Produits Splashtop Cloud

Présentation de la sécurité

Mis à jour le 17 avril 2026

Sommaire

Introduction 3
Produits 3
Présentation de l'architecture 4
Protocoles et composants 6
Fonctionnalités de sécurité 7
Infrastructure 11
Conformité 12

Introduction

Ce livre blanc présente une vue d'ensemble technique des produits professionnels Splashtop Cloud sous l'angle de la sécurité. Il couvre l'architecture, les protocoles, l'infrastructure et les composants des produits Splashtop. Ce document peut aider les professionnels de la technique et de la sécurité à comprendre la conception de Splashtop du point de vue de la sécurité. Il peut également les aider à utiliser les produits de manière à respecter et à compléter les exigences de sécurité de leur organisation.

Remarque à l'attention des utilisateurs de l'Union européenne (UE)
Par défaut, les utilisateurs de l'UE sont invités à créer leur compte utilisateur sur l'infrastructure cloud de Splashtop située en Allemagne. Il s'agit d'une infrastructure indépendante, distincte de celle basée aux États-Unis qui dessert les utilisateurs de Splashtop dans le reste du monde. Cette séparation permet aux utilisateurs de se conformer aux exigences en matière de souveraineté des données auxquelles ils peuvent être soumis.

Produits

Ce livre blanc concerne la suite de produits Splashtop de bureau à distance **basés sur le cloud** destinés aux entreprises (décrits ci-dessous). Ces produits permettent aux particuliers et aux entreprises de contrôler et de gérer à distance des ordinateurs et des appareils mobiles à des fins de productivité et d'assistance.

Ces produits sont conçus dans un souci de sécurité, afin de garantir que seuls les utilisateurs autorisés y aient accès, de protéger les données de bout en bout et de permettre aux utilisateurs d'auditer intégralement l'activité.

La suite de solutions de bureau à distance dans le cloud de Splashtop comprend trois produits :

- *Splashtop Enterprise*. Destiné aux organisations ayant besoin d'un accès et d'une assistance à distance de niveau entreprise, avec authentification unique, contrôles granulaires, capacités de journalisation étendues (y compris l'exportation SIEM et l'enregistrement dans le cloud), workflow de centre de services, intégration ITSM, accès programmé, API ouvertes, accès RDP/VNC/SSH, et bien plus encore.

- *Splashtop Remote Support*. Destiné aux MSP et aux professionnels de l'informatique pour accéder à distance aux ordinateurs qu'ils gèrent. Le logiciel agent est préinstallé sur les ordinateurs. Les autorisations d'accès sont strictement contrôlées.
  Les techniciens du service d'assistance peuvent également aider leurs utilisateurs de manière ponctuelle, sans installation préalable et grâce à un processus simple consistant à télécharger et à exécuter le logiciel.
- *Splashtop Remote Access*. Destiné aux professionnels ou aux petites équipes pour accéder à distance à leurs ordinateurs de travail à tout moment et depuis n'importe où. Le logiciel agent est préinstallé sur les ordinateurs. Les autorisations d'accès sont strictement contrôlées.

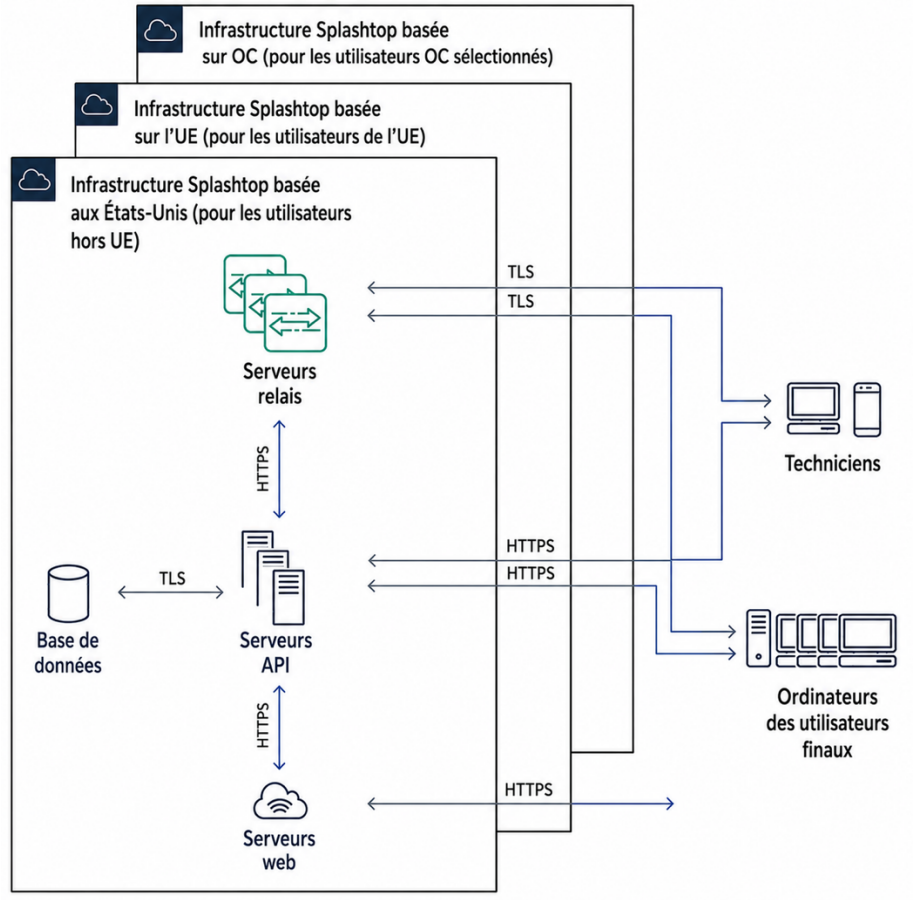
Vue d'ensemble de l'architecture

L'architecture des produits Splashtop basés sur le cloud se compose des éléments principaux suivants :

- Un logiciel agent installé sur les appareils des utilisateurs finaux (« *Splashtop Streamer* »)
- Une application pour techniciens installée sur les appareils des techniciens (« application *Splashtop Business* »)
- Des serveurs API
- Serveurs relais
- Serveurs Web
- Base de données

Splashtop gère trois ensembles d'infrastructures cloud : un pour les utilisateurs de l'UE, un pour les utilisateurs hors UE et un pour certains clients en Océanie. Chaque ensemble d'infrastructures cloud contient ses propres serveurs API, serveurs Web et base de données. Les données des utilisateurs sont totalement séparées entre les trois ensembles d'infrastructures. Les données au repos sont stockées sous forme chiffrée dans la région de souveraineté correspondante.

Le schéma ci-dessous illustre les principaux composants de l'infrastructure cloud de Splashtop, leurs voies de communication et les protocoles utilisés.



Les communications entre tous les composants susmentionnés sont chiffrées.

Les serveurs Web utilisent le protocole HTTPS standard sur le port 443

avec TLS 1.2. Les serveurs API utilisent le protocole HTTPS standard sur

le port 443 avec TLS 1.2.

Les serveurs relais utilisent le protocole TCP sur le port 443 avec TLS 1.2 et un chiffrement AES-256.

Protocoles et composants
(du point de vue de la sécurité)

Les serveurs API Splashtop sont répartis de manière équilibrée entre la Californie et l'Oregon pour l'infrastructure américaine, en Allemagne pour l'infrastructure européenne et en Australie pour l'infrastructure océanienne.
Les serveurs relais sont répartis sur plusieurs sites à travers le monde, afin d'être à proximité des utilisateurs et d'améliorer les performances pour ces derniers en Amérique du Nord, en Amérique du Sud, en Europe, au Moyen-Orient, en Afrique, en Asie et en Australie.
Les serveurs Web sont situés en Oregon pour l'infrastructure américaine, en Allemagne pour l'infrastructure européenne et en Australie pour l'infrastructure océanienne.
La base de données est également située en Oregon pour l'infrastructure américaine, en Allemagne pour l'infrastructure européenne et en Australie pour l'infrastructure océanienne, avec des systèmes de sauvegarde et de reprise après sinistre interrégionaux.

Serveurs API
Les points de terminaison (*Splashtop Streamer* et l'application *Splashtop Business*) communiquent avec les serveurs API via le protocole HTTPS standard. Le protocole HTTPS protège toutes les informations en transit. Chaque serveur API dispose d'un certificat SSL signé par une autorité de certification (RSA SHA-2 2048 bits), afin de garantir son identité et d'empêcher les attaques de type « man-in-the-middle ».
Le serveur API utilise le protocole TLS 1.2.

Serveurs relais
Les terminaux (*Splashtop Streamer* et l'application *Splashtop Business*) établissent chacun une connexion TLS sur TCP avec les serveurs relais. Le serveur relais met alors en place un tunnel de bout en bout entre les deux terminaux correspondants. Les deux terminaux négocient directement entre eux le protocole TLS et la clé de chiffrement AES-256. Le tunnel chiffré ainsi créé achemine les données de la session à distance. Les données sont protégées de bout en bout et ne peuvent être déchiffrées qu'au niveau des terminaux des utilisateurs.
Chaque serveur relais dispose d'un certificat SSL signé par une autorité de certification (RSA SHA-2 à 2 048 bits).
Le serveur relais utilise le protocole TLS 1.2.

Serveurs Web
Les serveurs Web fournissent aux clients l'interface de gestion en ligne. C'est là que les clients consultent et gèrent l'ensemble des ordinateurs, des utilisateurs, des techniciens et des journaux d'audit.
La console Web est accessible uniquement via HTTPS avec TLS 1.2, ce qui sécurise toutes les informations en transit.
Chaque serveur web dispose d'un certificat SSL signé par une autorité de certification (RSA 2048 bits, SHA-256).

Base de données
La base de données est un cluster de bases de données chiffré (AES-256). Elle est sauvegardée quotidiennement dans plusieurs régions. Les sauvegardes sont également chiffrées.
La base de données stocke les hachages des mots de passe des utilisateurs, et non les mots de passe eux-mêmes. Les hachages sont générés avec l'algorithme SHA-512 en utilisant un « salt » unique de 20 caractères pour chaque mot de passe.

Logiciels des terminaux
Le logiciel de terminal comprend l'application *Splashtop Business*, *le Splashtop Streamer* et l'application *Splashtop SOS* (pour l'assistance ponctuelle). Ces logiciels sont téléchargés depuis les sites web de Splashtop via HTTPS, ce qui garantit l'authenticité de la source.
Les binaires sont signés numériquement à l'aide des certificats appropriés afin de garantir leur intégrité.
Les exécutables Windows sont signés à l'aide de certificats X.509 à validation étendue (EV)
X.509 à validation étendue.
Les exécutables macOS sont signés à l'aide d'un certificat X.509, conformément aux exigences d'Apple pour les développeurs.

Fonctionnalités d' de sécurité

Les fonctionnalités de conception de Splashtop qui garantissent la sécurité de ses utilisateurs peuvent être classées en trois grandes catégories : **l'authentification**, **l'autorisation** et **l'audit**.

Splashtop est conçu selon des exigences **d'authentification** strictes, afin de garantir que les utilisateurs sont bien ceux qu'ils prétendent être.

Il existe également un ensemble robuste de contrôles **d'autorisation**, permettant de définir avec précision les droits et les autorisations d'accès des utilisateurs authentifiés. L'autorisation peut s'appuyer sur les fonctionnalités SSO (authentification unique

), SCIM (System for Cross-domain Identity Management) et JIT (Just-in-Time) de l'organisation pour un contrôle centralisé et une meilleure automatisation.

Enfin, un système complet de journalisation est en place pour permettre la surveillance et **l'audit**.

Authentification
Divers mécanismes sont en place pour garantir que les utilisateurs qui se connectent pour utiliser Splashtop sont bien ceux qu'ils prétendent être.

- *Identifiants Splashtop*. Les identifiants Splashtop (identifiant Splashtop et mot de passe) constituent la base de l'authentification. L'identifiant Splashtop est une adresse e-mail vérifiée. Le mot de passe doit répondre à certaines exigences de complexité.
  L'authentification unique (SSO) est disponible avec *Splashtop Enterprise*, afin de centraliser l'authentification via l'annuaire de l'organisation. Splashtop prend en charge le SSO via SAML 2.0 et OpenID Connect. Des connecteurs prêts à l'emploi sont disponibles pour la plupart des fournisseurs d'identité courants.
- *Authentification des appareils*. Chaque fois qu'un utilisateur se connecte à Splashtop, que ce soit via la console Web ou l'application *Splashtop Business*, un contrôle obligatoire d'authentification de l'appareil est effectué. Si l'appareil ou le navigateur est nouveau, l'utilisateur doit alors suivre une procédure d'authentification de l'appareil. Cette procédure vérifie que l'utilisateur est bien le propriétaire de l'adresse e-mail associée à son identifiant Splashtop.
  Les administrateurs et les utilisateurs peuvent consulter la liste des appareils authentifiés et invalider des appareils à tout moment via la console Web. Le responsable de l'équipe peut également limiter la durée pendant laquelle les appareils restent authentifiés.
  De plus, les administrateurs ont la possibilité de faire en sorte que les e-mails d'authentification des appareils de tous les utilisateurs soient envoyés uniquement à eux-mêmes, afin de garder un contrôle total sur les appareils que les utilisateurs peuvent utiliser pour se connecter à distance.
- *Vérification en deux étapes*. Un utilisateur peut configurer la vérification en deux étapes. Celle-ci repose sur le protocole TOTP et nécessite l'enregistrement d'un appareil mobile et d'une application d'authentification. Parmi les applications d'authentification prenant en charge le protocole TOTP figurent *Google Authenticator*, *Cisco Duo Mobile* et *Microsoft Authenticator*. Une fois la vérification en deux étapes activée, la connexion au compte Splashtop sur la console Web ou dans l'application *Splashtop Business* nécessite la saisie d'un mot de passe à usage unique et à durée limitée généré par l'application d'authentification

sur l’appareil mobile enregistré.
Le responsable de l’équipe a la possibilité d’exiger que tous les utilisateurs de l’équipe utilisent l’authentification en deux étapes. Le propriétaire de l’équipe a également la possibilité de gérer les appareils de confiance des utilisateurs et la durée pendant laquelle ces appareils restent de confiance.

- *Liste blanche d’adresses IP*. Le propriétaire de l’équipe peut restreindre les adresses IP à partir desquelles l’application *Splashtop Business* et la console Web sont accessibles. Par exemple, un centre d’appels peut limiter l’utilisation de Splashtop aux seuls moments où les techniciens se trouvent sur site.

Autorisation

Le propriétaire et les administrateurs de l’équipe peuvent spécifier quels utilisateurs ou groupes d’utilisateurs ont accès à quels ordinateurs ou groupes d’ordinateurs précisément.
Le propriétaire de l’équipe et les administrateurs peuvent inviter, activer, désactiver et supprimer des utilisateurs via la console Web.
Les organisations disposant d’une authentification unique (SSO) et de fournisseurs d’identité prenant en charge SCIM ou JIT peuvent rationaliser davantage le flux de travail en effectuant le provisionnement, le regroupement et la configuration des autorisations via leurs annuaires, puis en répercutant automatiquement ces modifications de configuration vers Splashtop.
Les droits d’accès sont vérifiés à plusieurs niveaux, notamment au moment de l’établissement d’une connexion.
Une autorisation supplémentaire peut être requise lors d’une tentative de connexion. Par exemple, l’utilisateur peut être amené à saisir les identifiants du compte Windows ou Mac de l’ordinateur cible, ou un code de sécurité personnalisé spécifique à cet ordinateur.
L'ordinateur cible peut également être configuré pour exiger l'autorisation explicite de l'utilisateur se trouvant actuellement devant l'ordinateur (sous la forme d'une fenêtre contextuelle avec un compte à rebours), lors de la dernière étape de l'établissement de la connexion.
Dans le cas d’une assistance ponctuelle via *Splashtop Remote Support* ou *Splashtop Enterprise*, le processus d’accès à distance est lancé par l’utilisateur final sur l’ordinateur cible. L’utilisateur final doit cliquer explicitement sur un lien URL, télécharger une application, lancer l’application, etc. afin d’autoriser l’accès à distance du technicien.
Le responsable de l’équipe a la possibilité de désactiver complètement certaines fonctionnalités, si nécessaire pour se conformer aux exigences de sécurité de l’organisation. Ces fonctionnalités comprennent le transfert de fichiers, le copier-coller, l’impression à distance, les commandes à distance, l’enregistrement de session, le redémarrage, et bien d’autres encore. Avec *Splashtop Enterprise*, diverses fonctionnalités

peuvent être contrôlées avec une grande précision, jusqu'au niveau de l'utilisateur ou du groupe d'utilisateurs.
Lorsqu'un utilisateur accède à distance à un ordinateur cible (pour effectuer un contrôle à distance, un transfert de fichiers en arrière-plan ou une commande en arrière-plan), une notification obligatoire s'affiche sur l'ordinateur cible. Cela permet de se prémunir contre toute surveillance non autorisée et de garantir la confidentialité de l'utilisateur.
L'ordinateur cible peut être configuré pour mettre automatiquement fin à une session à distance s'il reste inactif pendant un certain temps. Il peut également être configuré pour revenir automatiquement à l'écran de verrouillage du système d'exploitation à la fin d'une session.
L'ordinateur cible peut être configuré pour que son écran s'éteigne automatiquement lorsqu'une session de bureau à distance est en cours. Cela permet de protéger la confidentialité des actions de l'utilisateur distant.

Audit
Toutes les sessions de bureau à distance sont consignées, avec les informations suivantes :

- Heure de début, heure de fin et durée
- Nom de l'ordinateur cible auquel on accède et son adresse IP
- L'identifiant Splashtop de l'utilisateur ayant effectué l'accès à distance, le nom de l'appareil utilisé pour l'accès à distance et l'adresse IP de cet appareil
- Les sessions de bureau à distance en cours sont signalées comme telles sur la console Web.

Toutes les activités de transfert de fichiers sont consignées, avec les informations suivantes :

- Horodatage
- Nom de l'ordinateur cible auquel on accède et son adresse IP
- L'identifiant Splashtop de l'utilisateur ayant effectué l'accès à distance, le nom de l'appareil utilisé pour l'accès à distance et l'adresse IP de cet appareil
- Nom et taille du fichier
- Sens du transfert

Les sessions de commandes à distance, les sessions de chat et les autres types de sessions sont également consignés, y compris la transcription complète de la session le cas échéant.
Tous les journaux ci-dessus peuvent être consultés dans la console Web Splashtop, pour les 90 derniers jours.

L'historique de gestion de l'équipe (gestion des utilisateurs, modifications des autorisations, ajout et suppression d'ordinateurs, connexions sur de nouveaux appareils, tentatives de connexion infructueuses, etc.) peut être consulté dans la console Web Splashtop pour les trois dernières années.
Les journaux des 12 derniers mois peuvent être archivés en les exportant au format CSV depuis la console Web. Avec *Splashtop Enterprise*, les journaux peuvent également être récupérés en continu et automatiquement via une intégration SIEM ou une intégration API ouverte.
Si le produit Splashtop est utilisé conjointement avec un système de tickets pris en charge, les journaux sont directement intégrés aux tickets correspondants dans ce système.
Les sessions de bureau à distance peuvent être enregistrées, les enregistrements étant stockés localement sur le poste de travail du technicien. L'enregistrement peut être lancé et arrêté à tout moment via la barre d'outils de la session. Le responsable de l'équipe peut également activer l'enregistrement automatique et obligatoire de toutes les sessions, ainsi que configurer le chemin d'accès au stockage et la taille maximale des enregistrements. *Splashtop Enterprise* offre en outre la possibilité d'enregistrer dans le cloud[†] , ce qui peut s'avérer important pour des raisons de facilité d'utilisation et de conformité. Les enregistrements dans le cloud sont conservés pendant 90 jours et peuvent être visionnés ou téléchargés via la console Web.

Infrastructure

L'infrastructure de Splashtop s'appuie sur des fournisseurs d'infrastructure en tant que service (IaaS) tels qu'Amazon Web Services (AWS), Google Cloud Platform (GCP) et Oracle Cloud Infrastructure (OCI).

Ces fournisseurs garantissent une disponibilité élevée et la sécurité physique de leur infrastructure. Splashtop a mis en place des couches supplémentaires de redondance et de logique de basculement entre les différents fournisseurs afin d'améliorer encore la fiabilité. Comme indiqué précédemment, Splashtop dispose de nombreux points de présence à travers le monde, afin d'être au plus près des utilisateurs pour garantir de bonnes performances et assurer une redondance interrégionale.

Splashtop utilise également divers services proposés par ces fournisseurs d'infrastructure, en plus des instances de calcul standard. Parmi les services supplémentaires utilisés figurent des bases de données gérées, le stockage dans le cloud, la mise en cache en périphérie, des équilibreurs de charge, un service DNS et divers outils de surveillance.

Conformité

Consultez la page https://www.splashtop.com/compliance pour obtenir les dernières informations concernant la conformité de Splashtop aux normes du secteur.

ISO/IEC 27001:2022
La norme ISO/IEC 27001 est une référence internationalement reconnue pour la mise en place et le maintien d'un système de gestion de la sécurité de l'information robuste. Grâce à son ensemble complet d'exigences strictes, cette norme favorise une approche holistique de la sécurité de l'information en évaluant de manière approfondie les personnes, les politiques et les technologies par le biais de tests et d'audits rigoureux. Splashtop se soumet à des audits annuels ISO/IEC 27001.

Service Organization Control 2 (SOC 2)
SOC 2 est un cadre de reporting complet mis en place par l'American Institute of Certified Public Accountants (AICPA).
L'attestation SOC 2 démontre que des contrôles sont en place et correctement utilisés par Splashtop pour garantir la sécurité et la confidentialité des données de ses clients.
Splashtop fait l'objet d'audits SOC 2 annuels et maintient sa conformité aux normes SOC 2 Type 2 et SOC 3.

Loi sur la portabilité et la responsabilité en matière d'assurance maladie (HIPAA) La conformité à la norme HIPAA ne s'applique pas à Splashtop, car Splashtop ne traite ni ne stocke aucune donnée informatique des utilisateurs et n'y a pas accès. Splashtop facilite la transmission de vidéo, d'audio et de données, mais ne stocke pas les flux.
La transmission est chiffrée de bout en bout.
Les produits Splashtop, lorsqu'ils sont utilisés correctement avec les contrôles de sécurité décrits précédemment, aident les utilisateurs à respecter les exigences HIPAA de leur organisation.

Loi sur les droits à l'éducation et la confidentialité des familles (FERPA) De même que ci-dessus, la conformité à la loi FERPA ne s'applique pas à Splashtop, car Splashtop ne traite pas, ne stocke pas et n'a pas accès aux dossiers scolaires des élèves.
Les produits Splashtop, lorsqu'ils sont utilisés correctement avec les contrôles de sécurité décrits précédemment, aident les utilisateurs à respecter les exigences FERPA de leurs établissements d'enseignement.

Règlement général sur la protection des données (RGPD)
Splashtop se conforme aux exigences du RGPD pour les utilisateurs de l'Union européenne, en tant que responsable du traitement et sous-traitant. Les utilisateurs ont le droit d'accéder à leurs données à caractère personnel, de les rectifier et de les supprimer.

Loi californienne sur la protection de la vie privée des consommateurs (CCPA)
Splashtop se conforme aux exigences de la CCPA pour les résidents californiens. Les utilisateurs ont le droit d'accéder à leurs données personnelles, de les rectifier et de les supprimer.

---

† Remarque particulière concernant l'enregistrement des sessions dans le cloud : nous sommes conscients que l'enregistrement des sessions est une question extrêmement sensible et confidentielle ; c'est pourquoi nous avons mis en place des mesures de sécurité strictes en conséquence. Les enregistrements de sessions ne sont pas accessibles aux employés de Splashtop. Ils ne sont accessibles que de machine à machine, dans le seul but de permettre à nos utilisateurs de visionner et de télécharger leurs propres enregistrements depuis la console Web. La seule exception concerne un accès temporaire et surveillé à des fins de dépannage, qui nécessite l'autorisation de la direction.