CITRIX CLOUD SOLUTIONS — ZERO TRUST NETWORK ACCESS

Citrix Secure Private Access

Citrix

Hybrid work, BYOD, and contractor access have made the corporate perimeter obsolete. Citrix Secure Private Access (SPA) replaces the VPN with a Zero Trust Network Access (ZTNA) framework — granting users least-privilege access to the specific applications they need, verifying identity and device posture at every step, and protecting sensitive data without restricting how people work.

- Zero Trust Network Access
- VPN-Less Application Delivery
- BYOD & Unmanaged Device Support
- Agentless Browser Isolation

OAS · Protect. Detect. Recover.

Prepared 11 September 2026

PLATFORM OVERVIEW

Two Technologies, One Shared Purpose

Understanding SPA starts with understanding where it fits alongside Citrix DaaS — the two products address different access scenarios and are frequently deployed together to meet the full range of an organisation's requirements.

Citrix DaaS — ICA/HDX Delivery: Application Runs in the Data Centre

Citrix DaaS virtualises an application inside the data centre and presents only the screen, mouse, and keyboard to the user over the ICA/HDX protocol. The application never leaves — only pixels travel across the network. Ideal for legacy Windows and Linux applications, GPU-heavy workloads, and users who need a full published desktop.

- Application executes on a remote Virtual Delivery Agent (VDA)
- Only screen output and input are transmitted — data stays centralised
- Best for legacy apps, complex workloads, and full virtual desktops
- Citrix Workspace App required on the user's device

Citrix SPA — ZTNA Delivery: Application Runs on the User's Device

Secure Private Access allows the application to run locally on the user's device or browser, with access to backend corporate resources flowing through a secure, encrypted ZTNA tunnel. Identity and device posture are verified continuously — not just at login — and access is granted at the application level, not the network level.

- Application runs locally — ZTNA tunnel connects to backend resources
- Zero Trust principles: constant verification, granular app-level controls
- Best for SaaS apps, internal web apps, and BYOD or contractor access
- Supports agentless access — no Workspace App required for web apps

WHEN TO USE WHICH

DaaS vs Secure Private Access — Side by Side

Neither DaaS nor SPA is universally superior. The right choice depends on the application, the user group, and the device. Most organisations deploy both — using each for the scenarios it was designed for.

| Feature | ICA/HDX Delivery — Citrix DaaS | Secure Private Access (SPA) |

| --- | --- | --- |

| Execution | Application runs on a remote Virtual Delivery Agent (VDA) inside the data centre. | Application runs locally on the user's device or in their browser. |

| Protocol | ICA/HDX protocol on ports 1494 or 2598. Only screen pixels and input travel the network. | HTTPS (port 443) or ZTNA tunnels for TCP/UDP traffic. |

| Primary use case | Legacy Windows and Linux applications, GPU-heavy workloads, and full published desktops. | Modern SaaS applications, internal web apps, and secure browser-based or client-based access. |

| Security model | Session-based isolation — application and data are contained within the VDA and never leave the data centre. | Zero Trust — continuous identity and device posture verification with granular, app-level access controls. |

| Data flow | Only screen pixels and mouse/keyboard inputs are transmitted. Data remains centralised at all times. | Application data flows to the local device through a secure, encrypted tunnel. App protection policies control what users can do with it. |

| Device requirement | Citrix Workspace App required. Managed and domain-joined devices preferred. | Supports managed, unmanaged, BYOD, and contractor devices — including fully agentless access via browser. |

The conundrum — which is better? Organisations today have many different user groups requiring access to a wide range of applications. Neither DaaS nor SPA is a one-size-fits-all solution. A user requiring access to SQL Management Studio via a locally installed tool needs SPA's ZTNA tunnel. A user requiring a full published Windows desktop with 12 legacy applications needs DaaS. Most environments require both — and OAS is experienced in designing architectures that deploy each correctly.

KEY CAPABILITIES

What Secure Private Access Does For Your Business

Six capabilities that make SPA the right choice for organisations extending secure access to a workforce that spans managed devices, personal laptops, and contractor hardware — without a VPN.

Zero Trust Access — Verify Everything, Trust Nothing

SPA does not grant network access — it grants application access. Every request is verified against identity, device posture, and location context before access is permitted. If a device becomes non-compliant mid-session, access is revoked automatically. No implicit trust, no lateral movement risk.

ZTNA FRAMEWORK

BYOD and Unmanaged Device Access

Employees using personal devices, contractors on unmanaged hardware, and remote workers on BYOD laptops can all access corporate applications securely — without installing agents, joining domains, or connecting to a VPN. Agentless access via the Citrix Enterprise Browser enforces watermarking, restricted copy-paste, and print controls.

AGENTLESS ACCESS

Remote Browser Isolation

For users accessing sensitive applications from untrusted devices or locations, SPA can redirect the session to a Remote Browser Isolation (RBI) environment in the cloud. The application renders in a secure remote browser — no data ever reaches the local device, eliminating the risk of data leakage or malware injection from unmanaged endpoints.

BROWSER ISOLATION

App Protection — Anti-Keylogging and Watermarking

SPA's app protection policies prevent keyloggers from capturing credentials entered in protected sessions, and apply dynamic watermarks to screens displaying sensitive data — embedding user identity and timestamp into every screen view. These controls operate even when the application runs on an unmanaged device outside corporate control.

DATA LEAK PREVENTION

Adaptive Authentication and Device Posture

SPA evaluates device posture at login and continuously during the session — checking for domain membership, certificate presence, OS version, screen lock status, and security software. Based on posture, users are granted full access, limited access, or redirected to an isolated environment. Trusted devices get a richer experience; untrusted devices get a secure, contained one.

CONTINUOUS VERIFICATION

Unified Workspace — SPA and DaaS Side by Side

SPA applications appear alongside published DaaS desktops and applications in the Citrix Workspace interface. Users see a single, unified portal — they do not know or care whether an application is delivered via ICA/HDX or a ZTNA tunnel. One login, one workspace, one experience, regardless of the delivery mechanism behind it.

SINGLE WORKSPACE

ACCESSING SPA APPLICATIONS

Three Ways Users Access Secure Private Access

The delivery method depends on whether you are using an agent-based or agentless approach, and how your users prefer to launch their applications. All three methods provide the same underlying Zero Trust security controls.

PRIMARY METHOD — AGENT-BASED

Citrix Workspace App

SPA applications appear inside the Citrix Workspace interface alongside any published DaaS apps and desktops. Web and SaaS applications open in the Citrix Enterprise Browser (CEB), enforcing security controls like watermarking and restricted copy-paste. TCP/UDP applications — such as a locally installed SQL Management tool — require the Citrix Secure Access agent and operate as if the user is on the internal network.

FULL FEATURE SET

NATIVE FEEL — AGENT-BASED

Local Application Shortcuts

The Workspace App can place Start Menu or Desktop shortcuts directly on the user's device for SPA-delivered applications. The Workspace App must be installed and authenticated to handle the ZTNA tunnel in the background, but users can launch the application directly from their local Start Menu — with no need to open the Workspace portal first. Ideal for employees who prefer a native application feel.

DESKTOP INTEGRATION

NO INSTALL REQUIRED — FULLY AGENTLESS

Agentless Browser Access

Users access SPA applications directly from any standard browser — Edge, Chrome, or Safari — with no Workspace App installed. For unmanaged or BYOD devices, Citrix can automatically redirect the session to a Remote Browser Isolation (RBI) environment in the cloud, keeping all data secure even when no corporate controls exist on the local device. Suited for contractors, partners, and BYOD scenarios.

BYOD FRIENDLY

ACCESSING SPA APPLICATIONS

Delivery Method Comparison

Delivery Method	Workspace App Required?	Where the User Launches the App
Workspace Portal	Yes	Inside the Workspace App interface
Local Shortcuts	Yes (installed and signed in)	Local Start Menu or Desktop shortcut
Workspace Web	No	Any browser — Edge, Chrome, or Safari
Direct / Agentless Access	No	Bookmarks or specific application URLs

Why this matters for South African businesses: With hybrid work, BYOD, and contractor access now standard, organisations must secure corporate resources across a device landscape they no longer fully control. SPA's agentless access and continuous posture verification mean security does not depend on owning the device — only on verifying the user and controlling what they can do. OAS can advise on how

DeviceTrust and Chrome Enterprise complement SPA for deeper device context. [Read our DeviceTrust product page](/products/devicetrust).

HOW IT'S DELIVERED

Delivered as a Managed Service by OAS

Citrix SPA involves complex decisions around licensing models, network routing, device posture policy, and integration with DaaS. OAS handles the full engagement — from architecture to ongoing operations.

Architecture & Licensing Consultation

SPA licensing is nuanced — different tiers unlock different capabilities, and the right model depends on your user groups, device mix, and application portfolio. OAS guides you through the options to ensure you are correctly licensed without overspending.

EXPERT DESIGN

Policy Configuration & Device Posture

OAS configures your access policies, device posture rules, adaptive authentication flows, and app protection settings — ensuring that managed devices, BYOD devices, and contractor hardware each receive the correct level of access and the appropriate security controls from day one.

FULLY MANAGED

Monitoring & Access Reporting

OAS monitors your SPA environment continuously — tracking access events, posture check outcomes, and policy violations. Regular reports provide the audit trail needed for POPIA accountability, insurance requirements, and internal governance reviews.

POPIA READY

Incident Response & Escalation

When access issues arise — a policy misconfiguration, a posture check failing for an entire user group, or a suspected unauthorised access event — OAS responds, investigates, and resolves. Your users stay productive and your environment stays secure.

EXPERT SUPPORT

THE CITRIX SOLUTION SERIES

Citrix DaaS has long been the industry standard for securely delivering applications to end users. Citrix has kept pace with Zero Trust adoption through **Secure Private Access** — designed for organisations that need to extend controlled access to SaaS and internal web applications, across managed and unmanaged devices, without the complexity of a traditional VPN.

Citrix DaaS

Ready to Move Beyond the VPN?

Discover how Citrix Secure Private Access and Chrome Enterprise are redefining Zero Trust — not just at the point of access, but throughout the entire user session.

TELEPHONE

+27 11 485 3454

EMAIL

info@oas.co.za

WEB

https://www.oas.co.za

OFFICE

25 Durham Street, Raedene Estate, Johannesburg

Request a demo: https://www.oas.co.za/contact/demo

Open Architecture Systems — Protect. Detect. Recover. Citrix Platinum Partner since 1987.