NetFoundry

Company Overview

Securing Machine & AI Workloads With Identity-First Reachability™

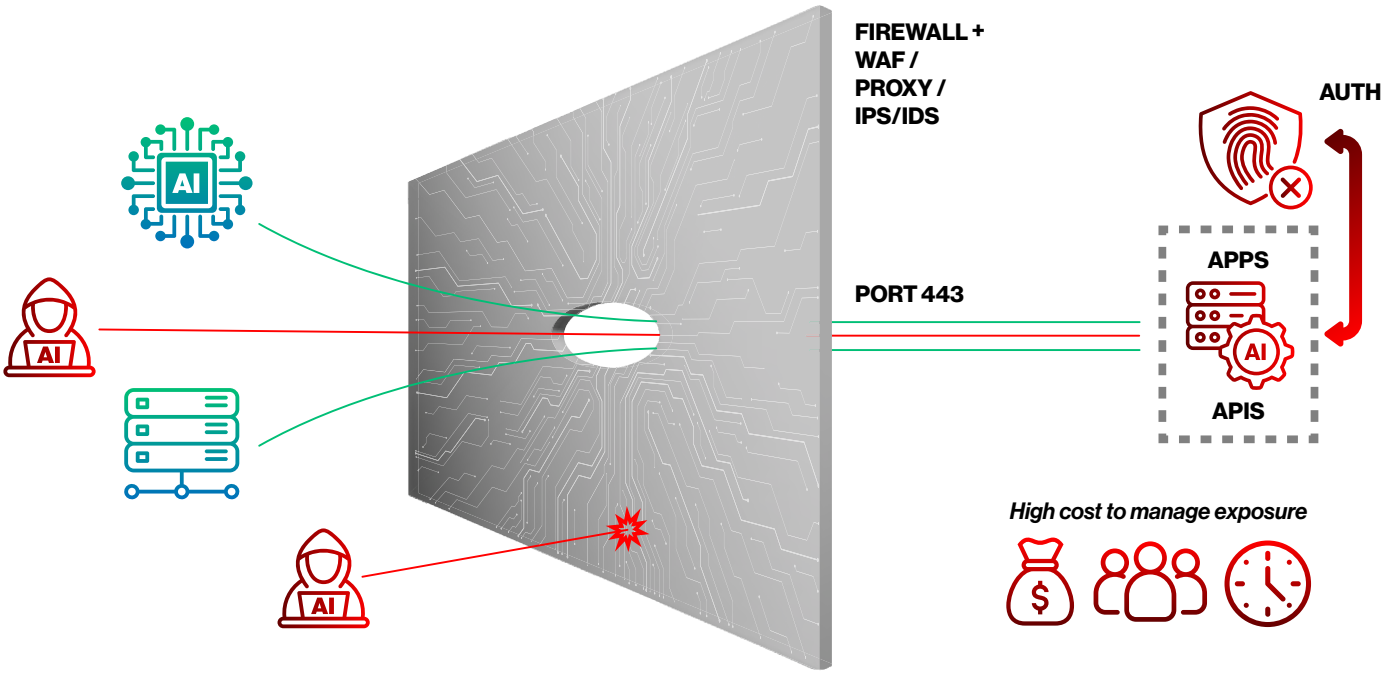
Exploitation Timelines Have Collapsed

Attackers now exploit vulnerabilities faster than organizations can respond. APIs, machine traffic, and AI-driven workloads are rapidly expanding enterprise attack surfaces, while traditional security architectures were never designed for machine-scale connectivity.

Protecting Exposed Infrastructure Is No Longer Viable

Traditional connectivity relies on exposed infrastructure, including inbound firewall ports, VPNs, IP-based trust, and shared credentials. **This creates reachability before authentication, allowing attackers to discover, scan, and exploit workloads.**

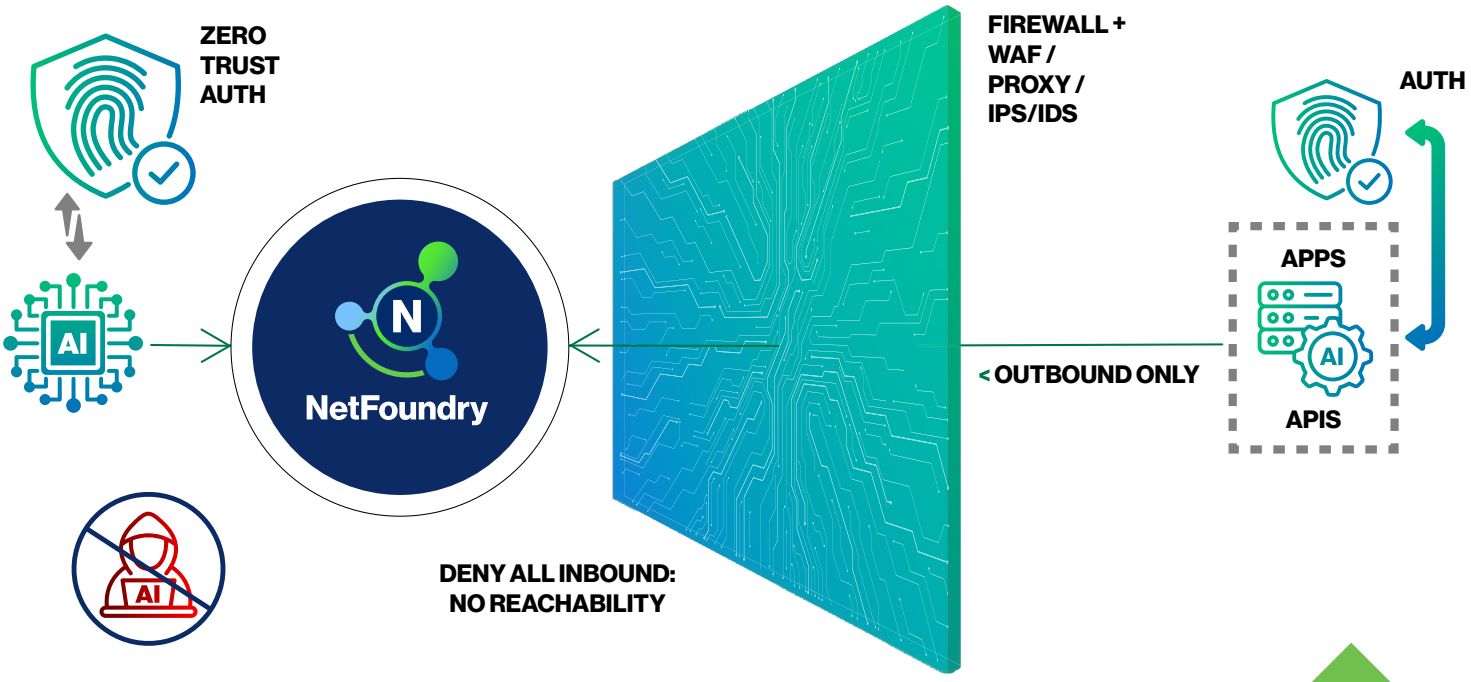
The result is a larger attack surface, greater lateral movement risk, constant operational overhead, and limited visibility across distributed environments. **Malicious actors now only need one reachable path.**



NetFoundry's Identity-First Reachability™

NetFoundry applies zero trust directly at the connectivity layer, enabling authenticate-to-connect networking where workloads remain unreachable until identity is verified. Outbound-only connections, identity-based access, and centralized policy governance eliminate exposed infrastructure while enforcing least-privilege connectivity across APIs, AI agents, OT systems, and distributed workloads.

This approach reduces external attack surface by up to 99.99%, prevents workload discovery and scanning, eliminates VPN exposure, and blocks lateral movement.



Flexible Deployment Options

NetFoundry supports SaaS-managed and self-hosted deployments to meet enterprise operational, compliance, and hosting requirements. Organizations can deploy within their own infrastructure or leverage NetFoundry's globally managed overlay with enterprise-grade availability and support.

The Results

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

Common Use Cases

- **Secure APIs & AI Agents** - Make APIs and AI services invisible until authenticated and authorized.
- **Hybrid IT / OT Segmentation** - Simplify secure connectivity across enterprise, industrial, edge, and cloud environments.
- **Third-Party & Partner Connectivity** - Replace VPNs and open firewall ports with identity-based least privilege access.
- **Microsegmentation** - Prevent lateral movement without operationally complex network redesigns
- **Customer & Remote Deployments** - Accelerate deployments without firewall modifications or IP allowlisting.

About NetFoundry

NetFoundry helps businesses secure connectivity between components of their widely distributed workloads, across any set of networks. Founded by the inventors and maintainers of the world's most-used open source zero trust software, OpenZiti, NetFoundry's Identity-First Reachability™ enables zero trust connectivity with no VPNs, no open inbound ports, and no firewall changes.