DoD ZT Mission Connectivity

Identity-First Reachability™ for Mission Systems, OT, Cloud, Edge, Partners and AI Workflows

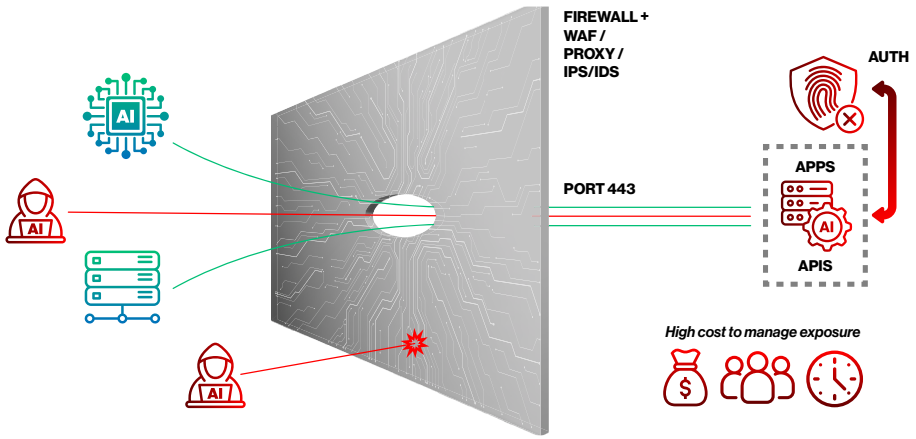
DoD Zero Trust Is Hard to Execute Across Mission Environments

DoD teams are under active pressure to implement Zero Trust across users, workloads, mission systems, OT environments, partners, cloud resources, AI workflows and tactical-edge services. **NIST SP 800-207, the DoD Zero Trust Strategy, RMF/ATO expectations and CMMC are making this a mission and compliance priority.**

But execution is hard across distributed environments and networks you do not fully own or control. Traditional approaches still require VPN setup, firewall rules, NAT, routing, approvals, accreditation friction and troubleshooting every time a new service, partner, device, identity or mission environment needs to connect.

Traditional Network Access Cannot Deliver Mission-Scale Zero Trust

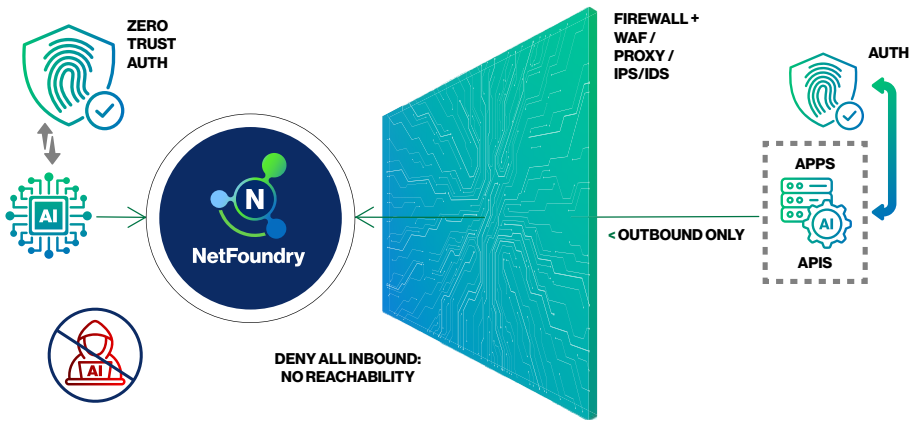
Legacy connectivity tools were built for a simpler world. They depend on exposed infrastructure, inbound firewall ports, IP-based reachability and repeated underlay changes. That makes it difficult to enforce least-privilege, service-specific Zero Trust across every user, workload, partner, OT system, cloud resource or edge site.



Downstream, this creates a recurring ***connectivity tax***: slower mission fielding, larger attack surface, lateral movement risk, accreditation drag and limited visibility across distributed environments. **None of that is acceptable when mission tempo demands speed and security in equal measure.**

NetFoundry's Identity-First Reachability™

Instead of connecting first and authenticating second, NetFoundry flips the traditional model. **Nothing is reachable until identity is verified, full stop.** Services stay dark by default: invisible, unscannable and unexploitable until an authorized identity requests access.



Outbound-only connections, cryptographic identity, centralized policy governance and least-privilege service reachability mean your teams can securely connect users, workloads, APIs, AI agents, OT systems, mission systems, partners, cloud, edge and tactical environments...**all without touching the underlay every time something new needs to connect.**

99.99%
Reduction in external attack surface

20 Days
Interim ATO vs. 45-day previous fastest

3,000+
Organizations securing workloads with NetFoundry

Mission Teams Will Be Able To:

- Close inbound firewall ports
- Eliminate S2S VPN complexity
- Accelerate secure deployment / ATO
- Simplify compliance and RMF initiatives
- Reduce operational overhead
- Improve visibility and governance across distributed environments

Supports Initiatives Aligned With:

- NIST Zero Trust
- RMF/ATO
- CMMC
- CJIS
- IEC 62443
- NERC/CIP
- FIPS-ready environments
- SOC 2 Type II
- HIPAA
- HITRUST and NIS2

Secure APIs & AI Agents

APIs and AI services stay invisible until authenticated and authorized, making them unscannable and unexploitable.

Third-Party & Partner Connectivity

Give vendors, mission partners and coalition workflows identity-based least-privilege access.

Hybrid IT / OT Segmentation

One consistent connectivity model across enterprise IT, industrial OT, mission systems, edge, cloud and tactical environments.

Mission Systems & Tactical Edge

Secure access to mission apps, edge workloads and tactical platforms without broad network exposure or underlay changes.

Microsegmentation

Block lateral movement with policies defined by identity and service, not IP address.

Flexible Deployment

SaaS-managed or self-hosted, across cloud, on-premises, edge and tactical environments.
100+ PoPs globally.

Not a Replacement; an Extension

Standard ZTNA handles human user-to-app access well. NetFoundry handles everything ZTNA wasn't built for: non-human identities, machine-to-machine traffic, OT systems, AI agents and tactical-edge platforms. If you're already running Zscaler, SD-WAN, cloud networking or Morpheus, NetFoundry sits above that infrastructure as a secure connectivity layer, no underlay redesign needed while extending Zero Trust beyond standard ZTNA to:

- **Non-human identities:** workloads, APIs, containers, AI agents, sensors and devices
- **OT and mission systems:** secure access without standing VPNs or broad network exposure
- **Tactical / DDIL environments:** deployable patterns for constrained or disconnected operations
- **Hybrid and multi-cloud:** service-level reachability and microsegmentation across any infrastructure
- **Mission partner / coalition access:** expose only authorized services, not whole networks

About NetFoundry

Founded by the inventors and maintainers of the world's most-used open source zero trust software, OpenZiti, NetFoundry helps agencies and enterprises secure connectivity between components of their widely distributed workloads, across any set of networks.