Universal ZTNA FAQ

1. What is “Universal” about Aryaka Universal ZTNA?

A: One policy model for all users, devices, and locations—HQ, branches, cloud, and remote—enforced through Aryaka’s global PoPs with per-app access, posture checks, and unified visibility.

2. How is it different from a traditional VPN?

A: VPN trusts the network and tunnels everything; ZTNA trusts identity + device + context and grants per-app access only. This reduces lateral movement, improves user experience, and simplifies policy.

3. Do we support both agent-based and clientless access?

A: Yes. Agent-based for any app/protocol and eventually, clientless for browser-accessible apps—both under the same policy and analytics.

4. What apps and protocols are supported?

A: Web (HTTP/S) and common client/server apps (e.g., RDP, SSH, DBs) via the agent; browser apps via clientless. (See “Details we’d like to confirm” for specific UDP lists.)

5. Which identity providers do we integrate with?

A: Standards-based SAML with major IdPs (e.g., Okta, Entra ID, etc.); we inherit MFA/SSO and can apply step-up based on risk/posture.

6. What device posture checks are available?

A: OS/platform, encryption, firewall status, certificate/trust, and other health signals to gate access before session start.

7. Can we segment access at a very granular level?

A: Yes—per-app micro-segmentation (FQDN/IP/port/path) with identity, group, device, and posture context. Policies are reusable across sites and users.

8. How does performance compare to VPN?

A: Users attach to the nearest Aryaka PoP; traffic rides Aryaka’s backbone with single-pass security—lower latency, fewer re-encryptions, and better SaaS/app responsiveness.

9. How does ZTNA interact with our SWG/NGFW/CASB/DLP?

A: It’s native to Aryaka Unified SASE: ZTNA grants per-app access, and traffic is inspected by SWG/NGFW/IPS with CASB and Next-Gen DLP for controls. This means one policy plane, one set of logs.

10. Can we handle unmanaged or BYOD devices?

A: Yes, eventually—with the future addition of clientless access combined with Next-Gen DLP controls for uploads/downloads, and we would require step-up auth for sensitive apps.

11. Does it work for contractors and third parties?

A: Yes—onboard external identities via the customer's IdP or a partner directory; restrict access to specific apps with time-bound policies.

12. How are DNS and private name resolution handled?

A: Connectors forward requests to customer-authoritative DNS; ZTNA resolves internal FQDNs per policy without exposing the private network.

13. What happens if a PoP or link fails?

A: Sessions fail over to the next best PoP; connectors are HA-capable; policies are cloud-hosted for rapid recovery.

14. Can we do split-tunneling per application?

A: Yes—per-app steering. Private apps traverse ZTNA; public/SaaS can go direct or through SWG, depending on policy.

15. How are threats like credential theft or token replay mitigated?

A: Short-lived, identity-bound sessions, posture re-checks, device certs, and continuous policy evaluation; risky posture triggers step-up or block.

16. Is traffic inspection encrypted end-to-end?

A: Yes—TLS to PoP, single-pass inspection within the platform (per policy), and encrypted onward to the destination or connector.

17. What telemetry and logs are available?

A: Per-user/per-app sessions, posture decisions, policy hits, and block/allow events. Export to SIEMs for correlation.

18. How does Universal ZTNA help with Shadow IT discovery?

A: Observability through Aryaka NGFW, CASB, SWG, and AI>Secure surfaces unsanctioned AI/tools and unknown destinations; with Universal ZTNA you can classify, allow with guardrails, or block and coach behaviors.

19. Can we enforce data controls (uploads/downloads) through ZTNA sessions?

A: Yes—tie Universal ZTNA to CASB/Next-Gen DLP to monitor/redact/block sensitive data in real time, including for AI/GenAI traffic.

20. What's the deployment model and time to value?

A: Cloud-delivered. Roll out the agent to users, drop connectors near apps, integrate IdP, and apply baseline policies—phased VPN co-exist/replace is common.

21. How is it packaged and licensed?

A: Three tiers:

• Tier 1 – Secure Remote Access: Secure remote access from anywhere + access to the Zero Trust client.

• Tier 2 – Essential Universal ZTNA: Everything in Secure Remote Access, plus device posture checks and security policy enforcement at the Unified SASE plan level.

• Tier 3 – Advanced Universal ZTNA: Everything in Essential Universal ZTNA, plus security policy enforcement at the Advanced Security plan level.

22. Does it support regulatory, and data-residency needs?

A: Policies/logs can be scoped by region, and traffic rides Aryaka's backbone with regional PoPs; confirm specific residency options per customer region.

23. What migration guidance do we give to replace VPNs?

A: Start with per-app access for high-value apps, onboard pilot users, enforce posture, then expand; keep VPN only for legacy edge cases until retired.