Splashtop Cloud Products

Security Overview

Updated May 5, 2020

Originally published September 17, 2019

Contents

Introduction

This white paper provides a technical overview of the Splashtop cloud business products from a security perspective. It spans the architecture, protocols, infrastructure, and components of Splashtop products. The document can help technical and security professionals understand the security design of Splashtop. It can also help them use the products in a way that complies with and complements their organizations' security requirements.

Products

This white paper is relevant to the suite of Splashtop **cloud-based** remote access products for businesses (described below). These products enable individuals and businesses to remotely view and control computers and mobile devices for productivity and support purposes.

These products are designed with security in mind, to ensure only authorized users have access, to safeguard data end-to-end, and to enable users to fully audit activity.

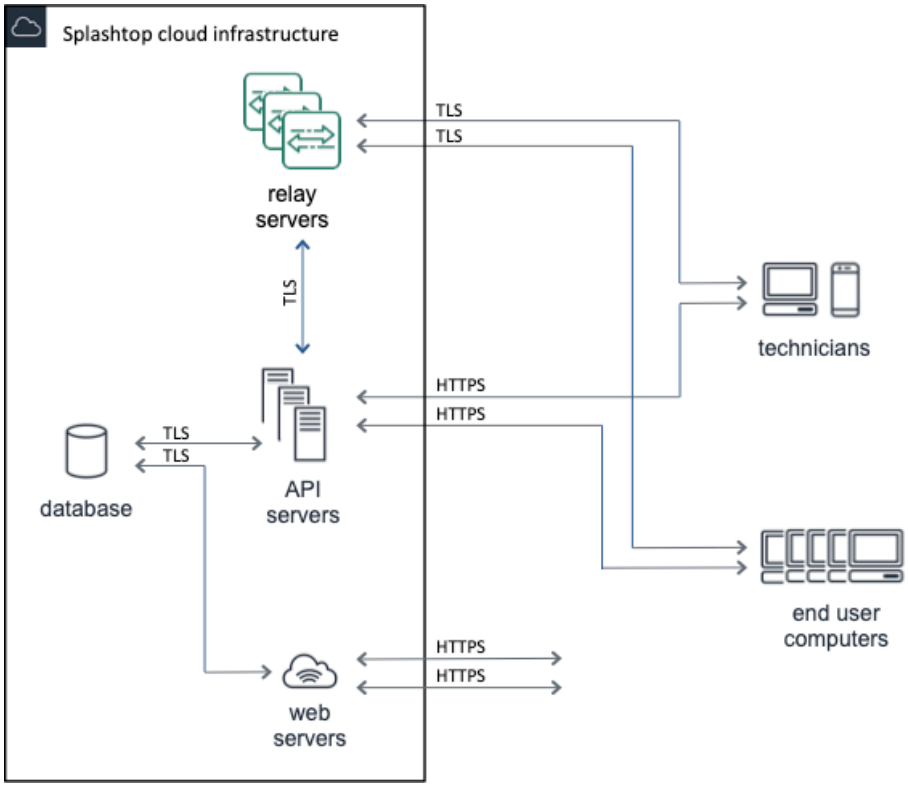
There are three products in the Splashtop cloud-based remote access suite:

- *Splashtop Business Access*. For working professionals or teams to remotely access their computers at any time and from anywhere. Agent software is pre-installed onto the computers. Access permission is strictly controlled.
- *Splashtop Remote Support*. For MSPs and IT pros to remotely access the computers they manage. Agent software is pre-installed onto the computers. Access permission is strictly controlled.
- *Splashtop On-Demand Support*. For MSPs and helpdesks to support their users on an ad hoc basis. No software needs to be pre-installed. End users need to initiate the process to allow the technicians to remote in.

Architectural Overview

The Splashtop cloud-based product architecture consists of the following components:

- Agent software that is installed on the end users' devices ("*Splashtop streamer*")
- Technician app that is installed on the technicians' devices ("*Splashtop Business app*")
- API servers
- Relay servers
- Web servers
- Database



Communications between all above components are encrypted.

API servers and web servers use standard HTTPS over port 443. TLS defaults to version 1.2.*

Relay servers use TCP encrypted with AES-256, set up via TLS. Communication with relay servers is over port 443 as well. TLS defaults to version 1.2.*

Protocols and Components
(from the security perspective)

The Splashtop API servers are located in California and Oregon.
Relay servers are in multiple locations around the globe, to be in close proximity and to enhance performance for users throughout North America, South America, Europe, and Asia Pacific.
Web servers are in California.
Database is in California as well, with cross-region backup and disaster recovery.

API Servers
The endpoints (*Splashtop streamer* and *Splashtop Business app*) communicate with the API servers using standard HTTPS. HTTPS protects all information in transit.
Each API server has a CA-signed SSL certificate (2048-bit RSA SHA-2), to ensure its identity and to prevent man-in-the-middle attacks.
API server supports TLS 1.2.*

Relay Servers
The endpoints (*Splashtop streamer* and *Splashtop Business app*) establish individual TLS connections over TCP with the relay servers. The relay server then brokers an end-to-end tunnel between the two corresponding endpoints. The two endpoints negotiate TLS and AES-256 encryption key with each other directly. The resulting encrypted tunnel carries the remote session data. The data is protected end-to-end and can only be decrypted at the users' endpoints.
Each relay server has a CA-signed SSL certificate (2048-bit RSA SHA-2).
Relay server supports TLS 1.2.*

Web Servers
Web servers provide the web-based management interface to the customers. It is where customers manage computers, users, technicians, and audit logs.

The web console is accessible only via HTTPS, which secures all information in transit.
Each web server has a CA-signed SSL certificate (2048-bit RSA SHA-256).

Database
Database is an encrypted (AES-256) database cluster. It is backed up daily to multiple regions. The backups are encrypted as well.
Database stores hashes of user passwords, not the passwords themselves. Hashes are generated with SHA-512 using a unique 20-character salt for each password.

Endpoint Software
Endpoint software consists of *Splashtop streamer* and *Splashtop Business* app. They are downloaded from Splashtop websites via HTTPS, which guarantees legitimacy of the source.
Binaries are code-signed with the appropriate certificates to ensure their integrity.
Windows executables are signed with organization validated (OV) X.509 certificates.
Windows drivers are signed with extended validation (EV) X.509 certificate per Windows Kernel Mode Code Signing requirements.
macOS executables are signed with X.509 certificate per Apple developer requirements.

Security Features

Splashtop is designed with strong **authentication** requirements, to ensure users are who they say they are.

There is also a robust set of **authorization** controls, to finely tune the rights and access permissions of authenticated users.

Finally, comprehensive logging is in place, to enable monitoring and **auditing**.

Authentication
Various mechanisms are in place to ensure users logging in to use Splashtop are who they say they are.

- *Splashtop credential*. At the foundation of authentication is the Splashtop credential: the Splashtop ID and password. Splashtop ID is an email address that is verified. Password must meet certain complexity requirements.
  Single sign-on is available for certain products, to gain further control over the authentication step.
- *Device authentication*. Whenever user logs into Splashtop, whether via the web console or the *Splashtop Business app*, a mandatory device authentication check is performed. If the device is new, then user must go through a device authentication process. The process verifies the user truly owns his or her Splashtop ID email address.
  Administrators and users can see the list of activated devices and can deactivate devices via the web console at any time.
  Additionally, administrators have the option of having all users' device authentication emails be sent only to the administrators, to maintain full control of what devices users may use to remote from.
- *Two-step verification*. A user can set up (optional) two-step verification. Two-step verification is TOTP-based and requires registering a mobile device and an authenticator app. The choices of authenticator apps are *Google*, *Duo Mobile*, and *Microsoft*. Once two-step verification is enabled, logging in with the Splashtop account on the web console or in the *Splashtop Business app* requires entering a time-based, one-time password from the authenticator app on the registered mobile device.
  The team owner has the option of requiring every user on the team to use two-step verification.

Authorization

Team owner and administrators can specify which users or groups of users have access to precisely which computers or groups of computers.
Team owner and administrators can invite, enable, disable, and delete users via the web console.
Access right is verified in multiple places, including right before starting a connection.
Additional authorization can be required when a connection is attempted. For example, user may be required to enter the

Windows or Mac account credentials of the target computer or a custom security code specific to the target computer.
The target computer can also be configured to require explicit permission from the user currently in front of the computer (in the form of a pop-up prompt with a timer countdown), at the final stage of establishing connection.
In the case of *Splashtop On-Demand Support*, remote access session is initiated by the end user at the target computer. The user must explicitly click on a URL link, download an app, run the app, and communicate the resulting 9-digit session code shown by the app to the technician.
Team owner has the option of disabling certain features, if necessary to comply with the organization's security requirements. These features include file transfer, copy-and-paste, remote print, session recording, etc.
When a user remotely accesses a target computer (to perform remote control, file transfer, or remote command), a mandatory notification is shown on the target computer. This helps to protect against unauthorized surveillance and to ensure user privacy.
The target computer can be configured to automatically terminate a remote session if it has been idle for a certain amount of time. The target computer can also be configured to revert to the OS's lock screen automatically when a session ends.
The target computer can be configured to automatically blank its screen when a remote desktop session is in progress. This helps to protect the privacy of the remote user's actions.

Auditing

All remote desktop sessions are logged, with the following information:

- Start time, end time, and duration
- Name of the target computer being accessed and its IP address
- Splashtop ID of the user who performed the remote access, the name of the device used for remote access, and the device's IP address
- Remote desktop sessions that are currently in progress are indicated as such on the web console.

All file transfer activities are logged, with the following information:

- Timestamp

- Name of the target computer being accessed and its IP address
- Splashtop ID of the user who performed the remote access, the name of the device used for remote access, and the device's IP address
- File name and size
- Direction of transfer

All of the above logs can be viewed in the Splashtop web console, for the past 60 days.
Logs for the past 12 months can be archived by exporting them in CSV format from the web console.
If the Splashtop product is used in conjunction with a supported ticketing system, the logs are directly entered into and archived in the corresponding tickets in the ticketing system.
Remote desktop sessions can be recorded. Recording can be started and stopped at any time via the in-session toolbar. The resulting video files are stored locally on the devices from where the sessions are initiated. Team owner can disable recording globally via the web console.

Infrastructure

Splashtop infrastructure leverages infrastructure providers such as Amazon Web Services (AWS), Google Cloud Platform (GCP), and Oracle Cloud Infrastructure (OCI).

These providers ensure the uptime and physical security of their infrastructure. Splashtop has built additional layers of redundancy and failover logic across the multiple providers to further improve reliability. As enumerated earlier, Splashtop has multiple points-of-presence around the globe, for close proximity to users and for cross-region redundancy.

Splashtop also uses various services from these infrastructural providers, besides the standard compute instances. The additional services include managed databases, cloud storage, edge caching, load balancers, DNS service, and multiple monitoring tools.

Compliance

Refer to https://www.splashtop.com/compliance for the latest information on Splashtop with regard to industry standards.

General Data Protection Regulation (GDPR)
Splashtop complies with the GDPR requirements for European Union users, as a controller and a processor. Users have the right to access, correct, and remove their personal data.

HIPAA
HIPAA compliance is not applicable to Splashtop, since Splashtop does not process, store, or have access to any of the users' computer data. Splashtop facilitates the transmission of but does not store the screen capture and file transfer streams, which are encrypted end-to-end.
The Splashtop products, when used properly with the earlier-described security features, help users with meeting their organizations' HIPAA requirements.

Service Organization Control 2 (SOC 2)
SOC 2 attestation demonstrates that controls are in place and used properly by an organization to ensure security and privacy of customers' data. Splashtop has achieved SOC 2 Type 1.

---

* In certain cases, negotiation may result in TLS 1.1 or TLS 1.0 to be compatible with the customers' environments. Customers wishing to restrict to only TLS 1.2 can do so by locking down their environments. All Splashtop components will then negotiate to TLS 1.2.