



Splashtop Secure Workspace

Interne en externe gebruikers meer mogelijkheden geven: overal veilige, hoogwaardige access

Veilige toegang voor IT, freelancers en werknemers

Splashtop Secure Workspace biedt uitgebreide controle en zichtbaarheid over third-party, privileged, and application access, inclusief internetconnectiviteit. Door gebruik te maken van een single-pass-architectuur authenticereert het identiteiten, beveiligd het endpoints, beveiligd het privileged accounts en filtert het traffic om bedreigingen te isoleren. Aangedreven door een architectuur waarvoor patent is aangevraagd en een nieuwe security technology stack, presteert het beter dan de concurrentie dankzij een snellere implementatie en minder operationele wrijving.



Belangrijkste functies en mogelijkheden:

Zero Trust Network Access (ZTNA)

- Vervangt traditionele VPN's door snellere, veiligere en veerkrachtigere netwerktoegang, waardoor de toegang tot applicaties op elk netwerk wordt beveiligd.
- Valideert de toegang op basis van identiteit, apparaatstatus en contextuele factoren, die BYOD ondersteunen voor zowel beheerde als onbeheerde apparaten.
- Handhaaft het Zero Trust-beleid voor hybride workloads, met beveiligde toegang via clients zonder client en via apparaten.

Privileged Access Management (PAM)

- Beveiligt de inloggegevens van geprivilegieerde accounts met seamless injection, zodat gebruikers zero visibility hebben, en wordt aangevuld met live monitoring en sessieopnames.
- Automatiseert het beheer en de rotatie van inloggegevens voor Windows/Active Directory, geïntegreerd met Secret Vault voor veilige injectie van inloggegevens.
- Implementeert Zero Touch Provisioning voor naadloze integratie met een bestaande infrastructuur zonder wijzigingen in de firewall of routing, en inclusief automatische detectie van toepassingen.

Just-in-time en on-demand access (JIT)

- Integreert met samenwerkingstools zoals Microsoft Teams en Slack en biedt zero standing privileges en gebruiksvriendelijke toegang.
- Maakt JIT-access mogelijk via hyperlinks of QR-codes voor verschillende soorten toegang, waaronder Zero Trust Network Access, Privileged Access en Remote Browser Isolation.
- Breidt JIT- en On-Demand access uit tot SaaS en non-SSO webtoepassingen, waarbij een Zero Trust-beleid wordt geïmplementeerd dat is geoptimaliseerd voor toegang door derden.

Beveiligde internettoegang (SWG, DNS, RBI)

- Biedt geavanceerde verdediging tegen bedreigingen met DNS- en URL-filtering, cloud controls, SSL-inspection, DLP, anti-malware en breidt RBI-controls uit om Zero Trust af te dwingen voor alle internetactiviteiten.
- Verplaatst Secure Web Gateway naar het endpoint voor een snellere, meer betrouwbare ervaring zonder omwegen in het verkeer of wrijving.
- Breidt de SWG-, DNS- en RBI-controls uit met ZTNA en toegang tot privétoepassingen.

Uitgebreide SaaS-security (CASB, BYOI, RBI)

- Implementeert Zero Trust-securitymaatregelen voor SaaS-toepassingen om ongeoorloofde toegang van gebruikers of apparaten tot gevoelige informatie te voorkomen.
- Maakt identitymanagement en identityproxy mogelijk met Single Sign-On (SAML, OIDC, OAuth2), Multi-factor-authenticatie (MFA) en voorwaardelijke toegang. Ondersteunt Bring Your Own Identity (BYOI) voor derden.
- Biedt uitgebreide controle over cloud-apps met CASB en DLP-diensten, die ervoor zorgen dat de wetgeving inzake gegevensbescherming wordt nageleefd.
- Integreert Privileged Access Management (PAM) en Remote Browserisolatie (RBI) voor een veiligere aanpak, waarbij veilige, bewaakte toegang tot SaaS-platforms wordt gegarandeerd.

Belangrijkste functies en mogelijkheden:



Standards & Compliance

Splashtop voldoet aan AVG, SOC 2 en ISO/IEC 27001-gecertificeerd en ondersteunt de compliance-standaarden van de sector, waaronder HIPAA, CCPA, FERPA, en PCI.



Trusted Solution Vendor

Meer dan 30 miljoen Splashtop-gebruikers, meer dan 250.000 zakelijke klanten, waaronder 85% van de Fortune 500-bedrijven, rekenen op Splashtop voor snelle, veiligere remote access.

Meer informatie vindt u op splashtop.com