SECURE

Zero Trust Architecture

BREACHES ARE INEVITABLE. DAMAGE ISN'T.

Breaches are inevitable, but escalation doesn't have to be. A well-designed Zero Trust Architecture delivers built-in containment by enforcing three core principles:

1. Explicit verification of users, devices, and workloads
2. Segmentation and isolation to limit lateral movement
3. Assume-breach controls at every layer

The core principle we enforce across all components: verify explicitly, grant least-privilege access, assume breach. Here's how ANM ensures your Zero Trust Architecture is customized from the start and built to last.

HOW ANM IS DIFFERENT

- We lead with discovery, not demos
- 30+ years of experience and 175+ engineers at you fingertips
- Customized workshops and assessments
- You get what's right for your organization, not what's easiest for us to sell

OUR APPROACH

Understanding Before Implementation

Understanding your environment is a prerequisite to designing effective architecture. Our upfront investment demonstrates a commitment to your success.

Our vendor-independent approach ensures technology recommendations align with your specific requirements, not our sales quotas.

TECHNOLOGY PARTNERS

ANM works with industry-leading providers, including:

- **Network Security:** Cisco Systems, HPE Aruba Networks, Palo Alto Networks
- **Micro-segmentation:** Illumio, Guardicore, Akamai, ColorTokens, Cisco Secure Workload
- And many others

Comprehensive Zero Trust Architecture Components

IDENTITY & ACCESS MANAGEMENT

Cyber-resilient IDP, SSO, MFA, PAM, IGA, ITDR, federation/syncing, device lifecycle management, workforce and consumer identities (CIAM).

- Cyber-resilient identity platforms: SSO, RBAC, MFA, PAM
- Identity governance and administration (IGA) for lifecycle management
- Federation for cross-domain authentication
- Identity threat detection and response (ITDR) for compromised credentials
- Machine identity management for APIs, service accounts, and AI agents

NETWORK & WORKLOAD SEGMENTATION

Network-based macro-segmentation for departments and IoT; agent-based micro-segmentation for applications across data centers and clouds.

- Network-based segmentation: Cisco ISE, Aruba ClearPass for VRFs and VLANs
- Agent-based micro-segmentation: Illumio, Guardicore, Akamai, ColorTokens, Cisco Secure Workload for workload-level policies
- SD-WAN deployment: software-defined perimeters and SASE architectures

DEVICES & ENDPOINTS

Continuous compliance monitoring, mobile device management (MDM), enrollment and lifecycle management, endpoint detection and response.

- Continuous compliance monitoring and enforcement
- MDM for remote workforces
- Device enrollment and lifecycle automation
- Behavioral monitoring for suspicious activity

SECURITY OPERATIONS (SECOPS)

SIEM, SOAR, XDR, attack surface management, centralized visibility and tooling.

- SIEM for centralized logging and correlation
- SOAR for automated response workflows
- XDR for unified threat detection across endpoints and networks
- Attack surface management to identify exposed assets
- AI-driven analytics for behavioral anomaly detection

MACHINE IDENTITIES

Controls for APIs, service accounts, and AI agents — the highest-risk identities because they operate at scale.

DATA PROTECTION

Policy enforcement ensuring authorized access under secure conditions with continuous monitoring.

- Policy enforcement for authorized access under secure conditions
- Integration with data classification and DLP tools

ANM's Zero Trust Engagement Models

Assessment & Workshop

We evaluate your:

- Existing security architecture against the NIST 800-207 framework
- Gaps across five Zero Trust pillars: Identity, Device, Network, Application, Data
- Current capabilities and integration points
- Use cases mapped to business outcomes

What you receive:

- Strategic plan with prescriptive steps
- High-level architecture design
- Phased roadmap with technology recommendations
- Insights into investments aligned to your Zero Trust goals

Investment: *You receive a roadmap whether you engage us for implementation or not.*

ARCHITECTURE DESIGN

We design an integrated Zero Trust system tailored to your infrastructure:

- Blueprint showing how segmentation, identity, and access controls work together
- Policy frameworks enforcing least-privilege access across all layers
- Integration architecture connecting existing tools with new capabilities
- Visibility and monitoring design for security operations teams

IMPLEMENTATION & CONSULTING

ANM provides hands-on expertise to deploy Zero Trust Architecture across every layer of your environment: identity and access management, security operations, endpoint and device security, data protection, and network security transformation.

- **Phase 1:** Remote access and external-facing applications — a secure perimeter for the distributed workforce.
- **Phase 2:** Campus networks and internal users — internal segmentation and access controls.
- **Phase 3:** Data center workloads and critical applications — micro-segmentation and containment architecture.
- **Ongoing adaptation:** Architecture reviews, policy refinement, technology updates, and monitoring that adapts to emerging threats.

Each phase delivers measurable risk reduction without forklift infrastructure upgrades or operational downtime.

Get Started

Ready to get started? Contact us today to schedule a consult with one of our security experts.

TALK TO AN EXPERT

info@anm.com anm.com (866) 527-8822