Security in the Sauce Labs Cloud

Practices and protocols used in Sauce's infrastructure and Sauce Connect™

Overview

It's impossible to deny that in this day and age internet security should be of high concern to businesses of all sizes, particularly those which rely heavily on the web to operate.

According to the Ponemon Institute's 2012 study on cyber crime on US companies, cyber attacks rose 42% between 2011 and 2012, with an average annualized cost of cyber crime for companies in the study of $8.9 million per year. The study found that the most costly cyber crimes are caused by denial of service, malicious insiders, and web-based attacks, accounting for 58% of all cyber crime costs per organization annually.

All this means that companies should take as many measures as possible to guard against cyber attacks. At Sauce Labs, we take security very seriously. We have built many industry standard security measures into our products and infrastructure to make them as secure as possible. You can test with confidence, knowing your data and code are safe in our cloud.

> "Cyber attacks rose 42% between 2011 and 2012, with an average annualized cost of cyber crime for companies in the study of $8.9 million per year."
>
> **Ponemon Institute**
> 2012 study on cyber crime on US companies

What is Sauce Connect?

Sauce Connect is a secure tunneling app which allows you to execute tests securely when testing behind firewalls via a secure connection between Sauce Labs' client cloud and your environment.

When Should I Use Sauce Connect?

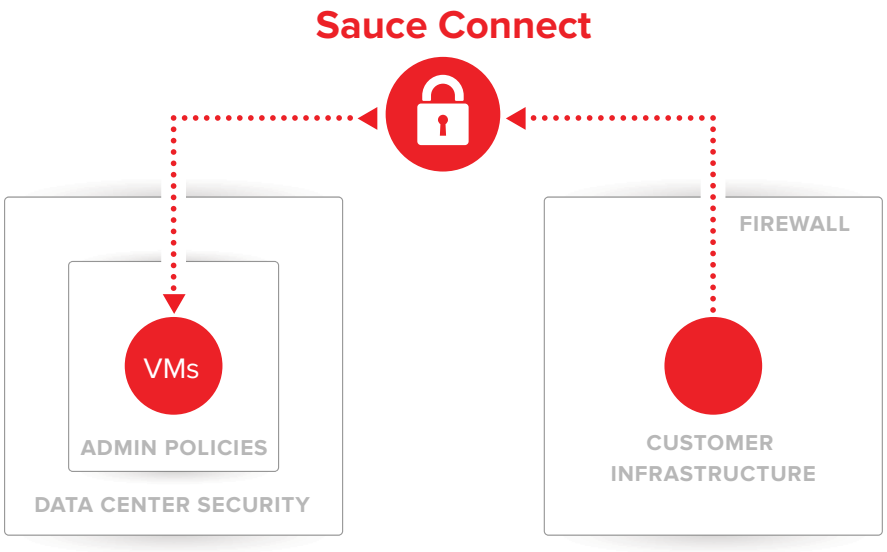
You should use Sauce Connect whenever you're testing an app behind a firewall. Sauce Connect is not required to execute scripts on Sauce.

You can also use Sauce Connect:

- as an alternative to whitelisting
- as a means of filtering traffic in your records (e.g. for Google Analytics)
- as a means of monitoring network traffic
- as a way to stabilize network connections (detecting/re-sending dropped packets)

Sauce Connect Diagram

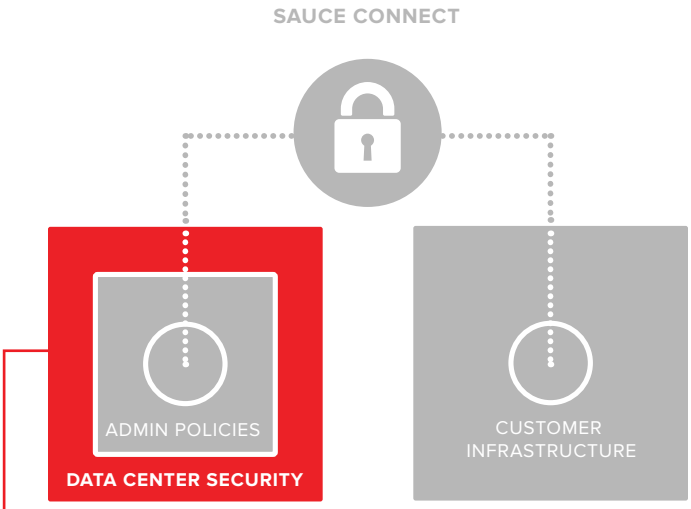
This graphic shows the different structures, both physical and virtual, that users' data flows through when connecting securely to the Sauce cloud from inside a firewall. At each step, we've taken actions to ensure that your data is secure against attack. Read on to learn how we secure your data, from our data center to the architecture of Sauce Connect™.



> The great thing about Sauce Connect is that it adheres to industry best practices.

Dominic Maraglia
Engineering Manager

puppet labs



Sauce Labs' Data Center Security

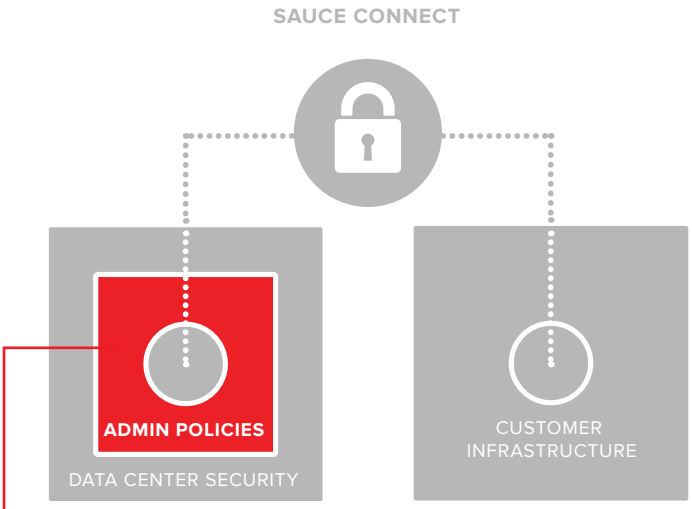
Sauce Labs' security starts with our data center itself and its machines. Our data center, located in Silicon Valley, employs many physical security measures to protect the center from intrusion, including restricted access to the premises, surveillance, and a secure cage for our machines with access restricted to select personnel.

We're also expanding our data center to a new facility that maintains advanced security and reliability measures. The center has undergone independent audits to assess its design and operational effectiveness. We chose this data center specifically because the facility employs measures that ensure it is flexible, reliable, and secure. The enterprise-grade facility allows us to make fiber connections to companies in the network, which is more secure than a standard internet connection.

The data center gives us enhanced flexibility and reliability in several ways. First, the center is powered by Silicon Valley Power, which, according to an ongoing nationwide survey by PA Consulting Group, ranks in the top quartile for several measures of reliability. Backup power can be supplied, with three backup Caterpillar generators on site, along with uninterruptable power supply, giving the facility N+1 redundancy. Climate control keeps the data center's environment stable, with two 1100 ton cooling towers and 18 million total BTUs for the facility. Dry-pipe and pre-action sprinkler systems provide fire protection. Physical security is also of high priority for the facility, with 62 cameras throughout the data center, on-site guards, proximity card readers, and biometric and keypad access control.

Our data center is very reliable

- Restricted access to the Silicon Valley premises
- 24-hour surveillance
- Powered by the highly-ranked Silicon Valley Power
- Backup power generators
- Climate control to keep the data center's environment stable



Administration Policies

The next area where we've designed security measures is our network system itself. The Sauce system uses Ubuntu LTS, an operating system that's well-known for being fast and secure.

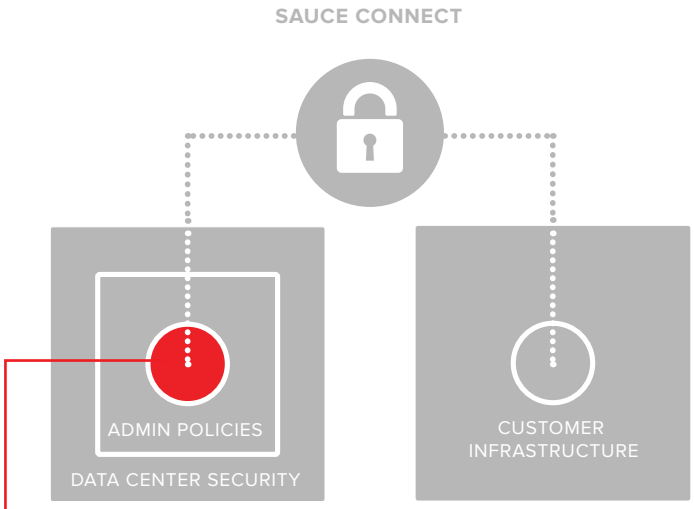
Ubuntu LTS is designed to be enterprise focused, well-tested, and provides a Mandatory Access Control (MAC) system. We chose Ubuntu LTS specifically because it receives regular security patches & upgrades, so we can be confident that it remains secure over time.

The Sauce network also 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. In spring of 2012 we conducted a 3rd party security assessment of our site and application, and made recommended adjustments based on the findings. A few of the adjustments implemented included further securing password storage, ensuring debugging features are disabled in production, implementing secure cookies, and disabling auto-complete.

We employ industry best practices

- Use safely escaping templates
- Set domain policy to avoid CORS
- Architect code to avoid SQL injection by using prepared statements and parameterized queries
- Perform data validation
- Use known and vetted JavaScript libraries



Virtual Machine Security

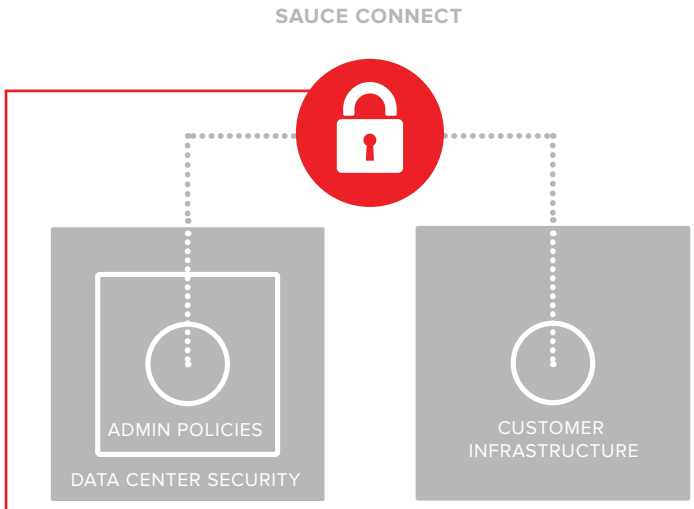
Sauce Labs also maintains very high standards for our VM security. Every time you run a test through Sauce Labs, we spin up a fresh, never-used VM for your test, which is destroyed immediately after you complete your test.

VM's are never reused for multiple tests or users, and 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. We also feel very strongly that 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. By avoiding the unsolvable problem of guaranteeing a system secure across anonymous use, we instead guarantee a system that has never and will never be used by any customer besides you.

Our VMs are also configured not to allow any outside inbound connections. As for assets recorded from tests, such as screenshots, videos, and logs, we store them in an Amazon S3 private bucket, and delete them after 30 days. Users who are concerned about the existence of test assets can choose to disable recording of test assets, in which case they will not be recorded at all.

Our VMs are secure

- We spin up a fresh, never-used VM for your test
- VMs are destroyed after your test runs
- VMs are never reused for multiple tests or users
- All data is only recorded to RAM, never to disk
- Our VMs are configured not to allow any outside inbound connections.



Sauce Connect™

All of these security measures, though, would be for naught if our tunneling system to connect your firewalled servers to our cloud were not secure.

This is why we designed Sauce Connect™ specifically to provide users with a secure way to test behind their firewall, using enterprise-grade security to proxy browser traffic between your servers and Sauce VMs. Sauce Connect can be configured for use with different proxies for both internal and external connections. We also support proxy autoconfiguration.

Security begins with the protocols and policies we employ for Sauce Connect™. All data is encrypted and transmitted between the tunnel, VM, and Sauce Connect™ via industry-standard SSL/TLS, using the top-rated AES-256 cipher. Sauce Connect™ also uses a caching web proxy 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 users' networks. Sauce Connect™ creates a dynamically controlled firewall that only allows VMs currently running a user's test access to the server-side of Sauce Connect™, which prevents any outside connection and any other VMs in the Sauce cloud from connecting to a local server.

We make it safe for you to test behind the firewall

- Employ enterprise-grade security to proxy browser traffic between local servers and Sauce VMs
- Configure Sauce Connect™ to use an internal or external customer web proxy. It also supports autoconfiguration.
- Destroy anything remaining in the cache at the end of a test run when Sauce Connect™ stops
- Sauce Connect™ prevents any outside connection and any other VMs in the Sauce cloud from connecting to a local server
- Encrypt all data and transmit it via industry-standard SSL/TLS, using the AES-256 cipher

Testing Securely on Sauce: Best Practices

We've built many security measures into our data center, VMs, and Sauce Connect™, but we've also developed best practices for how to properly use Sauce Connect™ for the most secure connection possible.

We recommend allocating a machine just for running Sauce Connect™, and firewalling that machine according to your company's standard. This way, you are in full control of the security of that machine, and can meet your own policies and standards for securing the machine. We also recommend firewalling the application under test from your internal infrastructure, so it retains as much separation from your internal systems as possible.

Furthermore, we encourage you to follow testing best practices and use no production data in your testing environment, or anonymize all sensitive information such as PII. No real data should be used in your testing environments.

One last best practice for using Sauce Connect™ is to make sure you are writing your tests as if you are testing locally, as opposed to connecting to the Sauce cloud itself.

> "Sauce Connect helps us catch bugs before they get to the staging environment."

Sage Rimal
Senior QA Automation Engineer

CAMPUS EXPLORER

About Sauce Labs

Sauce Labs is the most secure, reliable solution for automating functional testing for web, mobile, and hybrid apps. We believe continuous integration and delivery should be simple and painless for software teams. Based on the acclaimed Selenium and Appium open source frameworks, our cloud testing platform enables modern organizations to bring quality applications to market faster and more cost-effectively.