OVERVIEW

Identity-Defined Reachability™ for DoW Mission Systems

Aug 2026

NetFoundry

Developers of
OpenZiti
The leading open source
zero trust software

Problem: connectivity tax = mission change = network change

Fragmented workflows still depend on IP reachability, VPNs, firewall rules, NAT, routes, and enclave-specific approvals.

The operational pattern: mission access becomes network work

15–20
rules/policies across tools for one workload path

2+ weeks
to complete a connectivity change in a complex environment

20 vs 45
days to IATT in a tactical DoW deployment

Failure modes created

Reachability before authorization; exposed management and API surfaces; broad VPN trust zones; stale ACLs; service discovery and lateral movement risk.

Important nuance

Traditional control planes still matter for determinisitc latency, safety controls, and hardware isolation. NetFoundry targets mission reachability and authorization around those controls.

Mission effect

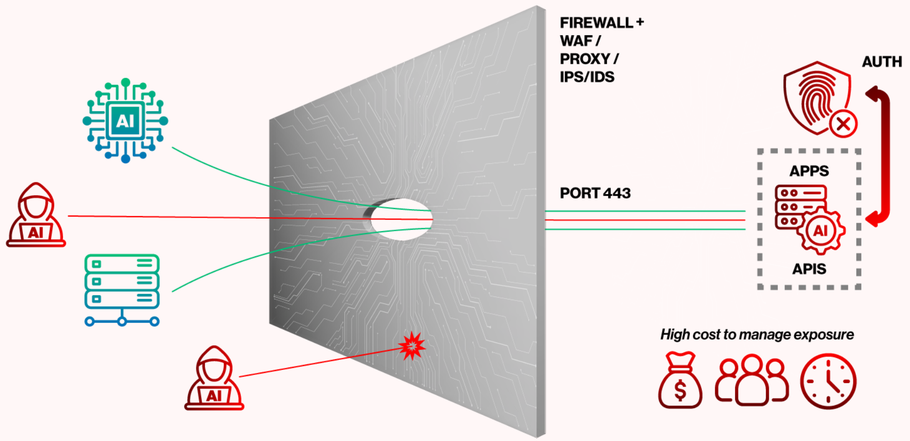
Every new mission path can become a network engineering, approval, and audit event — instead of a bounded identity and service-policy decision.

NetFoundry

Solution: no identity + no policy = no reachability

NetFoundry turns reachability from a topology decision into a cryptographic identity + service-policy decision.

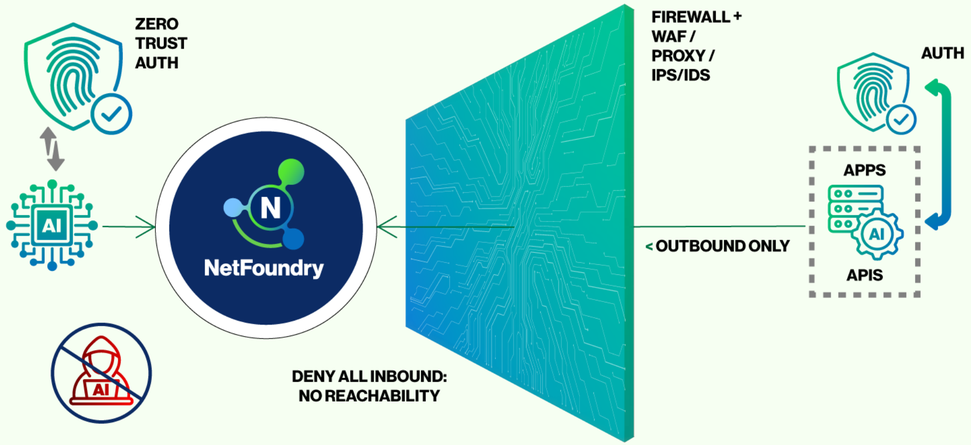
Connect-first



Routes, VPNs and ACLs create reachability before identity is enforced.

- Services can be discovered before authorization
- Broad network trust enables lateral movement
- Port, path, or location changes trigger underlay rework

Authorize-before-connect



X.509 identity and policy authorize a named service before any connection exists.

- No authorized identity = no route
- No matching policy = no session
- Port, path, or location changes become policy changes - not network changes

NetFoundry

Example: Mission outcomes already demonstrated

Quantified evidence, bounded dependencies, and explicit risk controls for mission deployment.

Recent tactical DoW distributed container platform

IATT achieved in **20 days**

Prior best **~45 days**

Primary mechanism: secured cross-enclave services without broad inbound exposure, new S2S VPN sprawl, repeated firewall/routing rework, or app-port-driven ATO churn.

Context: Distributed containerized platform spanning multiple network boundaries, enclaves, and data classification levels — supporting mission systems, human workflows, OT, drones, MPE, and machine-to-machine use cases.

1. Bounded dependencies

- IP transport over available bearers
- Lightweight connectors / routers
- Controller / policy plane
- X.509 identities + certificates
- Optional IdP, PKI, SIEM, IaC integrations
- No proprietary hardware required

2. Failure modes named

- Underlay loss or latency
- Router or control-plane outage
- Identity lifecycle failure
- Compromised identity or endpoint
- Policy error / excessive access
- OT safety / deterministic constraints

3. Risk strategy

- Self-hosted, HA, or air-gapped options
- Distributed routing + failover
- Cert rotation + least privilege
- Posture checks + continuous auth
- Audit logs by identity/service
- Preserve deterministic OT controls where required

Risk framing: NetFoundry does not remove identity governance — it makes identity governance the enforcement boundary for reachability.

NetFoundry

NetFoundry’s ‘Digital camouflage / dark services’

One common identity/governance model across cloud, edge, OT, AI, partner and mission systems

- AI agent or MCP
- API client
- OT, IoT or edge
- Third-party
- Site, VM, cluster

Identity-First Reachability™

- Authorization aware application fabric
- Just-in-time, continual authentication
- Mutual TLS and end-to-end encryption
- Smart routing
- Visibility, control, built-in audit
- Embeddable via SDK

SaaS, self-hosted, or hybrid

Deny-all inbound

Any workload target

1 Simple

No more firewall, VPN, IP management efforts or delays

2 Secure

All workloads are unreachable until authorized

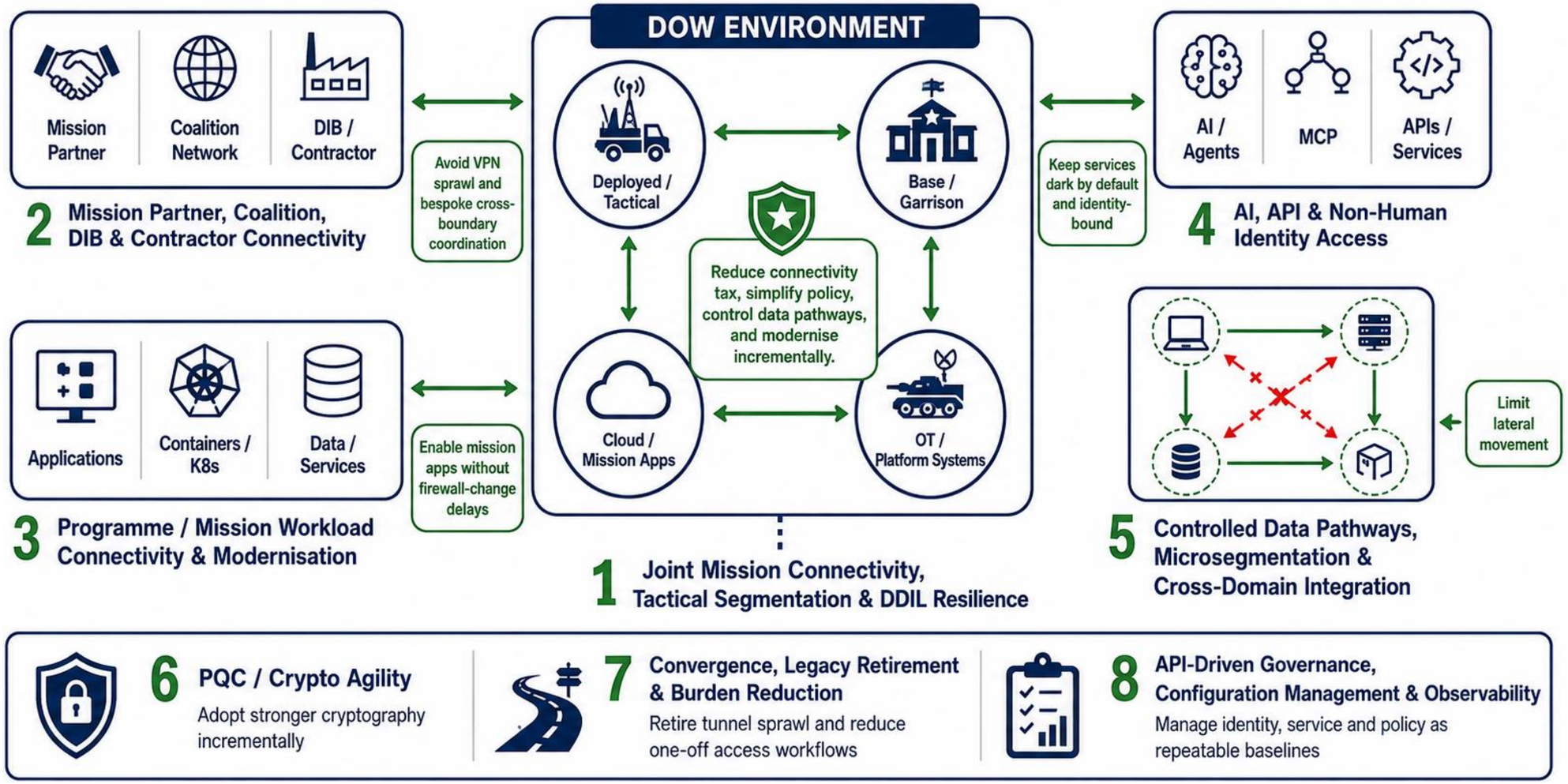
3 Scalable

Managed **any** workload with centralized policy and visibility

NetFoundry

DoW Use Cases for Identity-First Reachability™

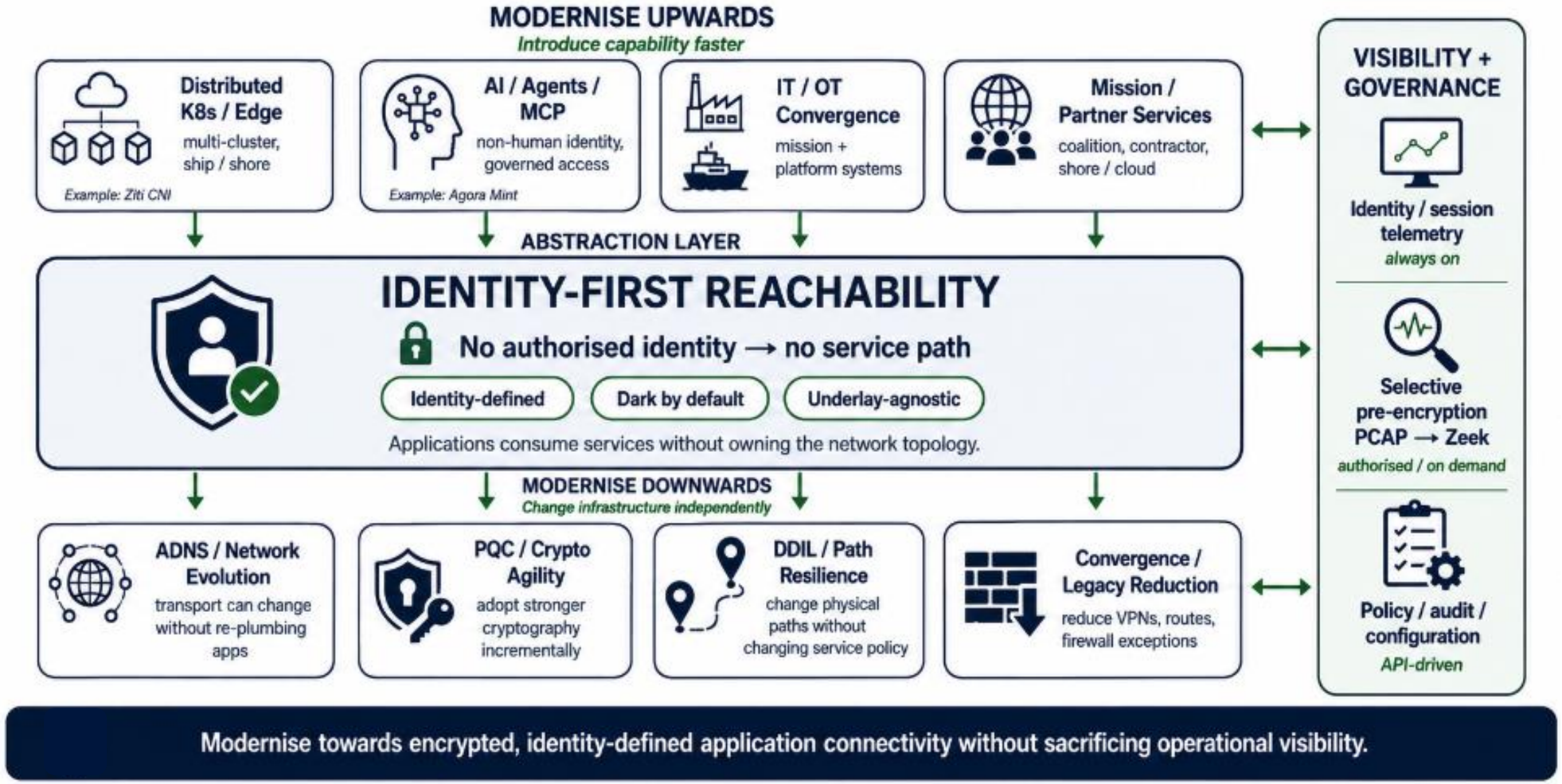
Reduce connectivity tax, simplify policy, control data pathways, and modernise incrementally



NetFoundry

DoW Modernisation Identity-First Reachability™ as abstraction

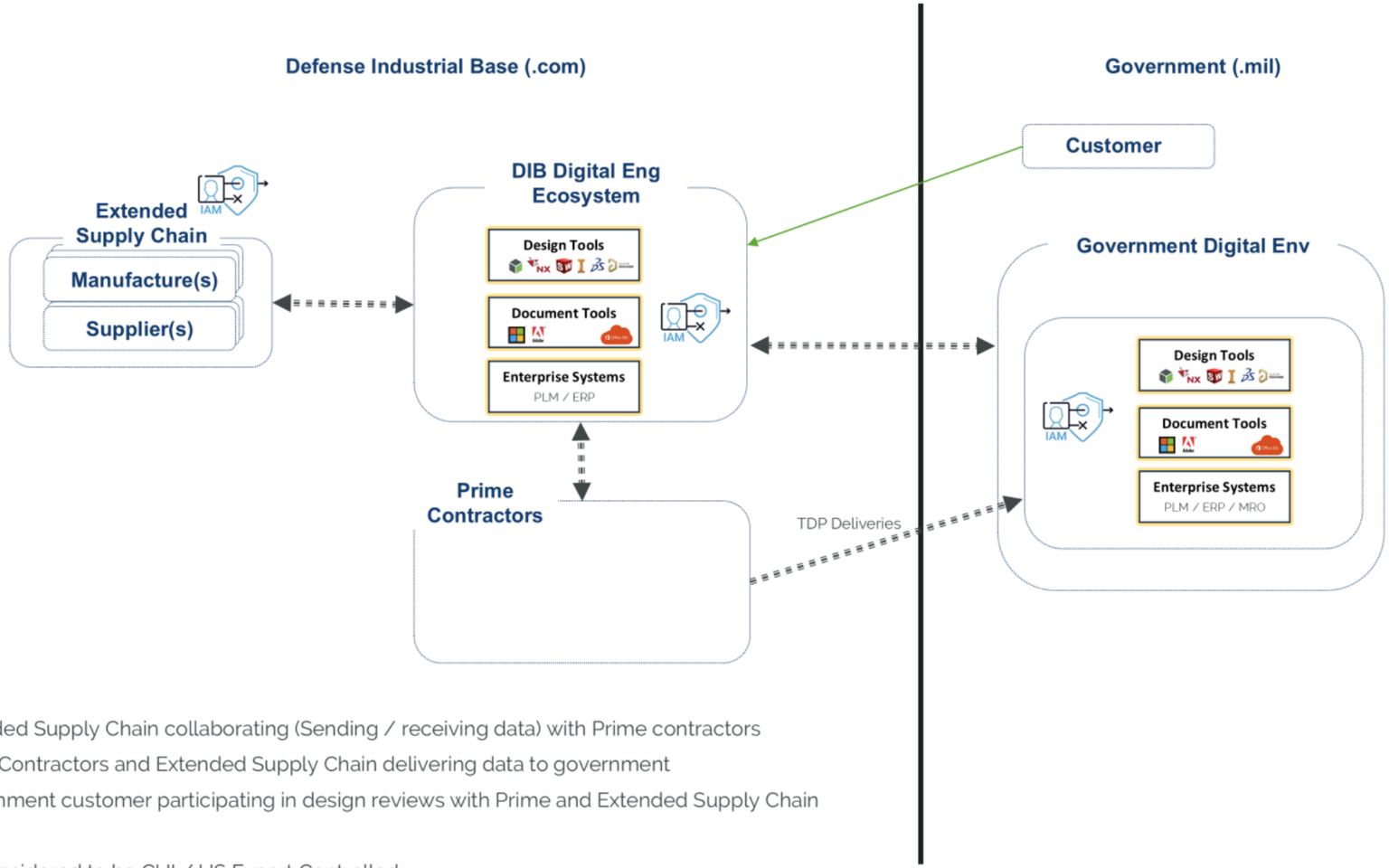
Decouple mission workloads from network topology so apps, platforms, security and transport can evolve independently.



NetFoundry

DIB Digital Engineering Ecosystem

Controlled CUI/ITAR service flows across independently managed supplier, prime and government environments without consolidating the networks



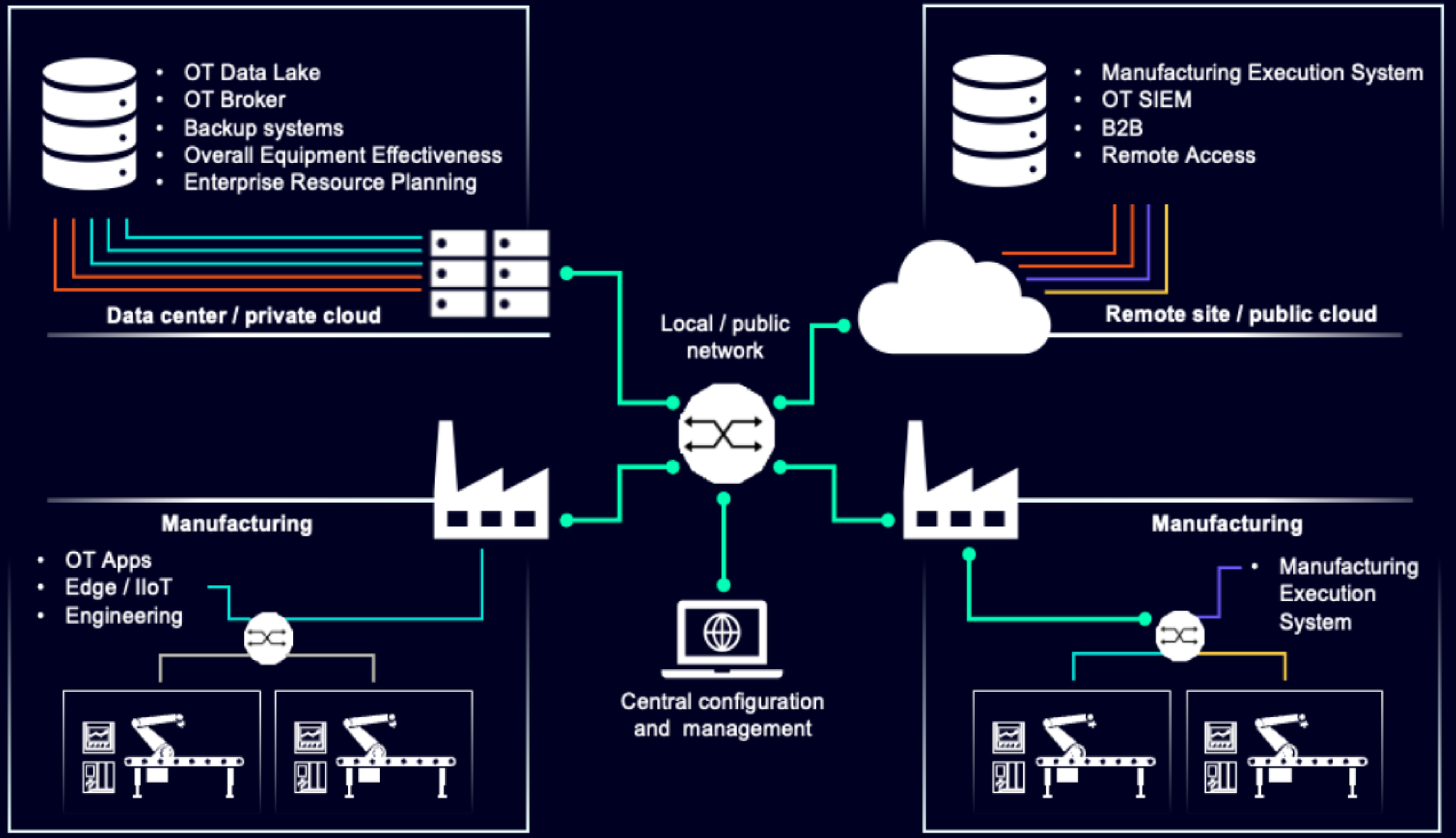
Use Cases:

1. Extended Supply Chain collaborating (Sending / receiving data) with Prime contractors
2. Prime Contractors and Extended Supply Chain delivering data to government
3. Government customer participating in design reviews with Prime and Extended Supply Chain

*All data considered to be CUI / US Export Controlled

NetFoundry

Overlay networks and zero trust communication
System overview and target design



Key take aways and main benefits

Scalable and **flexible** communication based on **overlay network**

Separated control and data plane offer **flexible deployment** options

Embedded zero trust principles and identities **increase cybersecurity**

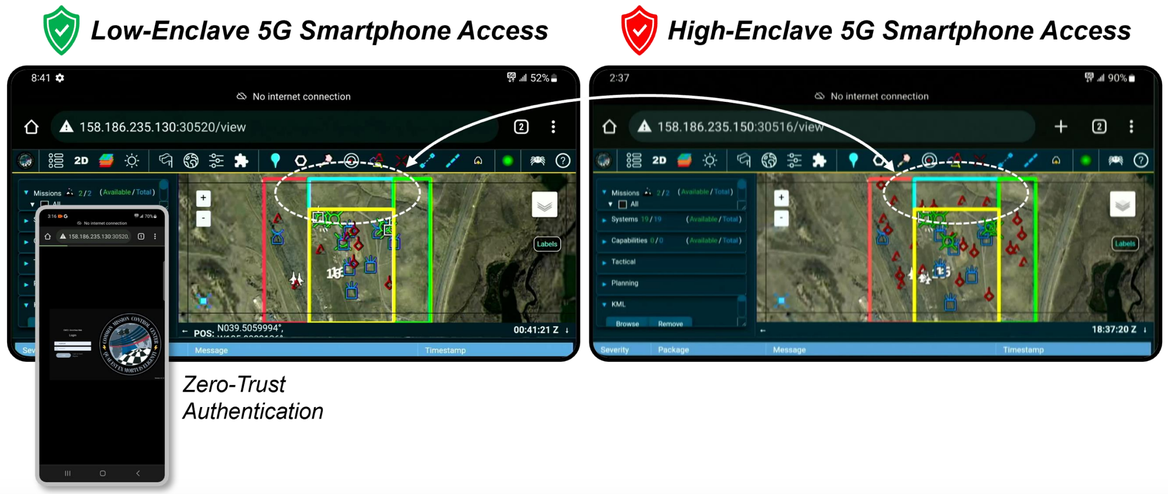
= data communication

= shared data streams (outbound only)

SIEMENS

Top U.S. military contractor

Deployment pattern / mission case study



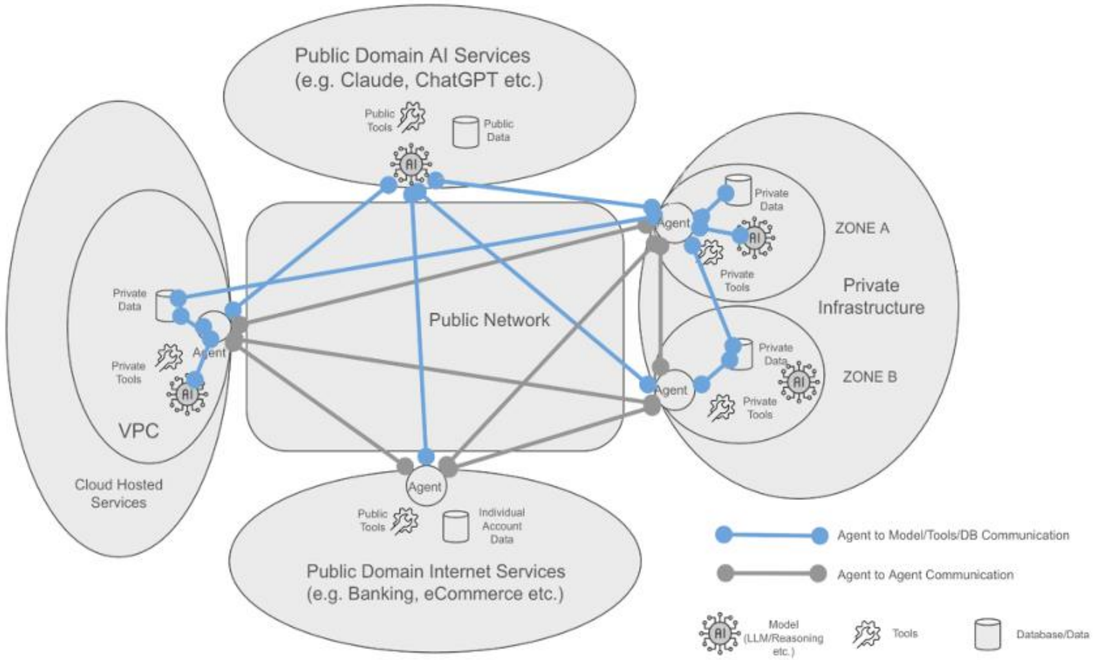
"the best adherence to NIST 800-207, including micro-segmentation and E2E encryption… with a breadth of architectures so we can run on anything. It includes its own CA/PKI to start without doing expensive integrations with ability to provide their own CA."

Technical Fellow

- **Desire business outcomes:** Provide secure, authenticated, encrypted access across warfighting domains with different security levels over a tactical 5G network.
- **Challenges:** (1) Guaranteed info segmentation (high-medium-low), (2) low SWaP-C tactical (mobiles, drones, etc), (3) DDIL & resilient system, (4) air gapped.
- **Solution**: ZTA Overlay embedded into cutting-edge commercial 5G with advanced defence tech, and for supporting many use cases, built on OSS.

Agentic is inherent cross-domain– identity must govern reachability

Agents, models, tools, APIs, and data move across enclaves, cloud, edge, SaaS, and partners



A2A and agent-to-tool flows routinely cross multiple trust and control domains

If those paths are already reachable, compromise can move from agent → tool → data → action

1. Identity attestation	2. Identity-defined reachability	3. Tool authorisation	4. Autonomy governance
Every agent proves who it is before traffic flows	No path exists unless policy explicitly creates it	Agents only see and use tools within policy scope	High-risk actions require stronger control or human approval

NetFoundry primarily enables Layers 1–2 and provides the governed connectivity foundation for Layers 3–4.

Identity is foundational — governance is the destination

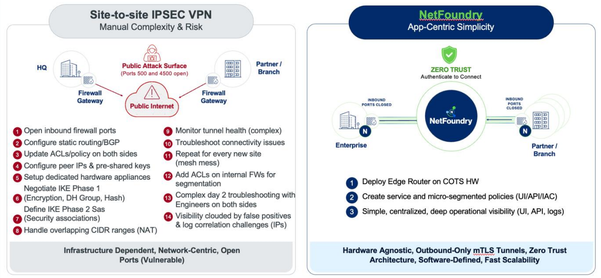
NetFoundry

Where NetFoundry fits

Beyond VPNs, cloud-only ZTNA, and topology-bound segmentation

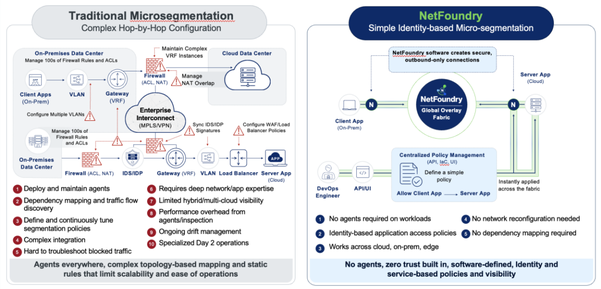
Common comparison assets

Operational Comparison: S2S VPNs



S2S VPN complexity

Operational Comparison: Internal Microsegmentation



Host / network microsegmentation complexity

Alternative	Where it helps	Why less desirable for this mission pattern
VPN / private links / firewall ACLs	Mature, familiar, and useful for some enclave designs.	Topology-bound; creates broad reachability before fine-grained authorization; rule, tunnel, and NAT sprawl.
Cloud ZTNA / SSE	Strong for human user-to-web or SaaS access.	Often assumes stable connectivity, cloud brokering, and browser/user patterns; weaker for DDIL, OT, and machine workflows.
Host microseg / SDN	Useful inside controlled enterprise workload estates.	Harder across unmanaged OT, partners, tactical nodes, air-gapped environments, and non-human identities.
Service mesh	Strong inside Kubernetes or application stacks.	Does not solve cross-domain, endpoint, partner, OT, or WAN reachability by itself.
NetFoundry	Identity-first reachability for users, workloads, APIs, services, devices, and agents.	Authenticate-before-connect across human and non-human identities, cloud, tactical, OT, and partner environments; no inbound exposure; software-only; SaaS, hybrid, on-prem, and air-gapped.

Innovation Adoption Kit

How NetFoundry supports IAK outcomes through burden reduction, convergence, and structured divestment

Reduce

- Routing / NAT / firewall / VLAN / NSG change burden
- Cross-team coordination for firewall, routing, and VPN changes
- Exposed services and IP-allowlist sprawl
- Repeated one-off connectivity tickets
- Repeated ATO / RMF friction tied to ports, rules, tunnels, and exposed services

Immediate operational burden reduction.

Converge

- E-W + N-S secure connectivity
- User, workload, site, & service access under one model
- Telemetry + policy evidence + selective inspection patterns
- Mission-specific consoles on the same API-driven platform
- Cross-boundary access as identity-to-service policy rather than enclave redesign

Immediate platform rationalization

Retire / shrink

- Recurring VPN / tunnel workflows
- One-off firewall / routing / access tickets
- Broad-network-access and connect-first patterns
- Exposed-service / inbound-listener patterns
- Parallel legacy access constructs across VPN, bastion, firewall exception, and ad hoc tunnels

Horizon 0 retirement potential

NetFoundry is not just identity-first Zero Trust networking; it enables measurable burden reduction, platform convergence, and structured divestment of redundant connectivity and security debt.

NetFoundry

Other DoW Activities

How NetFoundry is supporting the War Fighter

- **Tradewinds marketplace**: NetFoundry (and thus OpenZiti) is officially awardable. I think this is the correct link (though I am confirming). **6-26-2903 | NetFoundry Identity-First Reachability for Mission-Scale Zero Trust.**

- **Zero Trust Training:** We are working with the DoN CIO Zero Trust (and wider DoW ZT PfMO/WAU) to bring together a practical training on zero trust using open source across many use case and environments (NF/Ziti, Keycloak, Wazuh, Zeek). The first training will be delivered in the 1st week of September.

- **ZT Proving Ground:** We would participate in the DoW Zero Trust Proving Ground (led by MIT) to demonstrate, in a government-run scenario-based testbed, how NetFoundry/Ziti provides measurable additional Zero Trust security value through identity-first reachability, reduced lateral movement and lower connectivity complexity.

NetFoundry

Identity-First Reachability™

Reduce Operational Costs & Headaches
Simplify connectivity, centralize management, eliminate FW/VPN pain

Reduce Risk & Achieve Compliance
Apply zero trust for all connections, including non-human and external

Accelerate Business Enablement
Implement and scale without touching networks and firewalls

NetFoundry is SOC2 Type II compliant and helps customers achieve compliance goals such as FIPS, CRA, NIST, NIS2, IEC 62443, NERC/CIP, CJIS, HITRUST, HIPAA

Hydro Québec · MARK43 · Digibee · CERM · Microsoft · FREEWAVE · REDFAIRE · no-ip · TATA · OmniSYS a XIFIN® company

3000
companies use NetFoundry

2 of 5
of the largest US companies connect with NetFoundry

1 Billion+
sessions delivered per month

SIEMENS · Intrusion · RHAPSODY · KEO · LVT · CENTRALSQUARE · cerby · MARPOSS · lemongrass · tz

Developers and Maintainers of World Renowned OpenZiti Opensource Platform

NetFoundry