White Paper

Citrix Secure Private Access: A better ZTNA alternative than Zscaler Private Access.

A feature-by-feature comparison.

With the recent surge in remote 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, entire organizations now work 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 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. Further, VPN solutions are inherently more prone to lateral movement and zero-day attacks.

While many organizations still use traditional technologies like VPNs, ZTNA (Zero Trust Network Access) is the most modern choice for secure access to IT applications. VPNs may still be needed for IT administrators to manage behind-the-firewall assets such as servers and infrastructure systems. However, more than 90% of users do not need VPNs to access their applications and data — and ZTNA is the better choice. This means you need the flexibility to move workloads off of VPNs at the pace that works best for your business.

Now that we have established why VPNs should not be the norm for remote access to enterprise resources, let's investigate why not every security provider can deliver the comprehensive protection you need.

If you're looking for a Zero Trust Network Access (ZTNA) solution, there's a good chance you're comparing Citrix and Zscaler. You may have heard about exceptional features promised by products like Zscaler Private Access. But do those offerings provide everything you need to protect against data loss?

As you determine which option is the best fit for your business, it is vital to look at core capabilities. This paper discusses why Zscaler Private Access (ZPA) does not fulfill all of the requirements to provide secure and reliable access to all of your applications and how Citrix Secure Private Access has an edge for enabling a VPN-less zero trust architecture.

Choice of connectivity for IT-sanctioned applications

- Citrix offers multiple options for securing access to applications, including VDI, DaaS, and VPN. And with Citrix Secure Private Access, you'll have a modern way to provide access to IT applications using a cloud-delivered ZTNA solution. This hides application IP addresses and resources from the Internet, also known as anonymous network.
- Zscaler offers only one way to access IT sanctioned applications with Zscaler Private Access, which does not cover the entire enterprise application spectrum.

Support for Application Types

Web Applications – Citrix Workspace and Zscaler Private Access enable access to on-premises web applications. These applications are accessible via a browser, but are not ready to be exposed to the public internet as it hosts company confidential data.

- **Citrix Workspace Browser** – Citrix Secure Private Access enables IT to apply granular security controls to prevent data exfiltration. These security policies regulate user operations based on user access context and device posture check. They can enforce controls like restricting copy/paste, printing, downloads, or adding a watermark to the web application.
- **Secure Browser hosted in Citrix Cloud** – IT can be confident that end users can securely navigate the web with this browser without introducing risk to the corporate environment. Threats that may be introduced by visiting malicious websites are isolated off the corporate network and devices. In addition, the browser is discarded at the end of the session, ensuring that any malicious software encountered while browsing the web never reaches your infrastructure.
- **Native Browser** – Native OS browsers can be used in clientless scenarios using DNS-managed direct connect capabilities within Citrix Secure Private Access, enabling trusted devices to access internal applications natively.

Client/Server Applications - Monolithic and client-server applications require clients locally installed on the devices. Such applications are tactical, but still tend to serve a critical purpose. Citrix Secure Private Access provides Zero Trust Network Access (ZTNA) to all private corporate applications, whether these applications are web, SaaS, TCP, UDP, or VDI and virtual applications, are deployed on-premises or on any public cloud, or accessed from within or from outside of the Citrix Workspace App. However, because these applications can also require substantial bandwidth and perform poorly when delivered through a ZTNA or VPN, Citrix DaaS may be a better option.

Citrix Secure Private Access	Zscaler Private Access
Citrix Secure Private Access provides Zero Trust Network Access (ZTNA) to all private corporate applications, whether these applications are web, SaaS, TCP, UDP, or DaaS (Desktop as a Service) and virtual applications, are deployed on-premises or on any public cloud, or accessed from within or from outside of Citrix Workspace.	Zscaler Private Access does not offer UDP or a DaaS solution for latency or bandwidth sensitive applications that may affect user experience.

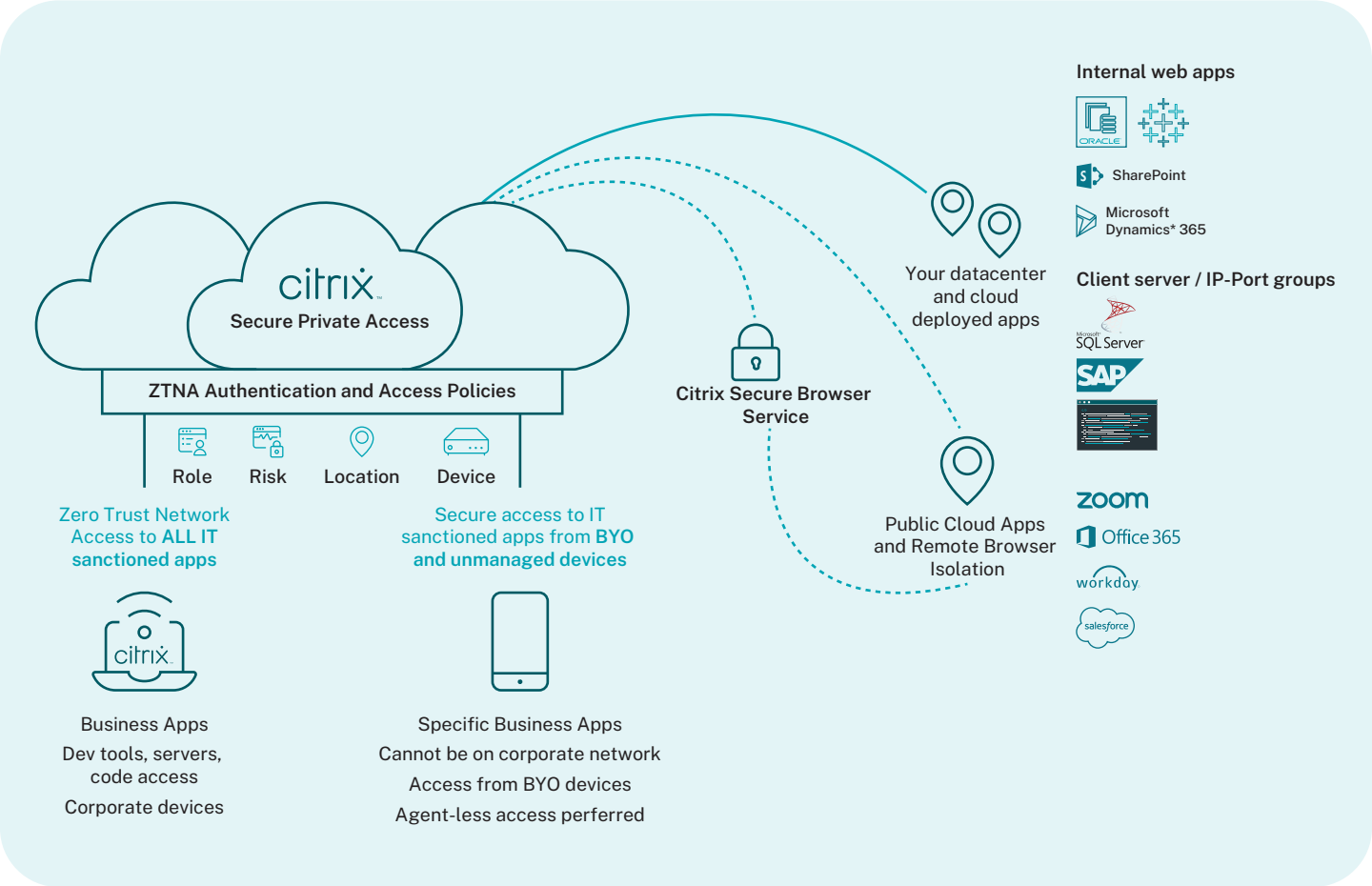
Native adaptive authentication and access policies

The way people work is changing, and traditional security architectures can't keep up. As your users become more distributed, and as more applications are delivered from the cloud, you need to protect against modern-day attacks looking to exploit applications and APIs. One of the best ways to strengthen your security posture is intelligent authentication with multi-factor authentication (MFA). By continually monitoring sessions for anomalous behavior, you can ensure your applications and data stay secure — without compromising the user experience or hindering productivity.

Citrix Secure Private Access	Zscaler Private Access
Citrix Secure Private Access features a native framework for adaptive authentication. Access is monitored at the application level based on factors such as geolocation, device posture, risk profiles, and more. Further, Citrix Secure Private Access adaptive authentication provides consistent policies that work across ZTNA applications and DaaS (Desktop-as-a-Service) already in use by Citrix customers.	Zscaler Private Access lean heavily on device posture and 3rd parties for risk profiles, not offering consistent policies across products and services. As a result, Zscaler Private Access administrators must create and maintain different policies across different products.

Session security

Both Citrix and Zscaler offer outbound connections and provide network and application isolation. Unlike what occurs with VPNs, both Citrix Secure Private Access and Zscaler Private Access do not allow the lateral movement of privilege from one application to the next. The connection is strictly outbound brokered. However, once an application session is established, Zscaler does not protect corporate data from being exfiltrated.



Keylogger and screen capture protection

With remote work on the rise, people are spending more time on public networks and personal devices—ones that can't be closely monitored by IT. That makes the risk from devices infected with keylogger and screen capture malware a constant concern. To protect against data exfiltration, it's imperative to have a security strategy in place that specifically addresses these threats.

Citrix Secure Private Access	Zscaler Private Access
Citrix Secure Private Access offers enforcing controls that prevent hijacking of user credentials or taking screenshots of applications accessed through Workspace app using keyloggers and screen capturing malware. These policies are mainly applicable for unmanaged and BYO devices that are exposed to any external threats.	Zscaler Private Access does not protect against malware looking to intercept and steal access to sensitive information. To protect against these threats, you'll need to buy a completely separate service.

Enhanced security policies and integrated remote browser isolation

As the use of BYO devices increases, existing solutions like traditional VPNs fall short. These traditional remote access technologies don't provide the protection you need. Because they require devices to be managed at all times, frustrated end users often go around IT when accessing corporate resources on personal devices.

Citrix Secure Private Access	Zscaler Private Access
With Citrix Secure Private Access, granular security policies let you control what users can do within applications based on which devices they're using. For example, you can provide full functionality on corporate-owned devices while disabling downloads or the ability to copy and paste from unmanaged and BYO ones. And with integrated remote browser isolation technology, users can securely access corporate applications from unmanaged devices or without a ZTNA plugin. Local sessions are also automatically redirected to a cloud-hosted browser, ensuring any malicious code on infected BYO devices won't reach your application workloads.	Zscaler Private Access does not include any in-session security controls apart from multi-factor authentication for BYO or unmanaged devices. It also requires a ZTNA plugin to be installed before a user can access even browser-based applications. And for granular security policies, Zscaler will push you to buy a completely new service such as Zscaler Internet Access, which can be costly.

With Citrix Secure Private Access, granular security policies let you control what users can do within applications based on which devices they're using.

Analytics

There is a common saying in the security world: "You can't protect what you can't see."

Citrix Secure Private Access provides basic insights into users' actions such as application access (Web, SaaS, TCP, UDP and Virtual), domains visited, files accessed and/or downloaded, and more.

Citrix Analytics easily integrates with Citrix Secure Private Access, providing comprehensive insights into user behavior, applications, devices, and networks. It uses machine learning algorithms to detect anomalous user behavior, troubleshoot user sessions, and view operational metrics for users in an organization that uses Citrix products. This helps reduce manual work for IT, provides timely enforcement, and reduces risk of breaches.

For more details on Citrix Analytics for Security, please visit here.

Ease of deployment

Citrix Secure Private Access offers both client-based and client-less ZTNA solutions. This enables access to applications on any device platform without having to download and install an agent, providing an excellent solution for both managed, unmanaged, and trusted devices.

Citrix Secure Private Access	Zscaler Private Access
Client-less – When accessing without the Secure Access agent using OS-native browsers, security policies defined by the administrator may automatically redirect the user to a secure hosted browser in Citrix cloud. This provides a web isolation solution, Secure Browser, that launches any web, SaaS, or virtual app while maintaining air gap between the device and the application. **Client-based with Secure Access Agent** – When accessing with client-based Secure Access agent, all private corporate applications can be accessed whether these applications are web, SaaS, 2, UDP, or VDI and virtual applications, are deployed on-premises or on any public cloud, or accessed from within or from outside of Citrix Workspace. Secure Access agent supports Windows, and macOS. **Client-based with Citrix Workspace app** – When accessing with the Citrix Workspace App, private corporate applications can be accessed whether these applications are web, SaaS, or VDI and virtual applications, or are deployed on-premises or on any public cloud. The Citrix Workspace app supports iOS, Android, Windows, macOS, Chrome OS, and Linux platforms, and provides the same experience as a browser-based HTML5 client.	Zscaler Private Access provides Zero Trust Network Access (ZTNA) only to web private corporate applications and does not support Chrome OS or Linux platforms.

The Citrix user experience

Many point solutions try unsuccessfully to fit your application and users' requirements into what a point product is capable of delivering. Citrix has an extensive portfolio of features and services that best fit your organization's multiple needs and enable IT to move at the speed of your business.

Furthermore, the client-based agent provides ZTNA and VPN access (via Citrix ADC), which enables a limited VPN footprint for organizations migrating from VPN to ZTNA in a phased manner.

Citrix Secure Private Access	Zscaler Private Access
Desktop as a Service – We have long known specific applications like client-server applications produce a poor user experience when accessed from a network that presents significant latency or loss. When users are not on the same network as these applications, their productivity will decrease, or in worst-case scenarios they will run into application issues. Users need a protocol built to deliver applications across poor network conditions, enabling the applications to run as they were designed. For such scenarios, Citrix Desktop as a Service with HDX offers the perfect remote secure access solution. Citrix HDX displays a protocol to run across any network, no matter how much latency exists or how many packets are lost. It optimizes audio, video, graphics, and even real-time communications. This also provides a great user experience, even when the network isn't very reliable. **Single sign-on (SSO)** – Citrix Secure PrivateAccess offers Single Sign-On (SSO) to access web applications, DaaS and virtual applications, and document repositories. This simplifies access for end-users, as they get a single pane of glass for all their applications and files. Citrix Secure Private Access acts as a broker and integrates with all major Identity Providers (Okta, Azure Active Directory, Active Directory, Google IdP, Cisco Duo, etc.), including providing support for SAML v2.0 that allow admins to plug any IdP of their choice and set up SSO from within the Citrix cloud. If your organization already has SSO and conditional access setup Citrix Secure Private Access will help expand existing conditional access policies and VPN with Contextual Access – While ZTNA is the most modern choice for secure access	Zscaler Private Access support Single Sign-On (SSO) for accessing only web applications with Identity Providers, including SafeNet, Okta, OneLogin, Ping, Active Directory.

Citrix Secure Private Access	Zscaler Private Access
to IT-sanctioned applications, VPNs may still be needed for IT administrators to manage behind-the-firewall assets such as servers and infrastructure systems. This means you need the flexibility to move workloads at the pace that works best for your business. Citrix ADC is a full-featured VPN solution *(additional licensing req.)* that can be deployed in parallel to Citrix Secure Private Access. As a leader in virtualization, only Citrix helps you access VDI and non-VDI applications using the latest ZTNA technology.	

Summary

When it comes to securing your hybrid remote workforce, there's a lot to consider. You need to protect unmanaged and BYO devices, control access to applications, and block malware that could exfiltrate data — all while providing an outstanding user experience. Though there are plenty of providers that specialize in individual categories, managing multiple vendors can be cumbersome and costly.

	Feature	Citrix Secure Private Access	Zscaler Private Access
Application Types	Client server apps	•	•
	Web apps	•	•
	SaaS apps	•	▪
	Desktop as a Service	▪	
	VPN	▪	

	Feature	Citrix Secure Private Access	Zscaler Private Access
Session Security	Anonymous Network	•	▫
	Session login monitoring of geolocation, device posture, risk profiles, etc.	•	◇
	Outbound app to app tunnel	•	•
	Browser navigation control	•	
	Integrated security analytics for continuous authentication and risk assessment	•	▫
	Data Protection: Watermarking, clipboard access etc.	•	
	Anti keylogger and screenshot protection	•	
Ease of Deployment	Access without a native client	•	•
	Access with a native client	•	•
	Client for iOS, Android, Windows and macOS	•	•
User Experience	Network optimization for Desktop as a Service	■	
	Single sign-on	•	

▫ Limited capabilities ■ Additional licensing required ◇ 3rd Party Vendor solution required

Relying on a solution such as Zscaler Private Access can also set the stage for overages and new charges each time you need another product or package. This is not the case with Citrix.

As the industry's most comprehensive offering, Citrix Secure Private Access provides ZTNA to all apps (virtual and non-virtual) with a single solution, offers different connectivity types (VPN, VPNless, micro VPN, and HDX) depending on the use case, and gives you integrated security analytics for continuous authentication and risk assessment. This empowers you to efficiently address the full range of zero trust capabilities while delivering an exceptional user experience — with no hidden costs or unexpected extras.

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