WHITE PAPER

AN OVERVIEW OF SAUCE LABS SECURITY PROCESSES

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 Automated Testing Platform.

SAUCELABS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

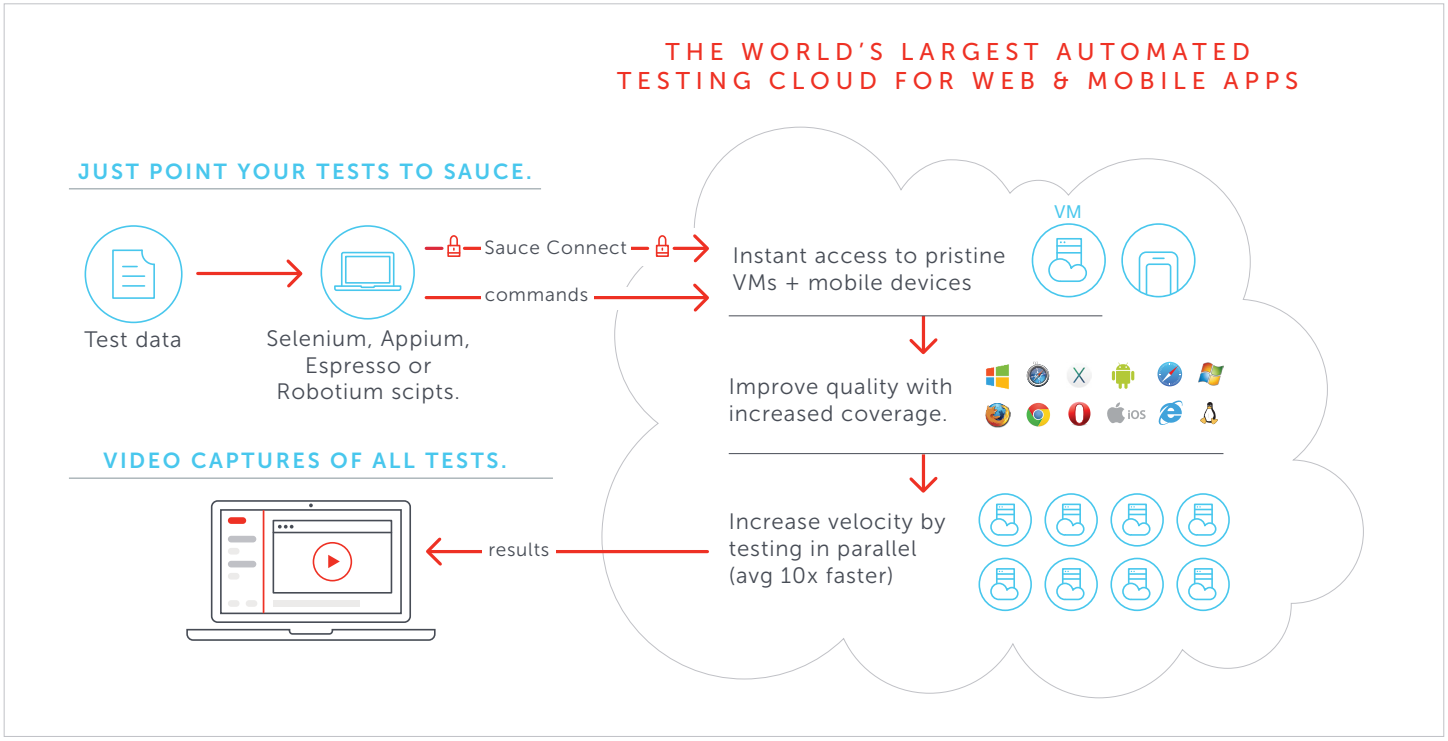
Sauce Labs provides a secure and scalable cloud computing platform for functional testing of web and mobile apps located in world-class data centers in North America and Europe. Having our own cloud enables us to provide our services faster, and with higher security, than can be delivered on a public cloud with shared resources. Managing our own data centers also means that we are responsible for delivering a consistent experience with the utmost concern for the security of our users' data. This white paper provides an overview of the services offered by Sauce Labs, an explanation of how we secure the transmission of test data and results, and our security policies and procedures.

SAUCE OVERVIEW

The Sauce Labs Automated Testing Platform is a cloud-hosted environment where we initiate browsers, mobile emulators and provision mobile devices on-demand for functional testing of web and mobile applications. We provide virtual machines with operating systems and browsers for Windows, Mac OS, Linux, Android, and iOS as well as iOS and Android mobile devices. We provision a new, pristine virtual machine for each test, and destroy it immediately afterwards so there are no residual data, temp files, or other artifacts that could interfere with a test. Mobile devices are cleaned and restored to a consistent starting configuration.

When we provision an operating system and browser, we spin up a new virtual machine (VM) that only runs for the duration of the test. VMs are never reused for multiple tests or users, and during a test all data is only recorded to RAM, never to disk. Our strategy of never allowing your data to be written to disk greatly reduces the threat that it could be accessed by unauthorized parties. Spinning up new VMs for every test is the only truly reliable way to ensure that a 3rd party cannot access your internal network, and that your data cannot be captured and sent to a 3rd party. Securing shared VMs in a multitenant environment is very difficult and requires constant active monitoring of the system. Instead, we provide a VM environment that has never been, and never will be, used by any customer besides you. Finally, our VMs are configured to not allow any external inbound connections, preventing any and all remote access.

Mobile devices are provided in public and dedicated private clouds. Public devices are commercial off-the-shelf devices that have been modified to run in a data center (pop ups are disabled). These devices are cleaned prior to reuse so all data, temp files and applications are removed and the device reset. Private devices are provisioned over a private, secure connection to



users and modified to run in the data center. Device cleaning is managed by the end user to meet their needs, data and apps can be customized and devices can be standardized to a custom starting configuration.

For virtual machine based tests, assets such as screenshots, videos, and logs, are stored in an Amazon S3 private bucket for up to 30 days, then automatically deleted. Users who are concerned about the existence of stored test assets can simply choose to disable recording of test assets. For real device tests, videos and other assets are stored in Amazon S3 as well and you can simply remove them by deleting your test results.

SAUCE TESTING OVERVIEW

You can develop functional tests in your preferred language (for example Ruby, PHP, JavaScript, or .NET), and use Selenium bindings to enable these scripts to drive your automated tests. We support a number of open source testing frameworks including: Selenium for web app testing and Appium, Espresso and Robotium for mobile app testing. Your tests scripts are run from your servers, behind your firewalls, from within your DMZ. Commands are sent to the Sauce Cloud via Sauce Connect, our secure proxy server, and are executed on the browsers and operating systems that you specify. Test results are streamed back to the Sauce admin console (and optionally recorded). Our testing architecture is unique, in that it enables you to run tests behind your firewall, using data and files that also reside within your firewall. Your

SAUCE LABS TESTING DIAGRAM

Commands from your tests are sent to our cloud and executed on pristine, new VMs or mobile devices across your target browsers and operating systems. Commands can be sent directly or securely via Sauce Connect using TLS encryption. Finally, complete test results, videos, screenshots and logs are viewed from your system.

SAUCELABS

Learn more at saucelabs.com

scripts, test code, and data never leave your servers, and any residual test data is destroyed when the operating system and browser, and the virtual machine hosting them, are destroyed, or the mobile device is cleaned, at the immediate conclusion of the test.

We currently support over 900 OS/browser combinations (including iOS Simulators and Android emulators) and over 1,000 real mobile device models in our public clouds, and are adding more on a constant basis. Because many "evergreen" operating systems and browsers release security patches only in connection with new versions, we support many combinations that do not have the latest security patches. Often these are specific combinations still in real-world use that our customers need to test against, and upgrading to apply security patches would meaningfully change the test configuration. However, all external inbound access to these VMs is disabled, preventing access to unpatched services. Additionally, our operating systems and browsers only exist for very limited, short periods of time (minutes), in private sessions that can only be accessed by the person who owns the testing account.

SAUCE CONNECT™ PROXY

Sauce Connect™ is a software proxy server that provides users with a secure way to test apps. Sauce Connect opens a secure connection between a Sauce Labs virtual machine running your browser tests, and an application, website, or data you want to test that's on your local machine or behind a corporate firewall. The Sauce Connect secure tunnel allows HTTP traffic to reach your server and communicate commands to the Sauce Cloud. Sauce Connect is not required to run tests with Sauce Labs, but only in situations where the website, application, or data 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. Extensive documentation on Sauce Connect can be found on our website.

The access that Sauce Connect has to your internal systems is completely within your control. We recommend Sauce Connect be run within a firewalled DMZ which has access only to those resources required for testing. Alternatively, Sauce Connect can be configured for use with proxies for both internal and external connections, and access can be controlled at the proxy. We also support proxy autoconfiguration.

Security was a primary concern in the choice of protocols and policies we employ for Sauce Connect. All data is encrypted when transmitted between the tunnel, VM, and Sauce Connect via industry-standard TLS (v1.2), using

the top-rated AES-256 cipher. Sauce Connect also uses a caching web proxy on the Sauce Labs side to minimize data transfer. When you connect to the Sauce Cloud using Sauce Connect, a tunnel is opened between your local server and a Sauce VM. During test runs, cached images are served to browsers running tests. Anything remaining in the cache at the end of a test run is completely destroyed when Sauce Connect is stopped.

Additionally, we designed Sauce Connect with server-side measures meant to protect your networks. Within the Sauce Labs network, Sauce Connect creates a dynamically controlled firewall that only allows VMs currently running your test to have access to the server-side of Sauce Connect. This prevents any outside connection, and any other VMs in the Sauce cloud, from connecting to a local server.

MOBILE DEVICE SECURITY

Physical Security

All real mobile devices are housed in our secure centers in California, Nevada or Germany. Only trusted Sauce Labs personnel are allowed into the data center to service our mobile devices. Mobile devices are further enclosed in device cages to prevent tampering.

Software Security

Most of our devices are purchased off-the-shelf as new and are never jailbroken so these devices are just like what your customers are buying and using. (We also support a few Android rooted devices for edge testing cases and these are clearly marked.) Mobile devices are cleaned using a proprietary cleaning script to remove any data / settings and restore them to a consistent starting configuration. Currently, we offer both manual and automated testing on iOS and Android mobile devices in both public and private clouds. This allows our users the greatest flexibility to test on devices that meet their security requirements. Dedicated private devices provide the highest level of security where users are in complete control of the apps, data and configurations their devices.

We run health checks of devices to ensure that devices are considered to be in a "healthy" state so they are ready to test. In addition, we run monitoring programs to identify and squash pop-up messages on our devices to ensure your tests don't get stopped by any messages.

Network Security

Through custom network configurations, we allow only our devices to connect to the wireless routers in the data center in order to ensure that no foreign devices can connect to the same network. The routers are also physically secured.

INFORMATION SECURITY MANAGEMENT

Sauce Labs has a documented Information Security Management Program that is updated annually. In general, we follow the ITIL v3 framework that guides our IT management practices. Further, we self-certify under the Cloud Security Alliance (cloudsecurityalliance.org); CSA STAR is the industry's most powerful program for security assurance in the cloud. STAR encompasses key principles of transparency, rigorous auditing, and harmonization of standards.

DATA CENTER SECURITY

We have 3 data centers located in Northern California, Nevada and Berlin. These are housed in secure, restricted access buildings that provide the highest levels of physical security. Our colocation providers (Internap and Switch) house our servers in a secure, restricted area accessible only by select Sauce Labs employees. The facility employs physical security including restricted access, 24 x 7 on-site security and engineering personnel, video monitoring, password / biometric access controls, and man traps with weight sensors to determine if equipment is being moved in or out of the facility.

FACILITIES AND POWER

Data center reliability is accomplished by building full overlays of electrical and mechanical systems in the colocation facilities that include redundant equipment as well as multiple distribution paths. This means that any component of data center infrastructure – whether electrical, mechanical or otherwise – can fail or be intentionally shut down without creating a disruption.

BUSINESS CONTINUITY MANAGEMENT

We have a documented plan for business continuity management that includes plans for restoring operations and ensuring availability of information following an interruption in service. We also have fail-over capabilities between our California and Nevada data centers so if there is a catastrophic failure at one, we can continue operations on the other data center.
We perform nightly backups of our system software to a SAN, replicated to a 2nd facility, and encrypted and transported to Amazon in a different region.

This gives us the ability to recover our data and resume business in the case of a major system failure in a minimum amount of time.

There is a logical separation of the Sauce Labs Cloud service from the Sauce Labs business. These are run on separate platforms so that if the business network suffers an outage it will not impact the service, nor is there any way someone could access our business systems from our service. Only a few selected individuals have access to those platforms to make changes. Strong passwords are generated for each application, and access is on a need-to-use basis.

INCIDENT RESPONSE

We monitor our testing infrastructure 24 x 7 with engineers on-call to address and drive resolution of business impacting events. We have definitions and tiers of failures that are documented that guide our response to incidents. Customers are informed of system incidents by email, by notices on their Sauce Labs dashboard,and via http://status.saucelabs.com.

NETWORK SECURITY

Sauce Labs is based on Ubuntu LTS, an operating system that's well known for being fast and secure. Ubuntu LTS is designed to be enterprise ready, well tested, and provides a Mandatory Access Control (MAC) system. We chose Ubuntu LTS specifically because it receives long-term security patches and upgrades, so we can be confident that it remains secure over time.

The Sauce network uses the Secure Shell (SSH) network protocol, the industry standard for secure data communication over insecure channels such as the Internet, with access by individual private keys assigned to a limited number of Sauce developers. SSH provides strong security by authenticating both the client and server ends of communication using RSA key pairs, and encrypting all traffic.

We also use good web development practices in our code to secure our website. We employ industry best practices to minimize cross-site scripting, which can present a serious vulnerability to website security. Some of these include using safely escaping templates, setting domain policy to avoid CORS, architecting code to avoid SQL injection by using prepared statements and parameterized queries, performing data validation, and using known and vetted JavaScript libraries.

SOFTWARE SECURITY

We have an established vulnerability management process to identify security vulnerabilities and assign risk ratings. Nessus is used for continuous vulnerability scans. In addition, we have third-party penetration tests performed on a quarterly basis, including black box and white box testing.

CREDENTIALS

To ensure that only authorized users and processes can access your Sauce Labs account, clients of Sauce Labs services are authenticated via user names and passwords or unique account-specific API keys. Integration with enterprise identity management systems is also available via SAML.

SOFTWARE ACCESS

We have a defined policy of who has access to our code and who can submit / update / make changes to our production servers. We have a centralized process for creating, maintaining, changing, and resetting keys and passwords. We keep records of all changes, and keep these available for auditing purposes. All employees are required to sign a NDA to ensure the confidentiality of our source code and customer data.

MANDATORY BACKGROUND CHECKS

At Sauce Labs, background checks are conducted on all candidates upon acceptance and contingent of our offer of employment. These include positions involving security and financial responsibilities. Sauce Labs uses a third-party accredited agency to conduct the background checks and to verify the accuracy of the information provided by the applicant during the selection process. Information collected by the agency includes criminal history search, Aux national criminal index, global terrorist search, and social security number trace.

CONCLUSION

In closing, Sauce Labs remains the choice for large enterprises looking to run automated and manual functional tests freeing their teams from the hassle and expense of maintaining an internal test grid or lab. You can rest assured knowing we take our commitment to provide a secure, reliable and scalable solution very seriously and have the appropriate measures in place. For questions or additional information, please contact us at saucelabs.com/contact.

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 deliver a flawless digital experience. Sauce Labs is a privately held company funded by Toba Capital, Salesforce Ventures, Centerview Capital Technology, IVP and Adams Street Partners. For more information, please visit saucelabs.com.

SAUCELABS

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

SAUCE LABS EUROPE GMBH
NEUENDORFSTR. 18B
16761 HENNIGSDORF GERMANY

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