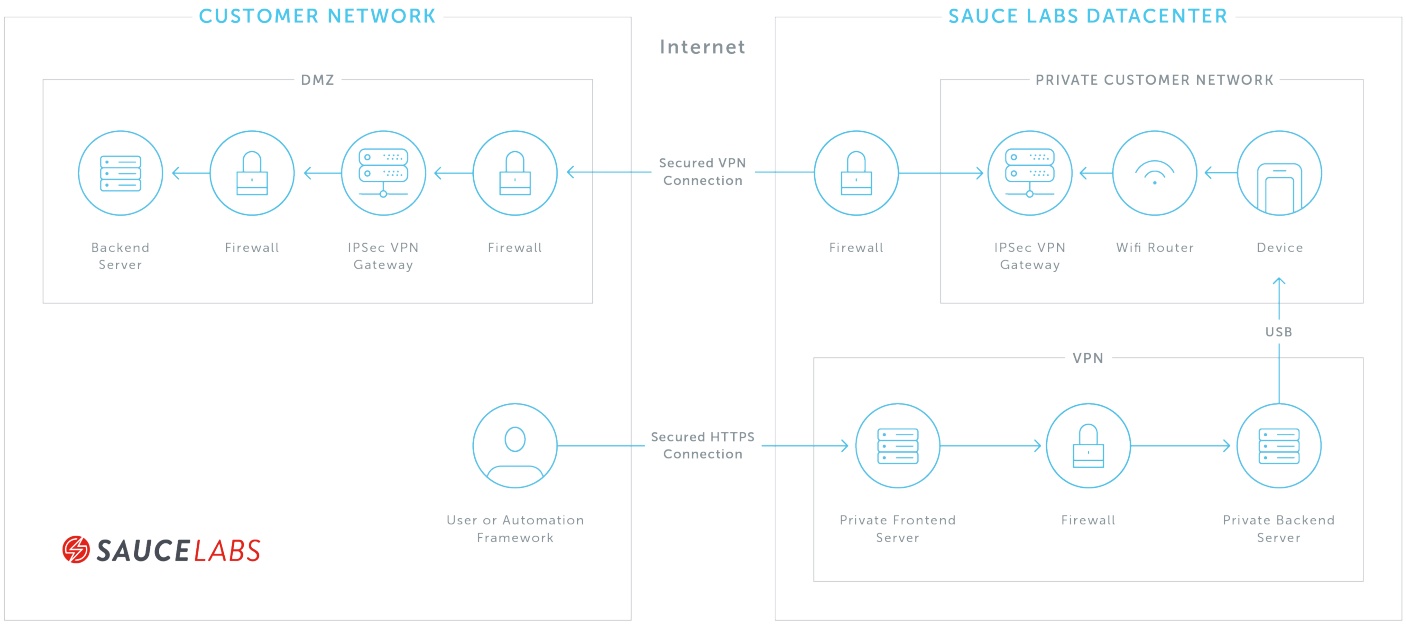

Figure 3: IPSec VPN Data Flow

The tunnel gateway is always on for the lifetime of the IPSec VPN connection, and plays an important role in DNS resolution, routing and security.

The tunnel gateway runs a firewall and only authorized test VMs are allowed to connect through the firewall. Authorized test VMs include:

- Test VMs created by the IPSec VPN tunnel owner
- Test VMs created by accounts with which the tunnel is shared
- All incoming connections from test VMs are blocked.
- The firewall allows these ports and protocols through the IPSec VPN connection as identified in Figure 4.

Direction	Protocol(s)
Outbound from Sauce	HTTP (TCP/80), HTTPS (TCP/443)
Outbound from Sauce	DNS (UDP/53, TCP/53, TCP/853)
Outbound from Sauce	Web Proxy (TCP/8080, TCP/8443)
Inbound from customer network	BGP (TCP/179)
Inbound from customer network	ICMP

Figure 4: IPSEC VPN Ports

DATA CENTER SECURITY

Sauce Labs leverages multiple data center locations in Santa Clara California, Las Vegas, Nevada, Frankfurt and Berlin Germany. US data centers are owned by Switch, Internap, Equinix, and Zayo. We use Equinix and eShelter colocation facilities in Germany. We also deploy various types of virtual machine workloads within the Google Compute Platform in available U.S. regions. Data center partners restrict access to premises, provide surveillance and a dedicated, secure cage for Sauce Labs infrastructure. All customer Test Data, primary and backup, is stored in AWS S3 buckets. All Sauce Labs hardware within the data centers is owned and managed by Sauce Labs with the exception of a private cloud of dedicated Apple Mac hardware co-located with Zayo Group and used to host workloads requiring MacOS.

Datacenter Offerings

Sauce Labs offers both virtual (VDC) and physical device clouds (RDC). Figure 5 provides an overview of which offerings are available from specific locations.

Data Center	RDC	VDC
Las Vegas, NV		×
Berlin, Germany	×	
Frankfurt, Germany		×
Santa Clara, CA	×	
San Jose, CA		×

Figure 5: Data Center Service Offerings

ACCESS CONTROLS

In addition to the physical security, Sauce Labs operations has implemented access control measures restricting access to customers' environments to only those support personnel that have a documented, current business need. Furthermore, all physical and electronic access to data centers is logged and audited routinely.

Application Access

Application access is managed by the customer designated administrator via the Teams function within the Sauce Labs UI. Teams allows for the authorization of individuals, and roles to access the customer's specific instance of Sauce Labs and report data. Additional support for single sign-on (SSO) integration with a customer's existing identity management solution is also available.

CHANGE AND PATCH MANAGEMENT

Sauce Labs updates all security tools and software, as needed, using appropriate patches. All critical patches are installed based on risk, per the Sauce Labs Change Management Policy, and with approval from the Sauce Labs change management team.

Changes are efficiently and securely planned, reviewed, tested, implemented, and validated to ensure that all environments are protected. Example processes include:

- Operational staff handle server software provisioning and configuration tasks.
- Sauce Labs code is deployed via continuous integration systems backed by source code management.
- System masters are hardened and pen-tested before deployment into production.

TESTING AND SCANNING

Sauce Labs performs multiple types of testing including:

- Vulnerability scans are performed using both internal resources and 3rd-party services. Whitebox penetration testing is performed at least annually by 3rd-party specialists.
- Static and dynamic code analysis testing is performed for all code releases.
- Customers may perform or contract their own testing with prior coordination and approval from Sauce Labs Security.

DISASTER RECOVERY/DATA BACKUP

Sauce Labs provides backup and redundancy for customer data to ensure full recovery in the event of service disruption or failure.

Our primary data centers are geographically separated co-location facilities (Internap and Switch SuperNAP) with 24x7 physical security, redundant power, HVAC, ISP connections, and fire protection. Primary databases are backed up daily to Amazon S3 to satisfy our Recovery Point Objective (RPO) of 24 hours maximum. Our Recovery Time Objective (RTO) to restore data in a catastrophic data loss situation is 48 hours. Customer test results are natively stored on Amazon S3 for security and safety.

Business Continuity

Central to the company's business recovery efforts is a requirement that each Sauce Labs business unit develop, test, and maintain recovery plans for each of its core functions. As part of these plans, each business unit identifies critical risks and puts in place the appropriate level of business controls and functionality necessary to mitigate those risks. The resultant plans document the functional requirements — equipment, applications, vital records and regulatory reports, relocation sites, and recovery teams and tasks — needed to reestablish essential business operations. The plans also assess the impact of a business disruption on the company's customers and business partners.

Testing and Validating Disaster Recovery

The Sauce Labs disaster recovery, incident response, contingency planning and recovery procedures are tested and validated annually. Sauce Labs simulates customer disaster declaration scenarios that cover failures and recoveries of each of our critical systems, and then analyze the results to continuously improve our operations. Testing is performed periodically, as needed.

INCIDENT RESPONSE

Sauce Labs incident response and management includes the Sauce Labs Customer Support, Operations, and Security teams. Team members are on-call 24x7 to respond to customer support requests and incidents.

The Sauce Labs Support team consists of three tiers of technical and engineering staff to provide incident response, triage, root cause analysis, and resolution.

Response procedures include the use of standard operating procedures that are maintained and kept current in a knowledge base, escalation to higher-expertise tiers and supporting teams, and bridge calls for collaboration. This team is responsible for managing incident severity, impact, and type classification for effective prioritization of support requests and assignment of qualified experts, with supervised monitoring of support request status and progress.

The Sauce Labs operations team provides contingency and disaster recovery plan activation and escalation, in the event of a major incident affecting multiple customers. In addition, partner and vendor incident response support as needed for triage and resolution. Reporting and analysis of incident response performance metrics are used to achieve SLAs.

ADDITIONAL RESOURCES

The following wiki links are provided for additional information:

The Sauce Labs Cookbook

Maintenance Windows for Sauce Labs

Sauce Connect Proxy

IPSec VPN

Account and Team Management

Using SSO with your Sauce Labs Domain

Headless Testing

ABOUT SAUCE LABS

Sauce Labs ensures the world's leading apps and websites work flawlessly on every browser, OS and device. Its award-winning Continuous Testing Cloud provides development and quality teams with instant access to the test coverage, scalability, and analytics they need to rapidly deliver a flawless digital experience. Sauce Labs is a privately held company funded by Toba Capital, Salesforce Ventures, Centerview Capital Technology, IVP, Adams Street Partners and Riverwood Capital. For more information, please visit saucelabs.com.

saucelabs.com/signup/trial

FREE TRIAL

SAUCELABS

SAUCE LABS INC. - HQ
116 NEW MONTGOMERY STREET, 3RD FL
SAN FRANCISCO, CA 94105 USA

SAUCE LABS EUROPE GMBH
C/O WEWORK STRALAUER
ALLEE 6 10245 BERLIN DE

SAUCE LABS INC. - CANADA
134 ABBOTT ST #501
VANCOUVER, BC V6B 2K4 CANADA