Splashtop On-Prem 产品

安全概述

发布时间：2024 年 9 月 9 日

目录

说明

本白皮书将从安全角度提供有关 **Splashtop On-Prem** 产品的技术概述，包括 Splashtop 产品的架构、协议、基础设施和组件。本白皮书可以帮助技术员和安全专业人员了解 Splashtop 的安全设计，帮助其以符合组织安全要求的方式使用 Splashtop 产品，以补充组织的安全要求。

产品

本白皮书是关于 Splashtop 面向企业的本地化部署远程访问产品（如下所述），使个人用户和企业能够远程查看和控制电脑和移动设备，达到提高生产力和支持水平的目的。

Splashtop On-Prem 产品重视安全性，确保仅授权用户可以访问，保护端到端传输数据的安全，使用户能全面审计活动。

Splashtop **On-Prem** 有以下三种典型的使用场景：

- *远程访问：*适用于工作人员或团队随时随地远程访问其电脑。被控端软件会预先安装在电脑上，同时严格控制访问权限。
- *远程支持无人值守的电脑/设备：*适用于 MSP 和 IT 专业人员远程访问托管电脑。被控端软件会预先安装在电脑上，同时严格控制访问权限。
- *远程支持有人值守的电脑/设备：*主要适用于 MSP 和帮助台临时支持其用户。无需预先安装任何软件。最终用户需要发起请求，允许技术员远程连接。

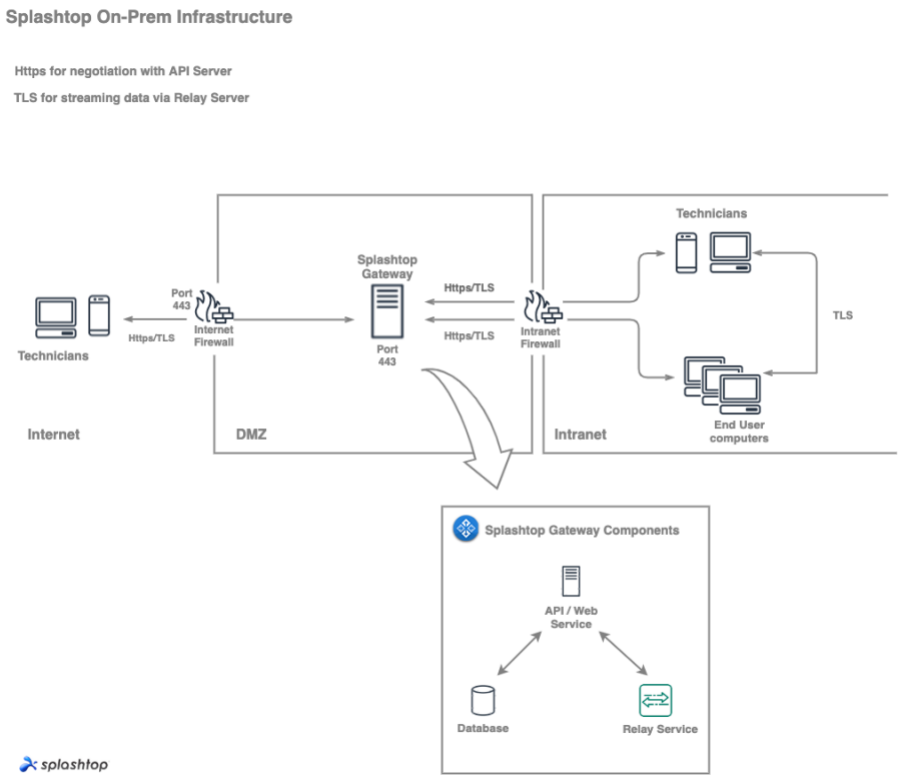
架构概述

Splashtop On-Prem 产品架构包括以下几个主要组件：

- 安装在需要被访问或者被管理的设备上的被控端软件（Splashtop Streamer）
- 安装在远程办公人员或者技术人员设备上的控制端软件（Splashtop On-Prem app）
- 具有以下子组件的本地 Gateway 服务器

- **API 组件**：为 Splashtop Streamer 和 Splashtop On-Prem 应用提供 API 服务。
- **Web 组件**：支持基于 Web 的管理控制台。
- **中继组件**：处理会话期间流数据的传输。
- **数据库**：存储和管理永久数据。

下图所示即为 Splashtop On-Prem 基础设施的主要组件及其通信路径和协议。



所有组件之间的入站和出站通信都经过加密。

Splashtop Gateway 服务器使用标准 HTTPS（HSTS）通过 443 端口处理入站/出站流量。TLS 默认版本为 1.2。

中继服务采用 TCP，使用 AES-256 加密算法，通过 TLS 协议建立。中继服务的通信通过 443 端口处理入站/出站流量。TLS 默认版本为 1.2。

Splashtop Gateway 数据库的本地连接使用 SCRAM-SHA-256 进行加密。

协议和组件

（从安全角度）

API 服务

端点（Splashtop Streamer 和 Splashtop On-Prem 应用）使用标准 HTTPS 与 API 组件通信。HTTPS 保护传输中的所有信息安全。

Splashtop On-Prem Gateway 允许系统管理员配置 CA 签名的 SSL 证书（2048 位 RSA SHA-2）以验证其身份并防止中间人攻击。

所有 Splashtop 组件默认使用 TLS 1.2 进行安全通信。

中继服务

端点（Splashtop Streamer 和 Splashtop On-Prem 应用）从 Splashtop Gateway 通过中继服务使用 TCP 分别建立 TLS 连接。

中继服务会在两个相应的端点之间建立端到端隧道。两个端点直接协商建立 TLS 连接，生成 AES-256 加密密钥。生成的加密隧道将安全传输远程会话数据。数据受到端到端保护，且只能在用户的端点解密。

中继服务使用与 Splashtop On-Prem 中配置的 API 组件相同的 CA 签名 SSL 证书。

Web 服务

Web 服务器为客户提供基于 Web 的管理界面，使其能够管理电脑、用户、技术员和审计日志。

Web 服务器上已部署 HTTP 严格传输安全协议（HSTS）。

网页控制台只能通过 HTTPS 访问，确保所有数据信息在传输过程中的安全性。

每个 Web 服务器都使用与 API 服务相同的 CA 签名 SSL 证书（2048 位 RSA SHA-256）。

数据库

Splashtop 数据库是一个加密（SCRAM-SHA-256）的独立数据库，用于存储用户密码的哈希值，而非明文密码本身。哈希值使用 SHA-256 算法和盐值生成。

端点软件

端点软件包括 Splashtop Streamer 和 Splashtop On-Prem 应用。可以通过 HTTPS 从 Splashtop Gateway 网页控制台下载，确保来源的合法性。

二进制文件通过适当的证书进行代码签名，以确保其完整性。

Windows 可执行文件使用组织验证（OV）的 X.509 证书进行签名。

Windows 驱动程序根据 Windows 内核模式代码签名要求使用扩展验证（EV）的 X.509 证书进行签名。

macOS 可执行文件根据 Apple 开发者要求使用 X.509 证书进行签名。

安全功能

首先，Splashtop 采用强大的**身份验证**要求，以确保用户身份的真实性。

其次，Splashtop 具备强大的**授权**控制功能，允许为通过身份验证的用户精细调整访问权限及其他权限。授权可以利用组织的活动目录身份验证。

最后，Splashtop 可提供包括 syslog 集成在内的全面日志记录，便于进行监控和**审计**。

身份验证

Splashtop 采取各种机制确保登录使用 Splashtop 的用户身份的真实性。

- *Splashtop On-Prem 凭据。*Splashtop On-Prem 凭据是身份验证的基础：系统管理员通过 Splashtop Gateway 管理门户创建用户凭据，只有授权用户才能访问服务。创建的密码必须符合复杂性要求。

- *Splashtop Gateway 可以与活动目录和单点登录集成，*通过组织已建立的目录服务和身份验证来集中完成身份验证。

- *强制实施复杂密码。*可以在 Splashtop Gateway 中进行配置，以确保用户凭据的复杂性，降低密码暴力攻击的风险。

- *强制密码过期。*可以在 Splashtop Gateway 中进行配置，以在所需的时间段强制执行密码轮换。

- *账户锁定策略。*账户锁定策略即在达到指定的失败登录尝试次数后锁定账户，可以选择开启或关闭此策略。

- *设备和浏览器身份验证。*每当用户登录 Splashtop 时，无论通过 Splashtop Gateway 网页控制台还是 Splashtop On-Prem 应用，都会强制执行设备和浏览器身份验证检查。如果是新设备或浏览器，则用户必须进行身份验证。此过程可以验证用户是否是 Splashtop ID 电子邮件地址的真正持有者。管理员和用户可以随时通过网页控制台查看已激活的设备和浏览器列表，并可以进行停用。此外，管理员可以选择将所有用户的设备和浏览器身份验证邮件仅发送给管理员，以保持对用户可能用于登录的设备和浏览器的完全控制。

- *两步验证。*用户可以设置两步验证。两步验证基于 TOTP，需要注册移动设备和身份验证器。可供选择的身份验证器包括 Google、Duo Mobile、Okta Verify、Microsoft 和其他 TOTP 身份验证器。启用两步验证后，在网页控制台或 Splashtop On-Prem 应用中使用 Splashtop 账户登录时，需要在已注册的移动设备上的身份验证器中输入基于时间的一次性密码。团队所有者可以选择要求团队中的所有用户使用两步验证。

- *会话有效期控制。*Splashtop On-Prem 允许系统管理员配置浏览器会话超时控制，以保持高安全标准，从 Splashtop Gateway 网页控制台强制注销长时间空闲用户。

- *IP 过滤限制。*团队所有者可以选择添加所需的 IP 地址到系统中，仅允许从已添加的 IP 地址访问 Splashtop Gateway 网页控制台和 On-Prem 应用。

- *MAC 地址限制。*团队所有者可以选择通过 MAC 地址将特定的技术员设备列入白名单，阻止任何具有未知 MAC 地址的设备登录和建立会话。

授权

团队所有者和管理员可以指定允许用户或用户组访问的特定计算机或计算机组，可以通过网页控制台创建、启用、禁用和删除用户。

使用活动目录或单点登录（SAML2）的组织可以通过其目录配置、分组和设置权限，以进一步简化工作流程。许多情况都需要验证访问权限，包括建立连接时。

尝试连接时需要额外授权。例如，用户可能需要输入目标计算机的 Windows 或 Mac 账户凭据或目标计算机特定的自定义安全码。

目标计算机还可以配置为在建立连接的最后阶段，要求获得当前电脑前用户的明确许可（以弹出倒计时提示信息的形式）。

在 *Splashtop 有人值守支持* 的情况下，远程访问会话由目标计算机上的最终用户发起。最终用户必须明确点击 URL 链接，下载并运行应用，并将该应用上显示的 9 位会话码告知技术员。

如果需要遵守组织的安全需求，团队所有者可以选择禁用某些功能，包括文件传输、复制粘贴、远程打印、会话录制等。

当用户远程访问目标计算机（执行远程控制、后台文件传输或后台命令）时，目标计算机上会显示强制通知，以防止未经授权的监控并确保用户隐私。

目标计算机可以配置为在空闲一定时间后自动终止远程会话。

目标计算机也可以配置为会话结束时自动返回操作系统锁定界面。

目标计算机可以配置为在远程桌面会话中自动显示黑屏，以保护远程用户操作的隐私性。

审计

所有远程桌面会话均有日志记录，包括以下信息：

- 开始时间、结束时间和持续时间
- 被访问的目标计算机名称及其 IP 地址
- 执行远程访问的用户的 Splashtop On-Prem 账户名称、用于远程访问的设备名称以及其 IP 地址

- 网页控制台会显示当前正在进行的远程桌面会话

所有文件传输活动均有日志记录，包括以下信息：

- 时间戳
- 被访问的目标计算机名称及其 IP 地址
- 执行远程访问的用户的 Splashtop ID、用于远程访问的设备名称以及其 IP 地址
- 文件名和大小
- 传输方向

团队管理历史记录（管理用户、权限更改、添加和删除电脑、在新设备上登录、团队设置更新、登录尝试失败等）遵循相同的日志结构。

最近 12 个月的日志可到 Splashtop On-Prem 网页控制台以 CSV 格式导出，便于查看和存档，也可以实时持续转发至 syslog 服务器。

Splashtop On-Prem 产品与支持的工单系统集成时，日志会自动存档到相应的工单中。

远程桌面会话可以录制。团队所有者可以通过网页控制台，启用对所有会话的自动录制功能，并为录制内容配置存储位置。可以通过会话工具栏随时开始和停止录制。

基础设施

Splashtop On-Prem 支持多种部署选项。

单节点部署

Splashtop On-Prem 可作为单节点 Windows 安装程序使用，适用于服务要求较低的小型组织。系统管理员可以通过 Windows 环境安装额外的安全工具以增强安全性。

集群节点部署

对于服务要求较高的大型组织，Splashtop On-Prem 支持在集群的 Windows 环境中部署，以提高可扩展性和性能。

合规性

请到网站 https://www.splashtop.com/compliance 了解 Splashtop 有关行业标准的最新信息。

ISO/IEC 27001
ISO 27001 是建立和维护强大信息安全管理系统（ISMS）的最受国际认可的基准。

Splashtop 获得 ISO 27001 认证，可向客户、合作伙伴和利益相关者保证已实施强大的安全措施，以保护信息安全并保持数据的机密性、完整性和可用性。

服务组织控制 2 (SOC 2)
SOC 2 认证表明组织已经建立并正确使用控制措施，以确保客户数据的安全和隐私。

Splashtop 保持对 SOC 2 Type 2 和 SOC 3 的合规性。

健康保险可携性与责任法案（HIPAA）
HIPAA 合规标准不适用于 Splashtop，因为 Splashtop 不处理、存储或访问用户计算机数据。Splashtop 传输但不存储屏幕捕获和文件传输流数据，采用端到端加密。

如果 Splashtop 产品可以正确使用上述安全控制，则有助于用户遵循其组织的 HIPAA 要求。

家庭教育权和隐私法案（FERPA）
与上述情况类似，FERPA 合规标准也不适用于 Splashtop，因为 Splashtop 不处理、存储或访问学生的教育记录。

如果 Splashtop 产品可以正确使用上述安全控制，则有助于用户遵循其组织的 FERPA 要求。

通用数据保护条例（GDPR）
Splashtop 作为数据控制者和处理者遵循欧盟用户的 GDPR 要求。用户有权访问、更正和删除其个人数据。

加州消费者隐私法案（CCPA）

Splashtop 符合面向加利福尼亚居民的 CCPA 要求。用户有权访问、更正和删除其个人数据。