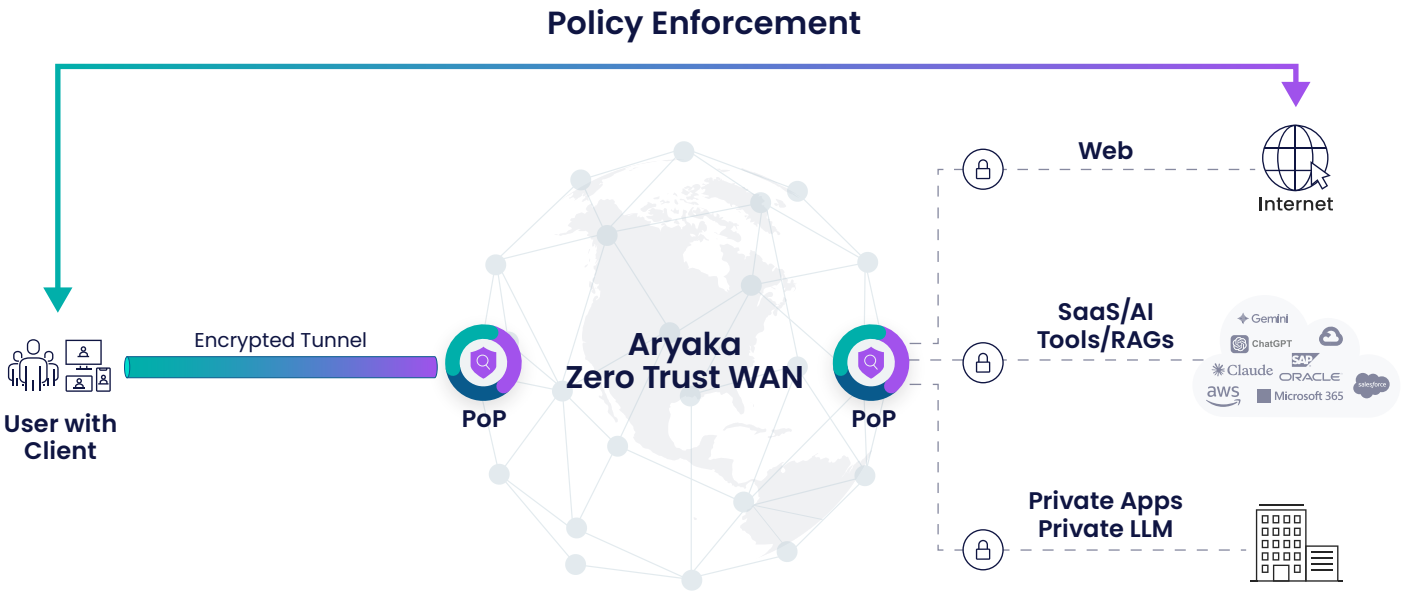
Aryaka Universal ZTNA

The modern workforce is increasingly hybrid, with employees accessing cloud and on-premises applications from diverse locations and devices. Traditional perimeter-based security can't keep up, leaving organizations exposed to unauthorized access, lateral movement, and data leaks. IT teams also struggle to maintain consistent policy enforcement and visibility across all users and networks while ensuring reliable performance.

Tackling Secure Network Access with Aryaka Universal ZTNA

Aryaka extends its Unified SASE platform to the hybrid workforce with an integrated, lightweight Zero Trust Network Access (ZTNA) client integrated into Aryaka Unified SASE as a Service. The client, powered by Cloudbrink, establishes identity and posture-verified sessions to Aryaka's Zero Trust WAN, where our OnePASS Architecture delivers consistent protection and low-latency performance for SaaS, IaaS, and private applications. Customers gain rapid time-to-value through instant zero-trust access, continuous device posture enforcement, and a unified policy framework already protecting branch and data-center traffic-resulting in a Universal ZTNA service that pairs best-in-class user experience with enterprise-grade security.



- **Performance Layer** – Mitigates packet loss, normalizes jitter, and compresses flows to deliver up to 30× faster application response.
- **Security Layer** – Aryaka's Unified SASE as a Service applies uniform policy regardless of access path, in addition to continuous device posture enforcement.
- **Control Layer** – MyAryaka remains the primary console. The addition of SSO provides seamless access to rich session analytics and control.

Use Cases

VPN Replacement for the Hybrid Workforce	■ **What:** The ZTNA App steers traffic to the nearest Aryaka PoP where Unified SASE as-a-service applies single-pass security. ■ **Why:** Centralized, cloud-delivered policy for remote and branch users—no new appliances, no hair-pinning, same controls everywhere. ■ **Outcome:** Faster connects, reduced lateral movement vs. full-tunnel VPN, continuous device posture enforcement and consistent enforcement/logging from the SASE services.
High-Performance Access to SaaS & Private Apps	■ **What:** Users anchor to the optimal traffic path; sessions are aggregated into the nearest Aryaka PoP to ride Aryaka's private core to SaaS/IaaS/private apps, while Unified SASE as-a-service provides SWG/NGFW/IPS/CASB/DLP(future) in one pass. ■ **Why:** Global PoPs and a private backbone deliver predictable latency and loss/jitter mitigation—with security inline, not bolted on. ■ **Outcome:** Smoother video/voice and faster app response without bypassing corporate policy.
Unified Visibility & Rapid Troubleshooting	■ **What:** End-to-end telemetry visibility and exports to SIEM from the Unified SASE as-a-service platform. ■ **Why:** One policy plane for remote and site traffic; changes in policy and monitoring take effect globally. ■ **Outcome:** Faster root-cause isolation, fewer escalations, and consistent reporting for compliance and operations.

Capability	Customer Value	Description
Ultra Low Latency On Ramp	**Office like performance for SaaS, data and file transfers, even over high loss home or public WiFi networks.**	The ZTNA Client automatically connects remote users to the closest edges that are typically less than 20 milliseconds away. Each edge maintains secured tunnels to the geographically nearest Aryaka PoP, minimizing latency.
Zero Trust Posture Enforcement	**Blocks unmanaged or risky devices at the edge and eliminates the "connect then check" loophole common in legacy VPNs.**	Before a session is established, ZTNA Client performs multifactor SAML authentication and verifies device health (OS patch level, EDR status, disk encryption, etc.). Only compliant devices receive a short-lived mutual TLS 1.3 certificate to continue.
Unified SASE Security	**Consistent policy and logging for all remote users, branch, and data center without duplicating rules or hardware.**	Traffic flows through Aryaka's OnePASS™ Architecture, which deliver Layer 7 firewalling, advanced web filtering, TLS inspection, IPS, CASB, etc. in a single transaction

Key Capabilities

Area	Feature	Description
		Aryaka Universal Zero Trust Network Access (ZTNA)
Performance	**Proximity**	A global mesh of PoPs ensures every user is “local” to the network. If traffic patterns shift, new network edges can be spun up in minutes without any customer action.
	Quality Index	Each session is scored in real time by combining latency, jitter, loss and throughput into a single number (BQI). Help desk agents can sort or alert on the BQI to find the noisiest problem users instantly.
Security	**Rotating Mutual TLS 1.3 Tunnels**	ZTNA Client issues short-lived certificates that rotate automatically, reducing the risk of credential theft and eliminating reliance on pre -shared keys.
	OnePASS™ Architecture	Aryaka inspects traffic once, applying URL filtering, DNS security, IPS signatures, anti malware scanning, application control and DLP (when available) evaluation in a unified process that adds negligible latency.
Management	**Unified Observability**	Performance (RTT, loss, BQI), security events (policy hits, IPS alerts) and asset data (client version, license status) are presented in a common UI through admin SSO.
	Named User Licensing	One subscription covers up to five devices per user, eliminating hidden egress or regional fees and simplifying budgeting.

Technical Specifications

Category	Details
Supported Endpoints	Windows 10/11, macOS 13+, iOS 15+, Android 11+. Linux is supported via command line client (beta).
Client Encryption	Mutual TLS 1.3 with 256 bit cipher suites, automatic certificate rotation every 24 hours (configurable).
Secured Tunnel	Static IPSec (SVTI) tunnel using IKEv2 and AES 256 GCM.

PoP Security Stack	NGFW, Secure Web Gateway, DNS Security, IPS, Anti Malware, CASB, DLP (when available) - all orchestrated in a single pass architecture.
Operational SLAs	Aryaka Zero Trust WAN: up to 99.999 % availability with <30 ms backbone latency across major regions.
Telemetry & Logging	Per session RTT, jitter, packet loss, throughput, BQI, application visibility, user ID, device posture, policy ID, SIEM export, etc.
Compliance Coverage	ZTNA App posture templates aligned with ISO 27001, PCI DSS, HIPAA, and GDPR requirements.

Licensing

ZTNA as a part of Aryaka Unified SASE as a Service utilizes per site licensing under three tiers of features and capabilities:

Tier 1 **Secure Remote Access**	Tier 2 **Essential Universal ZTNA**	Tier 3 **Advanced Universal ZTNA**
	Everything in Secure Remote Access, plus:	**Everything in Essential Universal ZTNA, plus:**
■ Remote access from anywhere ■ Zero trust ready client	■ Posture check ■ Security policy enforcement for Unified SASE	■ Security policy enforcement for Advanced Security ■ Clientless access option ■ Policy driven access selection

About Aryaka

Aryaka is the leader in delivering Unified SASE as a Service, a fully integrated solution combining networking, security, and observability. Built for the demands of Generative AI as well as today's multi-cloud hybrid world, Aryaka enables enterprises to transform their secure networking to deliver uncompromised performance, agility, simplicity, and security. Aryaka's flexible delivery options empower businesses to choose their preferred approach for implementation and management. Hundreds of global enterprises, including several in the Fortune 100, depend on Aryaka for their secure networking solutions. For more on Aryaka, please visit www.aryaka.com.

Schedule a Free Network Consultation with an Aryaka Expert

See How It Works Live

+1.888.692.7925 | info@aryaka.com