Data Sheet

Citrix Secure Private Acces

Protect access to all your IT-sanctioned apps with Citrix Secure Private Access service, a cloud-native Zero Trust Network Access (ZTNA) solution. Citrix Secure Private Access increases productivity by providing a unified portal for all IT-sanctioned apps; gives your employees the flexibility to use managed, unmanaged, or BYO devices; removes the day-to-day management overheads of appliance-based solutions; and improves the security of your IT environment with a zero-trust approach.

With the recent surge in hybrid work, IT has been tasked with enabling thousands of remote users with secure access to applications and data. Rather than a few users accessing the corporate networks via VPN, employees now work from both inside and outside the office. This has flipped the entire security posture of countless organizations.

While a few use cases may require traditional VPN solutions, these are disappearing as applications are rebuilt for the web, and some moved into the cloud. Additionally, in the race to provide remote access for employees and contractors, VPN clients are now running on unmanaged and untrusted devices. This has exposed organizations to many risks as IT lacks insight into the health of these devices or the contextual circumstances of users accessing their networks.

While many organizations still use traditional technologies like VPNs, ZTNA (Zero Trust Network Access) is the modern choice for secure access to IT-sanctioned applications.

Secure Private Access is an application access technology that follows a Zero Trust framework and helps customers looking to solve challenges for their remote and hybrid workforce. Based on the principles of Never Trust and Always Verify, ZTNA allows flexibility for end users to use managed, unmanaged, and BYO devices. It provides IT with granular and flexible security controls to monitor the user's device context, monitor end user's behavior throughout the user session, and enforce security controls as anomalies are detected in the user behavior to reduce the risk of unauthorized access.

VPNs may still be needed for IT administrators to manage behind-the-firewall assets such as servers and infrastructure systems. However, over 90% of users do not need VPNs to access their applications and data— ZTNA is the better choice. This allows you the flexibility to move workloads off VPNs at the pace that works best for your business.

Citrix Secure Private Access offers a broad range of features to protect your workforce independent of your working location and used device.

- **Zero Trust Network Access (ZTNA)** to all IT-sanctioned apps
- **Adaptive Authentication** to apply dynamic Multi-Factor-Authentication by classifying devices using Device Posture service (including 3rd party integration of Microsoft Intune or Crowdstrike), user role, geo-location and more
- **Adaptive Access & Security Controls** to provide granular access to applications and apply contextual security controls on browser-based apps to protect sensitive corporate data
- **Enterprise Browser** — A fully managed and locally installed chromium-based browser to access internal Web and SaaS apps, and to securely navigate the web both on managed and BYO devices
- **Single Sign On** for seamless access to browser-based apps
- **Remote Browser Isolation** to navigate the web without risk to corporate environments using a one-time browser
- **Visibility & Monitoring** to provide visibility across all application and user traffic in a single monitoring dashboard

Citrix Secure Private Access

Citrix Secure Private Access is a cloud delivered ZTNA solution that delivers adaptive access to IT-sanctioned applications whether they are deployed on-prem, or in the cloud. Traditional VPN solutions provide access at the network level and are vulnerable to network-level attacks, require backhauling of all traffic, and often need device management to capture the state of all end-user devices. Citrix Secure Private Access helps avoid these pitfalls. Citrix Secure Private Access provides access only at the application layer, preventing network-level attacks, and does not require traffic backhauling, creating a better end-user experience and providing IT with a set of security controls that offer employees the choice to access IT-sanctioned applications on any device, regardless of it being managed or personal (BYOD).

As a cloud service, it is available across all GEO locations and scales automatically as the user base and usage increase, delivering agility and always-on security for the best user experience and security. A fully managed service, Citrix Secure Private Access allows IT to focus on strategic initiatives rather than managing appliances across their data centers.

Citrix Secure Private Access – Use Cases

Replacing your existing VPN with Zero Trust access delivered as cloud service

Keeping application access secure was simpler when employees came to the office to work and when apps still lived in the corporate data center. As the workforce has moved to a hybrid work environment, employees are increasingly working from home on networks not secured by IT and on devices that are not managed by IT — and the security risk has grown infinitely large.

Citrix Secure Private Access removes the need for a VPN solution by providing a cloud-delivered zero trust-based approach to grant the user just enough permission to do his daily work. Enhance user productivity and experience while applying security by allowing direct access to SaaS apps to overcome the burden of backhauling traffic through the data center

Improve security for a successful BYOD program

If there's one struggle every IT professional will face, it's the rise of flexible BYO work policies. Citrix Secure Private Access provides both client-less or client-based secure access on BYO devices. Users can use their native browser to securely access applications through the Workspace for Web portal or by exposing the application to the internet using the Direct Access option. While the native browser is unable to apply security controls, the cloud-based Remote Browser Isolation service launches a one-time browser to provide the highest possible security.

If the user likes a client-based solution, Citrix Workspace app that includes the Citrix Enterprise Bowser can be installed on the BYO device to access all applications.

> “With Citrix, we have found a way to increase productivity and deliver a better employee experience. We’ve made remote work more secure. We’ve used analytics to provide better service to users.”
>
> – Gilliard Delmiro – CTO HDI

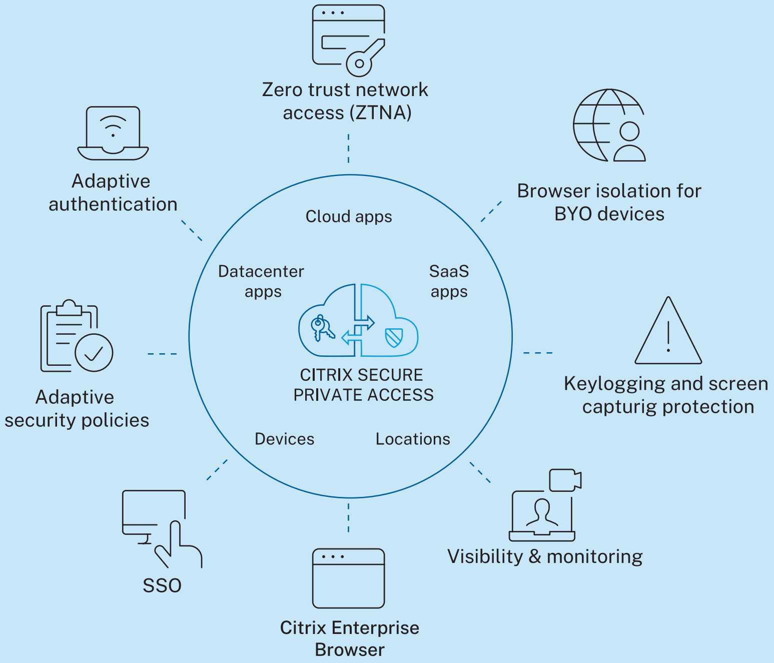
SSO with adaptive access

SSO solutions are intended to reduce the cost of management and provide better security, all while delivering an improved user experience. However, many solutions fall short, covering only one type or a subset of application types. This forces you to implement several access solutions from different vendors to cover your entire application landscape—negating the productivity and user experience benefits you hoped for. The complexity of this type of implementation runs counter to the zero-trust initiatives that many organizations are undertaking. Citrix Secure Private Access helps you to provide single sign-on to all the applications your team needs to be productive.

Faster onboarding of new employees and locations during M&A

For organizations that are growing fast and inorganically through mergers and acquisitions (M&A), it takes a long time to onboard new employees and new locations, thereby affecting their productivity and increasing the cost of these mergers. Citrix Secure Private Access supports smooth transitions and minimizes the impact on the business.

> “A Citrix zero trust architecture helps prevent malware, data exfiltration, or VPN breaches and attacks. Citrix Secure Private Access user identity verification and secure workspaces are the mechanisms that help alleviate these risks.”
>
> – Sriram Sitaraman – CIO Synopsys


Zero trust network access (ZTNA)
Browser isolation for BYO devices
Adaptive authentication
Cloud apps
Datacenter apps
SaaS apps
CITRIX SECURE PRIVATE ACCESS
Devices
Locations
Adaptive security policies
Keylogging and screen capturig protection
SSO
Citrix Enterprise Browser
Visibility & monitoring

Feature	Description	Citrix Secure Private Access Standard	Citrix Secure Private Access Advanced
Management Framework	Citrix-managed cloud service (SaaS)	●	●
Secure Access	Zero Trust Network access to intranet web apps	●	●
	Zero Trust Network access to SaaS apps	●	●
	Zero Trust Network access to TCP/UDP apps		●
	Secure access from a native mobile app, SaaS access and internal web access from mobile device	●	●
	Client-less access to internal web apps	●	●
	Custom portal for users to easily access all applications, files, email and other IT resources	●	●
	Broad client support for Citrix Workspace app for Win 32- and 64, macOS, Linux, iOS and Android	●	●
	Curated end user experience through Citrix Enterprise Browser	●	●
	Citrix Enterprise Browser that provides secure and SSO access to SaaS and web apps	●	●
Single Sign-On	SAML 2.0 Single Sign-on (SSO) for SaaS and intranet web apps	●	●
	Single Sign-on (SSO) to Intranet Web Apps (Basic/NTLM, Forms, Kerberos)	●	●
	One URL – Unified Portal to access all applications	●	●
	Identity provider support, including Microsoft AD, AAD, Okta, Google Cloud Identity and Adaptive Authentication	●	●
Multi-Factor Authentication	Support MFA with RADIUS (and 3rd party integrations)	●	●
	Native one-time password (TOTP)	●	●
Device Posture (Endpoint analysis)	Integrated endpoint scans client devices to determine if client security products (antivirus, personal firewall or other mandatory corporate programs) are active. It also scans for device location, device configuration, and more		●
	Enhanced device identity scans authenticate a device by scanning for a valid company-issued device certificate		●
	Advanced endpoint analysis capabilities using industry-standard APIs like OPSWAT		●
Security policies and controls	Adaptive Authentication and Adaptive Access (SaaS and web apps) with role, geo-location, and device posture check enable control over how users access and interact with SaaS and web apps. Capabilities include the ability to insert watermarks, restrict copy/paste, printing, and up/downloads.		●
	App Protection policies ensure user sessions and any sensitive information like user credentials, PHI, etc., stored in apps, is protected from dangerous malwares like keyloggers and screen capturing		●

Feature	Description	Citrix Secure Private Access Standard	Citrix Secure Private Access Advanced
	Browser isolation technology to allow users accessing IT-sanctioned apps from a BYO device, securely and seamlessly. Citrix Remote Browser Isolation service hosted in Citrix Cloud allows IT to isolate the end-user device from the application, hence protecting the application itself in case the device is compromised by malware or any malicious content		•
Visibility and Monitoring	Monitor app usage and troubleshoot issues like authentication, app enumeration, device compliance and more	•	•
Application and data security	All communication is secure through SSL/TLS encryption	•	•
High Availability and Fault tolerance	Basic high-availability configuration Links gateway appliances to create an active-passive pair, ensuring sessions remain active if the master fails	•	•
	Global server load balancing (GSLB) routes client connections to the cloud point of presence (PoP) based on availability, health, proximity and responsiveness	•	•
Simplified administration	Guided admin workflow provides an intuitive series of click-through screens and instructions for installation and configuration	•	•
	Administrative auditing and logging. Monitors configuration changes made by administrators to ensure accountability and easy rollback of configuration errors	•	•
	Auto-downloading and auto-updating client agents. Depending on your configuration, the Citrix Secure Access and Device Posture agent automatically downloads when the user connects to Citrix Cloud via Citrix Workspace app and ensures that the user always receives the latest version of the client software.	•	•
Data entitlements	Data consumption by end-user, but can be shared across user base	1 GB per user/month	5 GB per user/month
Connector Sizing	• Deploy connectors in pairs (Active - Active) for high availability. • Each connector supports up to 2000 concurrent users. • N+1 connectors recommended, where N is the number needed to reach the bandwidth/concurrent user requirement, with +1 for Fault Tolerance. Minimum requirements: 20 GB disk | 2 vCPUs | 4 GiB RAM | IPv4 network		

citrix™

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States

01Feb2024