NetFoundry

Secure Your Workloads with Identity-First Reachability™

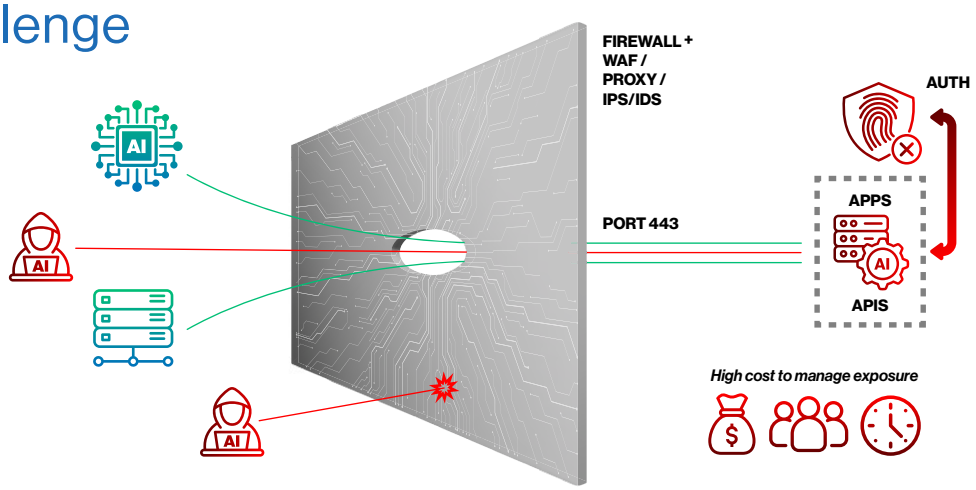
Accelerate Deployments and Eliminate Cyber Exposure

Distributed workloads, such as those that enable modern applications, industrial devices and AI Agents, are a headache for operations—and a dream for attackers. As enterprises deploy workloads across hybrid, multi-cloud, edge, OT, IoT, and partner environments, traditional IP-based networking introduces risk, complexity, and cost.

NetFoundry's Identity-First Reachability™ embeds zero trust directly into workloads, eliminating inbound attack surface, while accelerating deployments and reducing cyber exposure by up to **99.99%**.

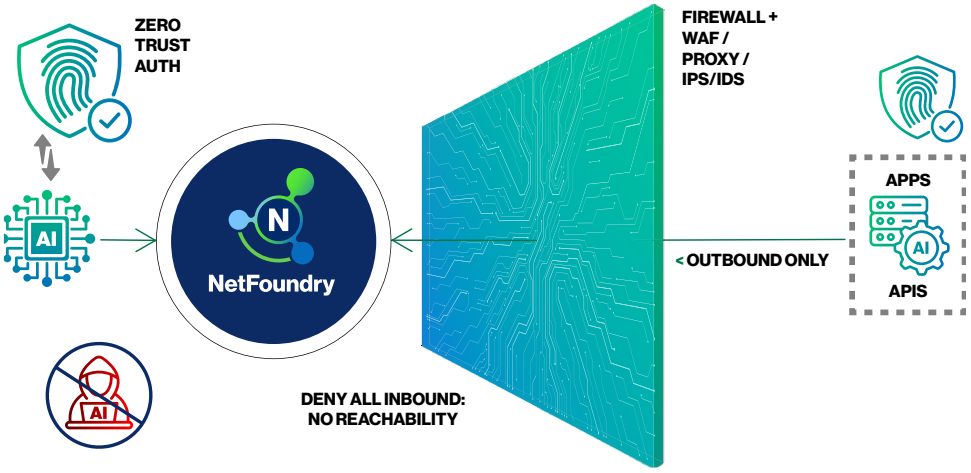
The Enterprise Challenge

Modern workloads are dynamic, distributed, and highly exposed. Firewalls, VPNs, and internet-facing APIs require constant updates, expand the attack surface, and grant excessive access. NAT, DNS, and IP abstraction further reduce visibility and control—increasing the risk of misconfiguration and lateral movement.



Our Solution

Identity-First Reachability™ replaces network-centric security with identity-based access. Private, zero trust overlays connect applications securely across any infrastructure—without exposing IP addresses or opening inbound firewall ports. Unlike traditional networking, which is built on a connect-to-authenticate architecture, NetFoundry makes it easy to deploy an authenticate-to-connect approach. Distributed sites and workloads connect without a VPN yet are hidden from the internet, unable to be scanned or attacked.



> *"NetFoundry helped us scale faster, safer, and more cost-effectively—eliminating VPN and NAT dependencies."*
>
> *—Rodrigo Bernardinelli, CEO, Digibee*

> *Our customers don't need to open a single inbound firewall port for us to manage our software."*
>
> *—John Wilson, CEO, TZ Limited*

Key Features	Benefits
Identity-based network access control	• Establish true least privilege access with ease • Control and audit access by identity and service, not IP Address
Outbound-only zero trust connectivity	• No VPNs to manage • No firewall rules to adjust • No connectivity until authenticated • No open inbound ports for attacker to discover
Connectivity by site, host, container or application (via API integration)	• Broad workload coverage, tunable to meet your security needs • Embed zero trust directly in your applications
Software-only, private network overlay, hosted by you or NetFoundry (100+ POPS)	• Quick deployments that meet your privacy and hosting requirements • High availability solutions

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. Software and IoT solution providers use it for secure communications with workloads at their customers' sites. Enterprises secure access to their APIs and agentic AI services in order to avoid any opening that can be leveraged by an attacker. They also use NetFoundry to simplify the operation of hybrid IT/OT segmentation and enable identity-based microsegmentation.

Common Use Cases

Simplifying Hybrid IT / OT Site Segmentation: Simplify and centralize management of secure connectivity across enterprise IT, OT, edge and cloud sites. No operational burden and misconfiguration risk of VPNs, private links, and constant firewall rule changes.

Securing Partner Connectivity: Replace VPNs and open firewall ports with identity- and service based connectivity that ensures least privilege access. Identity-based auditability of all 3rd party activity.

Accelerating Customer Deployments: Eliminate delays in customer evaluations and deployments. No need for customer IT teams to deploy VPNs, update firewall rules, and endure lengthy customer security reviews.

Locking down APIs & AI Agents: Reduce your internet-facing API attack surface by up to 99.99%. APIs are invisible until the connection is authorized, making them unscannable and unexploitable.

Microsegmentation: Block lateral movement through microsegmentation that's simple to deploy. Define policies by identity and service, not IP Address.