

IMPLEMENTING ZERO TRUST FOR AI-NATIVE NETWORKS



One AI enabled platform. One networking experience. One strategic partner.

gtt.net

WHY ZERO TRUST?

Enterprise networks look nothing like they did just a few years ago. AI now drives much of the infrastructure, layering sophistication and new attack surfaces into everyday processes. At the same time, growing vendor sprawl has blurred our sense of traditional perimeters. Are your security teams still defaulting to typical border defenses? If so, you're missing critical exposures that attackers are all too eager to take advantage of.

Enterprises are long overdue for a fundamental shift from an architecture built on trust to one that questions everything all the time. Zero trust offers a pragmatic path through this change. So here's a clear, decision-ready roadmap meant to clarify the process and put you in charge of your transition to zero trust in the age of AI-powered networks.

Zero Trust Defines AI-Native Networks

Breach after breach has shown that historic trust models are no longer up to snuff. Zero trust flips the old paradigm on its head: trust no user, device, application or workflow without constant verification. Assume risk sits on both sides of every access request.

Fortunately, AI makes implementing zero trust both effective and scalable. With automation and real-time analytics, AI can parse vast streams of traffic, catching the outliers and anomalies that signal trouble. Human teams simply can't keep pace. The following steps provide a model that lets you safeguard your assets without sacrificing agility.

STEP 1.

ASSESS YOUR CURRENT NETWORK AND SECURITY POSTURE

You can't defend what you can't truly see. The transition starts with a candid and comprehensive environment evaluation.

Conduct a Security Audit

Identify weak spots across your network landscape. This means assessing your access controls, detection tools and network segmentation. Pinpoint visibility gaps that could let in bad actors.

Map Your Network

List all users, devices, critical applications and data flows. Surface priority assets and spots where risk most often appears. Precise knowledge of how data moves within your organization is the only way to determine where defenses are needed most.

Define Your Zero Trust Goals

Sharpen your focus. Where will zero trust have real impact? Which operational spheres need improvement the most? Prioritize your needs (e.g. risk reduction, faster response, cost efficiency, etc.) and link them to business goals.

STEP 2.

ESTABLISH STRONG IDENTITY AND ACCESS MANAGEMENT

In zero trust, identity replaces the perimeter.

Access decisions should always hinge on solid, contextual validation.

Implement Multi-Factor Authentication

Mandate multi-factor authentication for every user and device. This is the baseline for robust assurance.

Adopt Role-Based Access Control

Don't allow permissions to creep beyond what is needed. Tie access strictly to roles and keep privileges lean. Nobody—including senior staff—should have more access than absolutely necessary.

Leverage AI for Identity Verification

Get AI-powered behavioral analytics involved. Let your systems learn user patterns and flag inconsistencies fast. Automate what you can while the machine learning spots anomalies before an intruder gains access.

STEP 3.

SEGMENT YOUR NETWORK WITH MICRO-SEGMENTATION

One flat network gives attackers room to roam.
Break it down instead.

What Is Micro-Segmentation?

Micro-segmentation splits your network into small, purpose-built enclaves. Access is tightly controlled for each segment.

Benefits of Micro-Segmentation

This isolation makes lateral movement difficult. Even if one segment is compromised, others remain intact. You preserve core assets by enforcing rules that match their real-world risk.

How to Implement Micro-Segmentation

Lean on AI to suggest segment boundaries, mapping them to real usage and risk. Network traffic shifts over time, so revisit your segments and adapt as your organization changes.

STEP 4.

ENABLE CONTINUOUS MONITORING AND THREAT DETECTION

Don't treat zero trust as a set-and-forget operation.
Always be vigilant.

Real-Time Monitoring

Bring in AI-driven monitoring that works 24/7/365. When anomalies appear, your tools need to alert you before harm is done. The GTT Envision platform was built just for this, giving you orchestration and control to act beyond mere observation.

Behavioral Analytics

Machine learning helps define what a "normal" context looks like for your users and devices. Any deviation triggers an immediate call for review and warranted action.

Incident Response Automation

Routine detection and triage can and should be automated. This helps remove slow chains of human approval with streamlined workflows that let your organization react to threats more immediately.

STEP 5.

BUILD A CULTURE OF ZERO TRUST

No technology change works in a vacuum. How your people engage with zero trust often determines success (or failure).

Educate Your Team

Employ concrete training requirements. Explain how and why controls are shifting, and connect these changes to specific business goals.

Collaborate Across Departments

Bring in voices from IT, security and all relevant business units. Good policy reflects operational realities, not just best practices. Security should support outcomes, not become a bottleneck.

Establish Governance and Accountability

Assign responsibility for zero trust execution and maintenance. Review policies regularly and adjust as threats evolve.

Overcoming Common Challenges

Every transition is going to hit obstacles. Planning for them early pays off.

Resistance to Change

Expect apprehension about disruption or complexity. Focus on the measurable, long-term upsides: stronger security, streamlined operations and improved business continuity.

Integration With Legacy Systems

Many organizations rely on technology that was not built with zero trust in mind. Take a phased approach to avoid interruption.

Cost and Resource Constraints

AI can handle repetitive tasks, reducing manual workloads. Choose your strategic partners carefully; insist on expertise and real commitment to supporting your team and objectives.

The Path to a Secure Future

Zero trust is essential if you want resilience and security that scales for the future. Every step you take now is foundational for confidently meeting tomorrow's threats and taking advantage of coinciding opportunities.

ZERO TRUST

APPENDIX: ***CHECKLIST FOR*** ***ZERO-TRUST*** ***IMPLEMENTATION***

Use this checklist to track your progress and ensure a systematic rollout.

- Audit current network vulnerabilities and controls
- Inventory users, devices, applications and data flows
- Define zero trust goals tied to outcomes
- Require multi-factor authentication everywhere possible
- Restrict access using role-based and least privilege policies
- Apply AI behavioral analytics to identity verification
- Segment critical assets with micro-segmentation
- Enable continuous monitoring, not periodic checks
- Automate incident response wherever feasible
- Train staff in zero trust best practices
- Establish clear, cross-functional governance