

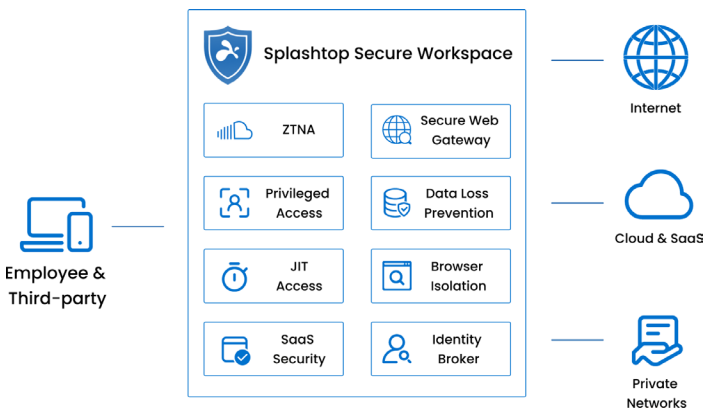


Splashtop Secure Workspace

Empowering Internal and External Users:
Secure, High-Performance Access Anywhere

Secure Access for IT, Third-Parties & Employees

Splashtop Secure Workspace offers comprehensive control and visibility over third-party, privileged, and application access, including internet connectivity. Leveraging a single-pass architecture, it authenticates identities, secures endpoints, safeguards privileged accounts, and filters traffic to isolate threats. Powered by a patent-pending architecture and a novel security technology stack, it outperforms competitors with quicker deployment and reduced operational friction.



Key Features and Capabilities:

Zero Trust Network Access (ZTNA)

- Replaces traditional VPNs with faster, safer, and more resilient network access, securing application access on any network.
- Validates access based on identity, device posture, and contextual factors, supporting BYOD for both managed and unmanaged devices.
- Enforces Zero Trust policies across hybrid workloads, providing secure access through both clientless and device clients.

Privileged Access Management (PAM)

- Secures privileged account credentials with seamless injection, ensuring zero visibility to users, and is complemented by live monitoring and session recording.
- Automates credential management and rotation for Windows/Active Directory, integrating with Secret Vault for secure credential injection.
- Implements Zero Touch Provisioning for seamless integration with existing infrastructure without firewall or routing changes and includes application auto-discovery.

Just-in-Time and On-Demand Access (JIT)

- Integrates with collaboration tools like Microsoft Teams and Slack, offering zero standing privileges and user-friendly access.

- Enables JIT access through hyperlinks or QR codes for various access types, including Zero Trust Network Access, Privileged Access, and Remote Browser Isolation.
- Extends JIT and On-Demand Access to SaaS and non-SSO web applications, implementing Zero Trust policies optimized for third-party access.



Secure Internet Access (SWG, DNS, RBI)

- Delivers advanced threat defense with DNS and URL filtering, cloud controls, SSL inspection, DLP, anti-malware, and extends RBI controls to enforce Zero Trust across all Internet activity.
- Moves Secure Web Gateway to the endpoint for a faster, more reliable experience without traffic detour or friction.
- Broadens SWG, DNS, and RBI controls to include ZTNA and private application access.

Comprehensive SaaS Security (CASB, BYOI, RBI)

- Implements Zero Trust security measures for SaaS applications to prevent unauthorized access by users or devices to sensitive information.
- Facilitates identity management and identity proxy with Single Sign-On (SAML, OIDC, OAuth2), Multi-Factor Authentication (MFA), and conditional access. Supports Bring Your Own Identity (BYOI) for third-parties.
- Provides comprehensive control over cloud apps with CASB and DLP services, ensuring compliance with data protection laws.
- Integrates Privileged Access Management (PAM) and Remote Browser Isolation (RBI) for a more secure approach, ensuring secure, monitored access to SaaS platforms.

Key Features and Capabilities:

| | |
|--|---|
|  Standards & Compliance Splashtop is compliant with GDPR, SOC 2, and ISO/IEC 27001 certified and supports industry compliance standards including HIPAA, CCPA, FERPA, and PCI. |  Trusted Solution Vendor 30+ million Splashtop users, 250K+ business customers, including 85% of Fortune 500 enterprises depend on Splashtop for fast, secure, remote access. |
|--|---|

Learn more at splashtop.com/secure

