Splashtop On-Prem Products

Security Overview

Originally published May 11, 2022

Contents

Introduction

This white paper provides a technical overview of the **Splashtop On-Prem** product 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 organization's security requirements.

Products

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

The product is 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 types of typical use case scenarios in the Splashtop **On-Prem**

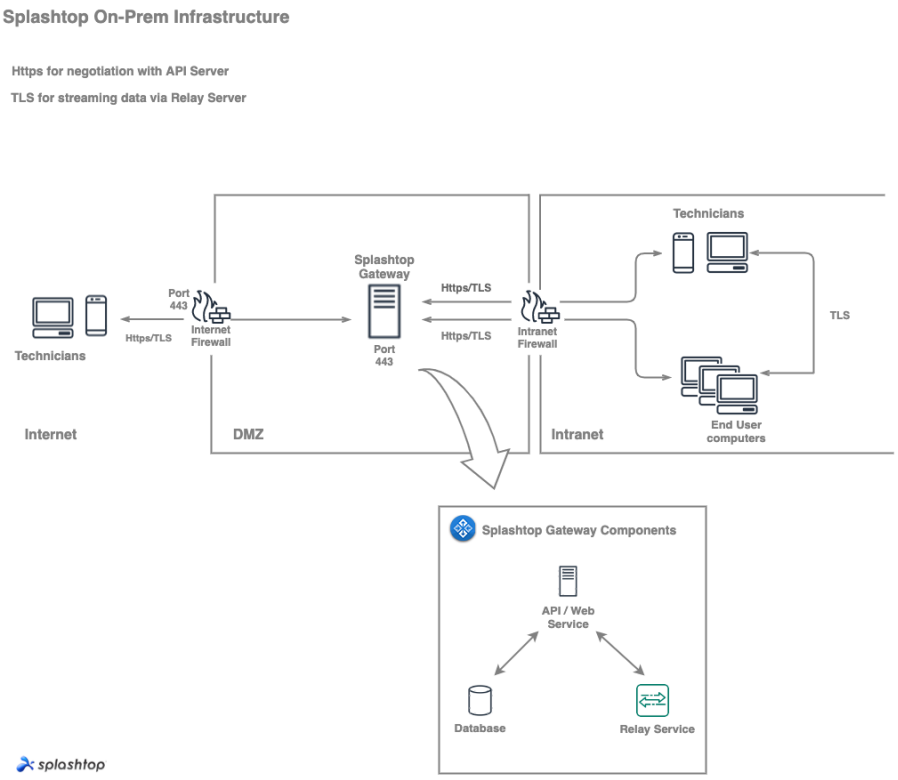
- *Remote Access*. For working professionals or teams to remotely access their computers at any time and from anywhere. Agent software is pre-installed onto the computers. Access permission is strictly controlled.
- *Remote Support of unattended computers/devices*. For MSPs and IT pros to remotely access the computers they manage. Agent software is pre-installed onto the computers. Access permission is strictly controlled.
- *Remote support of attended computers/devices.* For MSPs and helpdesks to support their users on a predominantly 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 On-Prem product architecture 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 On-Prem app*")
- On-premises Gateway server with below sub-components
    - API component
    - Web component
    - Relay component
    - Database

The diagram below illustrates the main components of the Splashtop on-premises infrastructure, their communication paths, and protocols.



Inbound and outbound communication between all above components are encrypted.

Splashtop Gateway server uses standard HTTPS (HSTS) over port 443 for inbound/outbound traffic. TLS defaults to version 1.2.

Relay service uses TCP encrypted with AES-256, set up via TLS. Communication with relay service is over port 443 for inbound/outbound traffic as well. TLS defaults to version 1.2.

Splashtop Gateway local connection for Database is encrypted by scram-sha-256.

Protocols and Components

(From the security perspective)

API Service

The endpoints (*Splashtop Streamer* and *Splashtop On-Prem app*) communicate with the API component using standard HTTPS. HTTPS protects all information in transit.

Splashtop On-Prem Gateway allows system admin to configure CA-signed SSL certificate (2048-bit RSA SHA-2), to ensure its identify and to prevent man-in-the-middle attacks.

All Splashtop components would negotiate to TLS 1.2 by default.

Relay Service

The endpoints (*Splashtop Streamer* and *Splashtop On-Prem app*) individually establish TLS connections over TCP with the relay service through Splashtop Gateway.

The relay service 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.

The Relay service uses the same CA-signed SSL certificate configured on API component in Splashtop On-Prem.

Web Service

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

HTTP Strict Transport Security (HSTS) is deployed on this server

The web console is accessible only via HTTPS, which secures all information in transit.

Each web server uses the same CA-signed SSL certificate (2048-bit RSA SHA-256) used by API service.

Database
Database is an encrypted (scram-sha-256) stand-alone database.

Database stores hashes of user passwords, not the passwords themselves. Hashes are generated with SHA-256 and salt.

Endpoint Software
Endpoint software consists of *Splashtop Streamer* and *Splashtop On-Prem* app. They are downloaded from Splashtop Gateway web console 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. Authorization can make use of the organization's Active Directory authentication.

Finally, comprehensive logging including syslog integration 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 On-Prem credential*. At the foundation of authentication is the Splashtop On-Prem credential: system admin creates the user credential through the Splashtop Gateway management portal, Only the authorized user can access the service. Password must meet the complexity requirements.
- *Active Directory integration* is available with *Splashtop Gateway*, to centralize authentication via the organization's established directory service and authentication.
- *Device and browser authentication*. Whenever user logs into Splashtop, whether via *Splashtop Gatewa*y web console or the *Splashtop On-Prem app*, a mandatory device and browser authentication check are performed. If the device or browser is new, then the user must go through an 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 browsers and can deactivate them via the web console at any time.

  Additionally, administrators have the option of having all users' device and browser authentication emails be sent only to the administrators, to maintain full control of what devices and browsers users may use to log in.
- *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. The choices of authenticator apps are *Google*, *Duo Mobile*, *Okta Verify, Microsoft, and other TOTP authenticator apps*. Once two-step verification is enabled, logging in with the Splashtop account on the web console or in the *Splashtop On-Prem app* requires entering a time-based, one-time password from the authenticator app on the registered mobile device.

Team owner has the option of requiring every user on the team to use two-step verification.

- *Session lifetime control*. *Splashtop On-Prem* allows system administrator to configure the browser session timeout control to maintain high security standard to force logout idled users from Splashtop Gateway web console.
- *IP filter restriction*. Team owner has the option to add desired IP addresses to the system to only allow access to *Splashtop Gateway* web console and *On-Prem app* from these IP addresses.

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 create, enable, disable, and delete users via the web console.

Organizations with Active Directory can further streamline the workflow by provisioning, grouping, and setting permissions via their directories.

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 *Splashtop attended support*, remote access session 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, 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, and more.

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 On-Prem account name 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

Team management history (managing users, permissions changes, adding and removing computers, logins on new devices, team setting updates, failed login attempts etc.) are following the same log structure.

Logs for the most recent 12 months can be viewed and archived by exporting them in CSV format from Splashtop On-Prem web console.

They can also be continuously sent to a syslog server in real-time.

If the Splashtop On-Prem product is used in conjunction with a supported ticketing system, the logs are directly archived in the corresponding tickets in the ticketing system.
Remote desktop sessions can be recorded. Via the web console, team owner can enable automatic recording of all sessions as well as configure where the recordings are to be stored. Recording can also be started and stopped at any time via the in-session toolbar.

Infrastructure

Splashtop On-Prem supports various deployment options.

All-in-one Windows installation
Splashtop On-Prem's all-in-one is packaged as Windows installer, which is suitable for small entities with small service loading. System admin can harden the Windows environment by installing extra security tools to enhance system security.

Clustering Windows or Linux deployment
Splashtop On-Prem can be deployed on Windows or Linux for clustering purposes, which is suitable for big entities with large service loading.

Compliance

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

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 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 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 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 organizations' 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.