Splashtop Cloud Products

Security Overview

Updated December 4, 2024

Contents

Introduction 3
Products 3
Architectural Overview 4
Protocols and Components 5
Security Features 7
Infrastructure 11
Compliance 11

Introduction

This white paper provides a technical overview of the Splashtop cloud business products from a security perspective. It encompasses 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.

Note for European Union (EU) Users
By default, EU users are directed to create their user accounts in Splashtop's EU-based cloud infrastructure, which is located in Germany. This is an independent infrastructure, separate from the US-based infrastructure that serves Splashtop users in rest of the world. Such separation enables users to comply with the data sovereignty requirements they may have.

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 control and manage 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 four products in the Splashtop cloud-based remote access suite:

- *Splashtop Enterprise*. For organizations needing enterprise-grade remote access and support, with single sign-on, fine-grained controls, extensive logging capabilities including SIEM export and cloud recording, service desk workflow, ITSM integration, scheduled access, open APIs, RDP/VNC/SSH access, and more.

- *Splashtop Business Access*. For working professionals or small teams to remotely access their work computers at any time and from anywhere. Agent software is pre-installed onto the computers. Access permission is strictly controlled.
- *Splashtop SOS*. For MSPs, IT pros, and help desks to remotely access the computers they manage as well as to support their users on an ad hoc basis with no software pre-installed.
- *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.

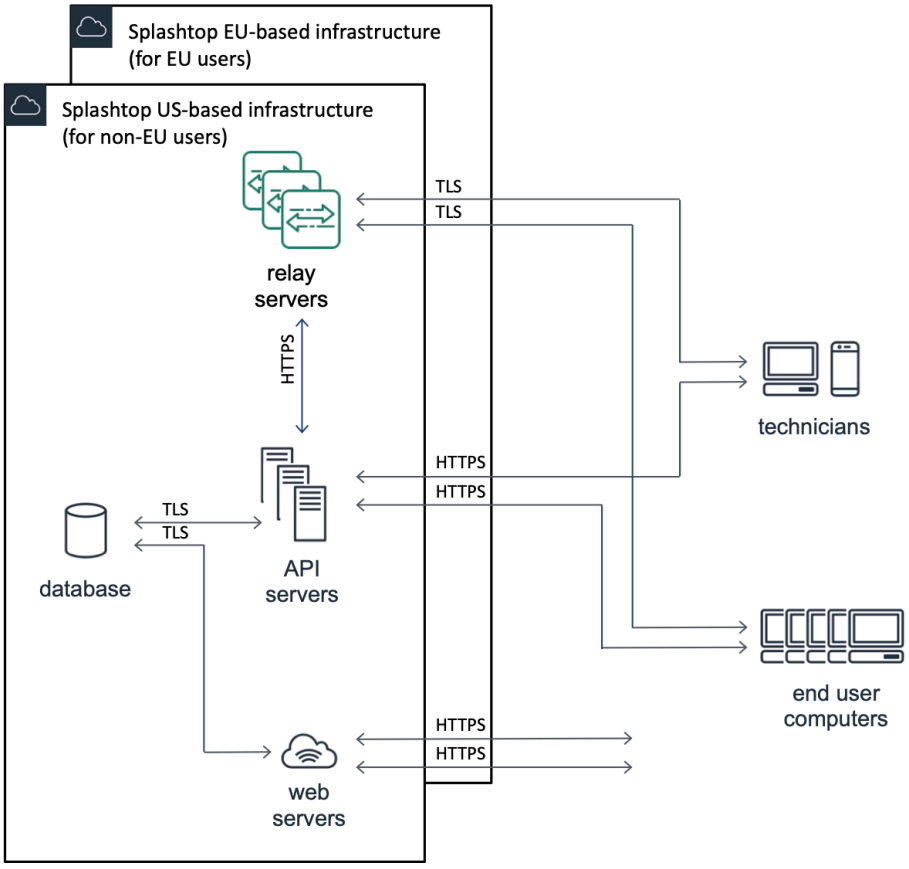
Architectural Overview

Architecture of the Splashtop cloud-based products consists of the following main 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

As aforementioned, Splashtop maintains two sets of cloud infrastructure, one for EU users and one for non-EU users. Each set contains its own API servers, relay servers, web servers, and database. User data is completely separate between the two sets of infrastructure. By default, EU users are directed to create their accounts in the EU-based cloud infrastructure and thereby retain their user data within EU.

The diagram below illustrates the main components of the Splashtop cloud infrastructure, their communication paths, and the protocols used.



Communication between all of the above components is encrypted.

Web servers use standard HTTPS over port 443 with TLS 1.2.

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

Relay servers use TCP over port 443 encrypted with AES-256, set up via TLS 1.2.

Protocols and Components

(from the security perspective)

The Splashtop API servers are load-balanced across California and Oregon for the US infrastructure, and in Germany for the EU infrastructure.

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, Middle East, Africa, Asia, and Australia.
Web servers are in Oregon for the US infrastructure, and in Germany for the EU infrastructure.
Database is in Oregon as well for the US infrastructure, and in Germany for the EU infrastructure, 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) individually establish 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 uses 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 with TLS 1.2, 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 Business* app, *Splashtop streamer*, and *Splashtop SOS* app (for ad hoc support). 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

The design features of Splashtop that ensure security of its users can be broadly categorized into **authentication**, **authorization**, and **auditing**.

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. Authorization can make use of the organization's SSO (single sign-on), SCIM (System for Cross-domain Identity Management), and JIT (Just-in-Time) capabilities for centralized control and better automation.

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 (SSO) is available with *Splashtop Enterprise*, to centralize authentication via the organization's directory. Splashtop supports SSO via SAML 2.0 and OpenID Connect. Pre-built connectors are available for most common identity providers.
- *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 or browser 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 authenticated devices and can invalidate devices via the web console at any time. The team owner can also limit the amount of time that devices stay authenticated for.
  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 two-step verification. Two-step verification is TOTP-based and requires registering a mobile device and an authenticator app. Authenticator apps supporting TOTP include *Google Authenticator*, *Duo Mobile*, and *Microsoft Authenticator*.
  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.
  The team owner also has the ability to manage users' trusted devices and how long those devices stay trusted for.

- *IP address allow list*. The team owner can restrict the IP addresses that the *Splashtop Business* app and the web console are accessed from. For example, a call center can restrict the use of Splashtop to only when the technicians are on-premises.

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.

Organizations with SSO and identity providers that support SCIM or JIT can further streamline the workflow by provisioning, grouping, and setting permissions via their directories then automatically propagating the configuration changes to Splashtop.

Access right is verified in multiple places, including at the point of 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 ad hoc support via *Splashtop SOS* or *Splashtop Enterprise*, remote access process is initiated by the end user at the target computer. The end user must explicitly click on a URL link, download an app, run the app, etc. in order to allow remote access by the technician.

Team owner has the option of completely disabling certain features, if necessary to comply with the organization's security requirements. These features include file transfer, copy-and-paste, remote print, remote command, session recording, reboot, and more. With *Splashtop Enterprise*, various features can be controlled at fine granularity, down to the user or user group level.

When a user remotely accesses a target computer (to perform remote control, background file transfer, or background 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

Remote command sessions, chat sessions, and other session types are also logged, including the full session transcript where applicable.
All of the above logs can be viewed in the Splashtop web console, for the past 90 days.
Team management history (managing users, permissions changes, adding and removing computers, logins on new devices, failed login attempts, etc.) is retained for three years. Logs for the past 12 months can be archived by exporting them in CSV format from the web console. With *Splashtop Enterprise*, logs can also be retrieved continuously and automatically via SIEM integration or open API integration.

If the Splashtop product is used in conjunction with a supported ticketing system, the logs are directly injected into the corresponding tickets in the ticketing system.
Remote desktop sessions can be recorded, with the recordings stored locally on the technician's workstation. Recording can be started and stopped at any time via the in-session toolbar. The team owner can also enable automatic, mandatory recording of all sessions, as well as configure the storage file path and maximum size of the recordings. *Splashtop Enterprise* provides the additional option of recording to the cloud, which may be important for usability and compliance reasons. Cloud recordings are stored for 90 days and can be played back or downloaded via the web console.

Infrastructure

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

These providers ensure high 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 numerous points-of-presence around the globe, for close proximity to users to ensure good performance and for cross-region redundancy.

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

Compliance

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

ISO/IEC 27001
ISO/IEC 27001 is an internationally recognized benchmark for establishing and upholding robust information security management system. With its comprehensive set of stringent requirements, the standard supports a holistic approach to information security by thoroughly assessing individuals, policies, and technologies through rigorous testing and auditing. Splashtop undergoes annual ISO/IEC 27001 audits.

Service Organization Control 2 (SOC 2)
SOC 2 is a comprehensive reporting framework put forth by the American Institute of Certified Public Accountants (AICPA). SOC 2 attestation demonstrates that controls are in place and used properly by Splashtop to ensure security and privacy of its customers' data.
Splashtop undergoes annual SOC 2 audits and maintains SOC 2 Type 2 as well as SOC 3 compliance.

Health Insurance Portability and Accountability Act (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 video, audio, and data and does not store the streams. Transmission is encrypted end-to-end.
The Splashtop products, when used properly with the earlier-described security controls, help users with meeting their organizations' HIPAA requirements.

Family Educational Rights and Privacy Act (FERPA)
Similar to above, FERPA compliance is not applicable to Splashtop, since Splashtop does not process, store, or have access to students' educational records.
The Splashtop products, when used properly with the earlier-described security controls, help users with meeting their educational institutions' FERPA requirements.

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.

California Consumer Privacy Act (CCPA)
Splashtop complies with the CCPA requirements for California residents. Users have the right to access, correct, and remove their personal data.

---

* API servers currently support negotiating down to TLS 1.1 or TLS 1.0 to remain compatible with all customer environments. Customers wishing to restrict to only TLS 1.2 can do so by locking down their environments. Splashtop API servers will phase out the older TLS in 2025.