

ZERO TRUST ARCHITECTURE IMPLEMENTATION

Avalon assesses where your agency stands against the CISA Zero Trust Maturity Model or DoD Roadmap, designs the target architecture, and implements the identity, device, network, application, and data pillars.

THE PROBLEM WE ADDRESS

DoD components must reach Target Level zero trust — 91 activities across seven pillars — by September 30, 2027, and civilian agencies remain accountable to OMB M-22-09 for maturity reporting.

Most agencies bought identity, EDR, ZTNA, and segmentation tools in 2022–2025 but haven't finished the integration work that turns licenses into working zero trust — unintegrated licenses are sunk cost.

WHAT WE DO

- Pillar-by-pillar maturity scoring against CISA ZTMM v2.0 or the DoD Roadmap/NSA ZIGs
- Target zero trust reference architecture per NIST SP 800-207
- Segmentation model: macro-segmentation of enclaves, then micro-segmentation of key assets
- Identity: phishing-resistant MFA, conditional access, federation, PAM
- Devices: asset inventory reconciliation, device compliance policy, EDR signal integration
- Networks: macro/micro-segmentation, ZTNA replacing VPN, encrypted internal traffic
- Applications & data: SSO integration, workload identity, data discovery and DLP policy
- Functional testing of access policies and segmentation, then a maturity re-score

HOW WE DO IT

1 KICKOFF & BASELINE

Sponsor alignment, interviews, and pillar scoring against the CISA ZTMM or DoD Roadmap.

DELIVERABLE

Baseline maturity score

3 IMPLEMENTATION SPRINTS

Pillar-by-pillar deployment — identity first, then devices, then network segmentation.

DELIVERABLE

Pillars implemented, sprint by sprint

2 TARGET ARCHITECTURE

Reference architecture, segmentation model, and a phased investment plan produced and approved.

DELIVERABLE

Target architecture + roadmap

4 VALIDATION & CLOSEOUT

Access-policy and segmentation testing, a maturity re-score, and knowledge transfer.

HANDOVER

Evidence binder + trained staff

VALUE DELIVERED

- › **Dark capabilities lit up, not re-bought.** The first deliverable shows exactly which owned tools are unintegrated and what it takes to activate them.
- › **Legacy handled first, not last.** Identity-aware proxy patterns and monitor-only-mode testing bring legacy apps and flat networks in safely.
- › **Countable progress against a deadline.** Phased sprints map to the specific maturity activities each one completes.
- › **No product conflict of interest.** Avalon holds no resale relationship, so the architecture serves the agency's actual license reality.

COMMONLY PROCURED AS

Zero Trust architecture assessment & implementation services

AT A GLANCE

Model	Fixed-price or T&M, scoped per engagement
Typical	6–9 months through two implemented pillars
NAICS	541512, 541511, 541519, 541611, 541690
UEI	Y9MXMMHY3HA1
CAGE	242T0
Standards	NIST SP 800-207, CISA ZTMM v2.0, DoD ZT Capability Execution Roadmap, NSA ZT Guidelines

WHO WE WORK WITH

- Zero Trust PMO lead / ISSM sequencing pillars against a mandate deadline
- CIO/CISO staff needing to activate already-purchased ZT tooling
- System owner with a flat network or legacy app blocking segmentation

COMMITMENT TO QUALITY

Avalon is led directly by a PMP-certified founder with a decade of enterprise engineering experience where every engagement gets senior-level attention, never a subcontracted bench. Delivery follows NIST SP 800-53, RMF, and FISMA, evidence-backed and control-mapped by design. ISO 9001/27001 is on the roadmap as the pipeline scales.

Status: Small business federal contractor based in Los Angeles, CA

NIST SP 800-207

CISA ZTMM V2.0

DOD ZT CAPABILITY EXECUTION ROADMAP

NSA ZT GUIDELINES

