Customer Connect
Accelerate Secure Customer Deployments

Software and service providers increasingly need secure connectivity into customer IT, OT, IoT, and cloud environments—for application delivery, managed services, monitoring, support, and service-to-service communications. Yet traditional networking approaches introduce new operational activities and issues that slow deployments, extend security reviews, and delay revenue.

NetFoundry Customer Connect accelerates customer deployments by embedding Identity-First Reachability™ directly into provider platforms—allowing secure connectivity to customer environments in minutes, without requiring customers to open inbound firewall ports, deploy VPNs, or modify firewall rules.

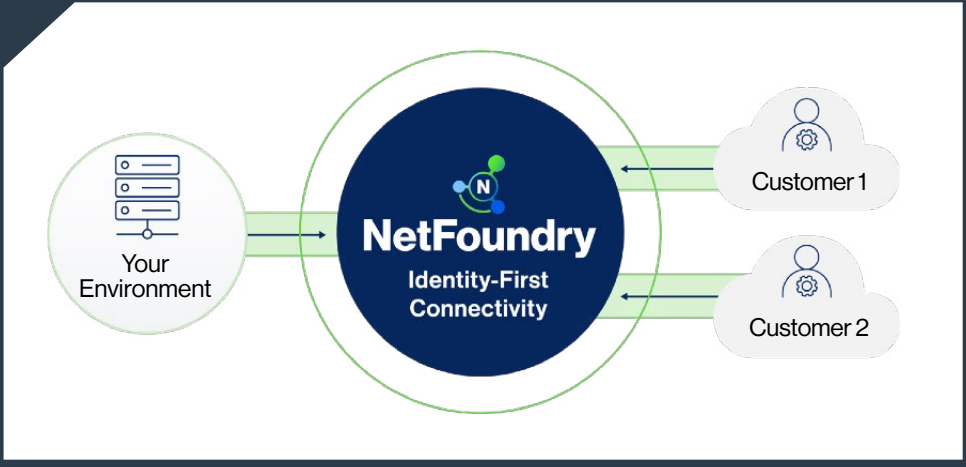
The Provider Challenge

Customer connectivity is a common—and costly—deployment bottlenecks for providers. Traditional approaches require providers to work with each customer to expose infrastructure to the internet, configure inbound firewall rules, manage VPN access, and maintain IP allowlists. These requirements trigger lengthy security reviews, increase operational overhead, and create excess access risk for customers and providers alike. Each deployment is different, and each one delays time-to-revenue.

The NetFoundry Customer Connect Solution

NetFoundry Customer Connect replaces network-centric connectivity with identity-based, Zero Trust access—designed for provider-to-customer environments. It establishes a private, software-defined network with customers.

- Authentication and authorization before connection
- All connections are outbound-only to NetFoundry routers
- No open inbound ports
- No VPN or firewall rule changes required



"Our customers don't need to open a single inbound firewall port for us to manage our software."

— John Wilson, CEO, TZ Limited

Key Benefits for Providers

Faster Customer Deployments - minutes instead of weeks or months

Shorter Sales Cycles - fewer security objections and simpler security reviews

Faster Revenue Recognition from accelerated deployments filter rather than a generic packet inspector.

Lower Operational Effort and Cost

Stronger Security Posture - zero trust access with no inbound attack surface

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

How Customer Connect Works

1. **Embed Connectivity** - Providers embed NetFoundry connectivity directly into their applications or deploy a lightweight connector that sits alongside the application.
2. **Deploy in Minutes** - Customer deployments are extremely simple, and don't require any firewall or network changes.
3. **Authenticate First, Then Connect** - Mutual authentication using X.509 identities establishes encrypted connections only between authorized endpoints.
4. **Enforce Least Privilege** - Access is defined by identity, workload, and service—not IP addresses or network location.
5. **Operate at Scale** - Providers centrally manage connectivity and access of each customer by identity, workload, and service. They have visibility across all customer environments.

Built to Support the Many Types of Provider Models

Customer Connect supports a wide range of provider use cases:

- SaaS platforms connecting to customer systems
- Managed service providers requiring operational access
- Industrial, OT, and IoT solution providers
- Hybrid and multi-cloud service delivery
- Human access and service-to-service communications

Connectivity works consistently across **on-prem, cloud, edge, OT, and IoT** environments—without network redesign.

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.