NetFoundry

WHITE PAPER

NetFoundry Zero Trust Overlay Strategy for DoD

Accelerating DTM-25-003 Outcomes with Identity-First, Authenticate-Before-Connect Networking

Learn more at www.netfoundry.io

Executive Summary

DoD components are under a clear mandate to achieve, at minimum, target-level Zero Trust across unclassified and classified systems (including national security systems) on the DoDIN by the end of FY2027, with priority of effort on NIPRNet and SIPRNet. Zero Trust principles must also be incorporated into weapon systems and the combined joint tactical environment, including denied, degraded, intermittent, and limited bandwidth (DDIL) operations.

The challenge is not a lack of security tools - it is the networking model. Traditional IP networking establishes connectivity first (routes, ports, VPNs, ACLs), then attempts to bolt on authorization and inspection. That approach creates network sprawl, slow cross-boundary segmentation, and an expanding attack surface - especially when applications span on-prem, cloud, tactical edge, and mission partners.

NetFoundry provides a fundamentally different approach: identity-first Zero Trust Connectivity Fabric that enforces authenticate-before-connect access to named services. It integrates with enterprise ICAM via BYO IdP (OIDC) and BYO PKI/CA, keeping trust anchors and credentialing under DoD control, and aligns strongly with NIST 800-207 - particularly for microsegmentation and end-to-end encryption. Instead of making networks broadly reachable and trying to constrain them with thousands of rules, NetFoundry makes services unreachable by default and creates connectivity only after identity, policy, and (optionally) device posture are verified.

This is the practical path to advanced Zero Trust networking: microsegmentation becomes a policy operation (identity > service) rather than a multi-week underlay change process (subnets > rules > change windows). A common operator observation captures the delta: ***"segmenting a workload from cloud to on-prem can require dozens of network/security changes and weeks of coordination - whereas an overlay can enable secure connectivity in seconds by updating identity-based policy."***

The highest-impact adoption path is not a network-wide rebuild, but targeted enablement of mission owners whose workflows span enclaves, classifications, installations, coalition partners, or contractor-operated systems. These teams experience the operational friction of traditional connectivity most acutely - VPN sprawl, firewall change queues, and cross-boundary delays. Identity-first, policy-defined connectivity allows these mission workflows to be secured and enabled quickly, creating measurable outcomes within 90 days and a repeatable path to scale.

NetFoundry is designed for mission conditions, combining multi-transport resilience and high availability with overlay-level performance features to sustain secure service access under load, latency, and link instability.

NetFoundry aligns strongly to DoD Zero Trust activities and capabilities across pillars, with particular strength in the Networks and Applications/Workloads pillars (the pillars that most often dictate schedule and operational risk). NetFoundry's model is also well-suited to both COA1 and 2 deployments because the fabric can be hosted and operated in DoD-controlled environments while spanning legacy networks without disruption.

1 DTM-25-003 and COA 1/2
What Must Be Achieved by FY2027

DTM-25-003 emphasizes rapid adoption and sustained implementation support to reach target-level Zero Trust by 2027, including technical assistance engagements, annual guidance to components, and incorporation of Zero Trust principles into a broad set of environments: enterprise DoDIN, classified systems, and weapon systems in the combined joint tactical environment.

Why COA matters for implementation velocity

The US DoD Capability Execution Roadmap (COA 1 and 2) approaches (DoD-controlled hosting and operations) demand solutions that can be deployed per use case, without requiring wholesale underlay redesign or risky changes to legacy applications. NetFoundry's service-specific overlay model supports incremental adoption: protect one service, one program, one enclave, or one mission workflow at a time - then scale.

2 Why Traditional Networking Struggles to Deliver Zero Trust

2.1 Connect-before-authenticate creates avoidable exposure - and accreditation drag

In traditional networking, reachability is established by IP routes and open ports. Security controls - firewalls, WAFs, proxies, identity gateways - are layered on afterward to constrain behavior. Even when well designed, this model leaves a wide discovery surface, where any error in routing, ACLs, or firewall policy can expose services. This is the opposite of Zero Trust's '*treat the network as compromised and hostile', as it allows any arbitrary endpoint from the network to try and exploit services.*

As shown in Figure 1, traditional networks expose a discovery surface because reachability exists before authorization. NetFoundry reverses the order: authorization happens first, and only then is a service-specific path created.

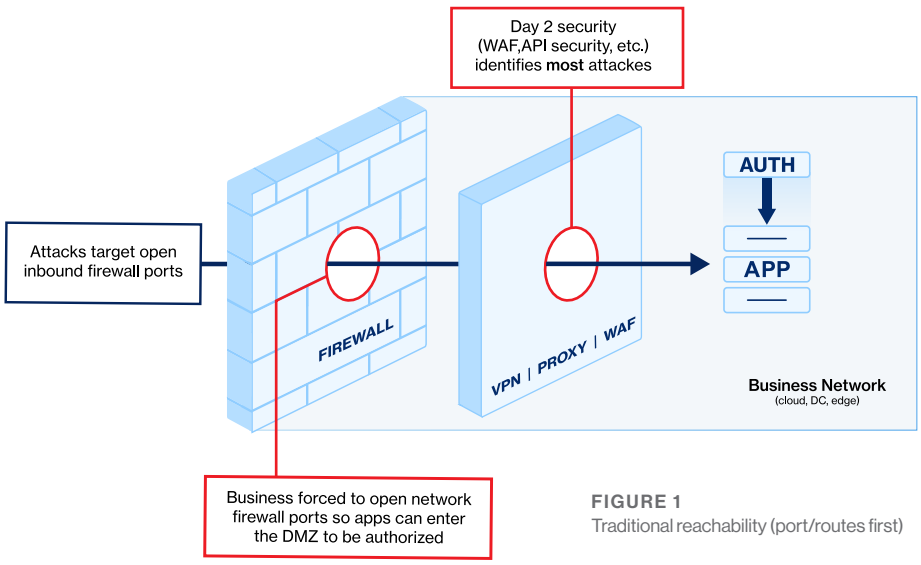

FIGURE 1
Traditional reachability (port/routes first)

In practice, this model also creates significant operational and accreditation friction.

A DoD application and mission leader described deploying containerized applications that needed to integrate with legacy systems. The container platform supported outbound HTTPS (port 443), but the legacy dependencies required nearly 30 additional ports and protocols. Each newly opened port required firewall changes and triggered an ATO update.

The outcome was predictable:

- Application delivery slowed by network and accreditation cycles
- Pressure to over-permit access "just to make it work"
- Expanded attack surface driven by integration needs rather than policy intent

This is a structural limitation of connect-before-authenticate networking. When access is defined by ports and protocols, Zero Trust becomes something layered onto the network - rather than enforced by it.

This outcome is fundamentally misaligned with Zero Trust's "assume breach" posture. Zero Trust requires that access decisions be made before connectivity exists, based on identity, policy, and context - not after the network has already been opened.

2.2 Cross-boundary microsegmentation becomes a ticket factory - especially in constrained and tactical environments

The most difficult segmentation problems are not intra-data-center. They are cross-boundary: cloud < > on-prem, enclave < > enclave, enterprise < > tactical edge, and partner < > DoDIN. Each boundary introduces different tooling, ownership, latency characteristics, and change processes. The result is network sprawl and brittle policy stacks that slow missions and make audit and rollback difficult.

These challenges are amplified in real DoD operating environments.

"VPNs take months to setup, add huge operational overhead, impact customer satisfaction and slows sales"

"We sometimes have 15-20 rules across multiple tools, firewalls, and other infrastructure to allow communication between workloads. It takes two weeks to make any change."

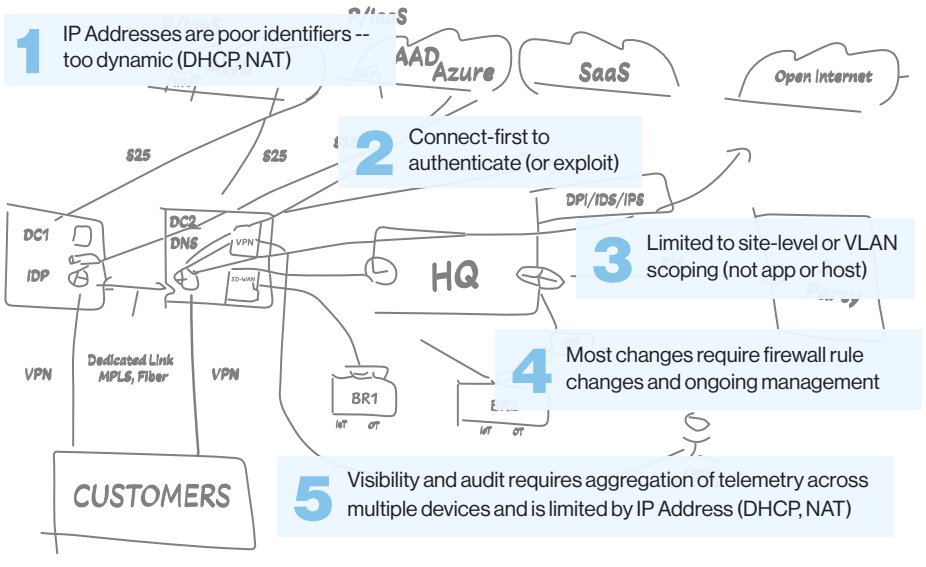

FIGURE 2

Mission owners routinely ask questions like:	Traditional networking assumes:
"We're deploying more drones and non-human systems."	Stable links
"Does this work on a Raspberry Pi?"	Human-driven workflows
"We have production networks that literally go underwater."	Stateful perimeter controls
"Our ships operate with inconsistent links and 500 ms round-trip latency."	Sufficient CPU and memory headroom

Modern DoD missions violate all of those assumptions. Segmentation strategies that depend on heavyweight agents, continuous inspection, or tightly coupled perimeter infrastructure break down in DDIL environments, on SWaP-C low-power devices, and across mobile or intermittently connected platforms.

In these conditions, every new integration becomes a bespoke engineering and accreditation exercise. Microsegmentation is no longer a security best practice - it becomes an operational bottleneck.

2.3 Proxy-based ZTNA does not replace the networking model

Proxy-based Zero Trust Network Access can be effective for specific user-to-application flows. However, it generally leaves the underlying IP reachability model intact. Networks remain routable, ports remain open, and segmentation is still enforced through layered controls and policy sprawl.

This creates three systemic gaps:

1. **It does not eliminate discovery surface:** Services may be "protected" by a proxy, but the network itself is still reachable and misconfigurations still matter.
2. **It struggles with non-human and east–west traffic:** Proxies are often optimized for user access, not machine-to-machine, workload-to-workload, or agentic systems operating across boundaries.
3. **It inherits the same scaling limits in constrained environments:** Proxy chokepoints, inspection overhead, and dependency on stable connectivity conflict with DDIL, maritime, and edge use cases.

As a result, Zero Trust programs can appear compliant in isolated scenarios while remaining blocked by the network pillar in practice. The core issue is unchanged: access is still fundamentally defined by network reachability first, with trust decisions applied later.

3 NetFoundry: Identity-First, Authenticate-Before-Connect Networking

3.1 The Core Idea

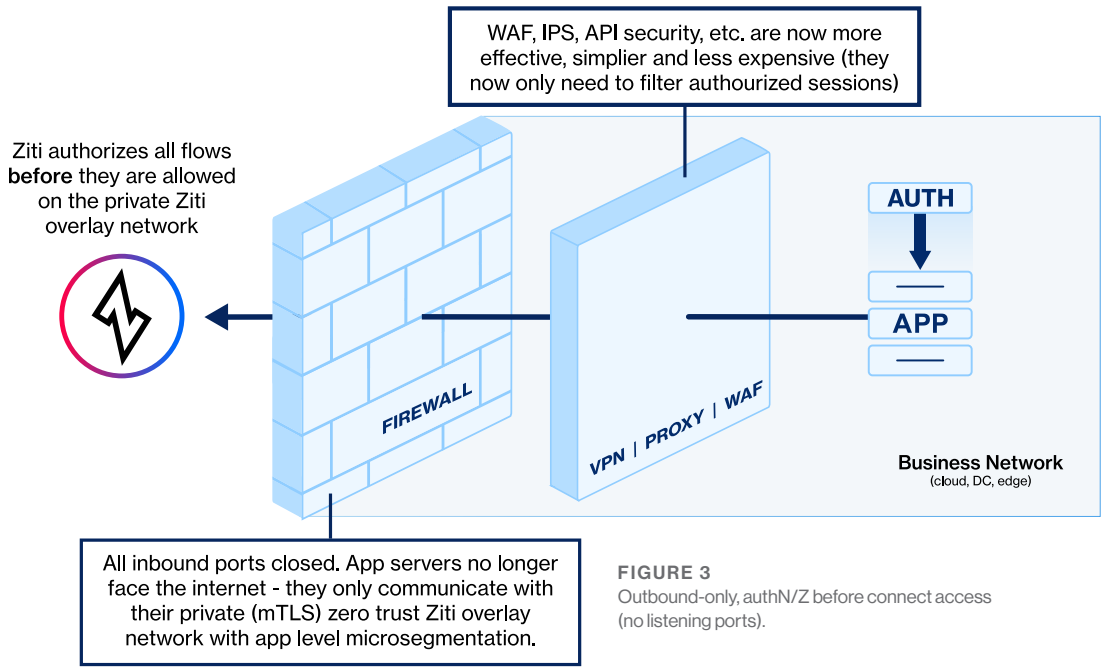

FIGURE 3
Outbound-only, authN/Z before connect access (no listening ports).

- Every workload, device, and user is represented by cryptographic identity.
- Policies bind identities to named services (not subnets to subnets).
- Connectivity is created only after authentication and authorization (authenticate-before-connect).
- Services can be ‘dark’ (not reachable or scannable) unless explicitly permitted.
- End-to-end encryption and per-session telemetry support oversight and audit.

3.2 What this enables that traditional networks struggle with

- Microsegmentation across any boundary (cloud, on-prem, edge, partner) using the same policy model.
- Rapid change: segmentation updates become policy changes, not underlay change requests.
- Reduced attack surface: fewer inbound ports and fewer discoverable services.
- Operational resilience: the overlay treats the underlay as transport and can use multiple transports.

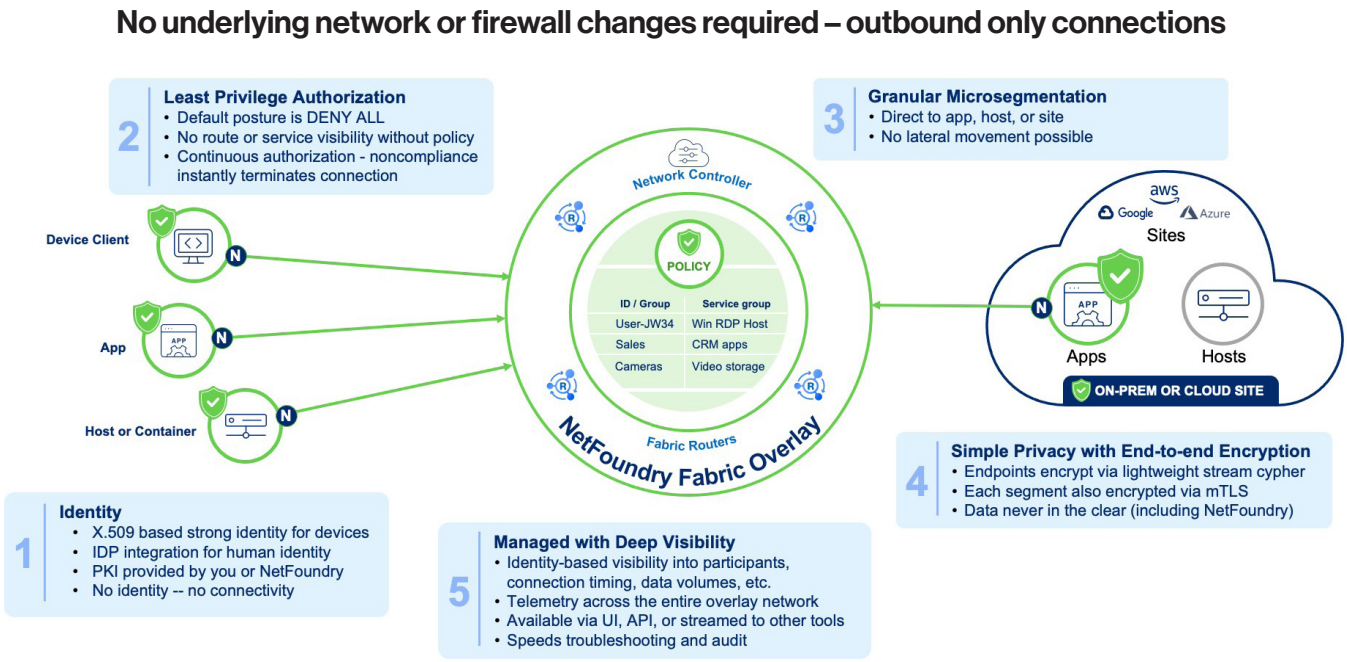

FIGURE 4
NetFoundry Identity-First Overlay Network - Sidestep the complexity of underlying networks

4 Mapping to DoD Zero Trust Activities and Capabilities

DoD Zero Trust implementation guidance emphasizes outcomes across seven pillars: **User, Device, Network & Environment, Application & Workload, Data, Automation & Orchestration, and Visibility & Analytics**. Together, these pillars define the capabilities required to reach **target-level Zero Trust by FY2027** across enterprise, tactical, and weapons-associated environments - including cross-boundary missions that span cloud, on-prem, edge, coalition/partner networks, and constrained links.

NetFoundry aligns to these pillars by applying an **identity-first, authenticate-before-connect** model that replaces broad "network access" with **service-specific access**. Practically, access is expressed as identity > named service > policy, rather than IP routes > open ports > firewall exceptions. This shift is most consequential in the pillars that typically drive schedule risk and operational complexity: **Network & Environment** and **Application & Workload**. Where traditional approaches require multi-domain rule stacks and repeated change windows, an identity-first overlay enables microsegmentation as a policy operation - repeatable across boundaries without redesigning the underlay.

Across the pillars, NetFoundry's contributions can be summarized as follows:

User: Least-privilege access to specific services with strong session attribution; integrates with enterprise identity (BYO IdP via OIDC) and identity lifecycle automation (SCIM), and supports BYO PKI/CA for certificate-based identities aligned to ICAM governance.

Device: Posture-aware admission and (where configured) continuous re-authorization, scoped per service rather than granting broad connectivity.

Network & Environment: Identity-to-service microsegmentation, default deny reachability, reduced discovery surface (e.g., closed inbound ports / "dark services"), and cross-boundary segmentation expressed as policy - rather than VLAN/subnet sprawl and brittle rule stacks.

Application & Workload: Adoption without breaking legacy via gateway patterns, plus SDK/containers options for modern apps; service-by-service onboarding aligned to incremental COA1 deployments as well as COA2 target-state architecture.

Data: Controls access paths to data services and protects data in motion with encryption; complements tagging, DLP, and at-rest encryption programs.

Automation & Orchestration: Policy-driven, ephemeral access (just-in-time/time-boxed) without ticket-driven port changes - supporting mission tempo, OEM workflows, and dynamic machine-to-machine needs.

Visibility & Analytics: Identity-and-service telemetry - who accessed what, when, and under which policy - to support audit readiness, investigation, and operational oversight beyond IP-only logs complicated by NAT, DHCP, cloud churn, and edge mobility.

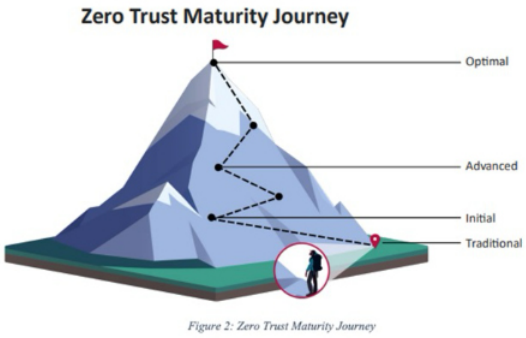

FIGURE 5
CISA Zero Trust Maturity Journey

Summary: 'Optimal' where applicable, across the 5 of the 6 pillars, particularly when integrated with other technologies

1. **Identity**: Zit has its own CA/PKI with ability to utilize third party & integrate with IdPs as well as usage metrics per service per endpoint
2. **Devices:** Various device posture checks (incl. TOTP, domain join OS, process identification, MAC address) with periodic renewal. Further ability to be app-embedded to not trust host OS even if compromised.
3. **Networks**: Supports different service specific micro segmentations across ZTNA/ZTHA/ZTAA, least-privilege, with various encryption & BYOE, and HA resilience. Deep telemetry with 'default-deny' and closed ports. Driven with SW & APIs.
4. **Apps and workloads**: Ability to make apps available across public networks with highest security, with ability to act as strong kill point for attack chains.
5. **Data**: OpenZiti only impacts data in motion, it plays only it's access controlling role within this category.
6. **Cross-Cutting**: Provides events and metrics (up to L4) and provides single view for auditing across the entire network instance(s) with automation and orchestration.

Finally, while pillar mappings are useful for capability planning, leadership ultimately cares about risk outcomes: containment, resilience, and mission continuity. For that reason, this section concludes with how NetFoundry's architecture contains blast radius - even when vulnerabilities are disclosed. In contrast to connect-first networks where trust can become transitive once connected, an identity-first fabric constrains exposure by design: services are not routable or discoverable without explicit authorization, access is granted per service rather than per network, and lateral movement is structurally limited. The result is a Zero Trust posture that is not only compliant in principle, but operable at scale across the environments DoD must secure by FY2027.

For detailed pillar-by-pillar mapping and supporting implementation notes, see Annex A.

5 RMF and ATO Acceleration Through Reduced Exposure and Policy-Driven Change

For many DoD programs, Zero Trust progress is constrained less by the availability of security technologies than by RMF (Risk Management Framework) and ATO (Authority to Operate) friction created by traditional networking models. In IP networks, reachability is established first through routes, ACLs, open ports, and VPN access. Even when strong downstream controls exist, making systems reachable expands the assessable attack surface and introduces continual change events that must be reviewed, documented, and often re-authorized. Program teams experience this as slow cross-domain integration, repeated ATO updates when ports or protocols change, and configuration drift across environments.

NetFoundry changes the RMF dynamic by replacing broad network reachability with service-specific, identity-governed connectivity. Services are unreachable by default and do not expose inbound listening ports; connectivity is created only after identity and policy are validated (authenticate-before-connect). This significantly reduces the assessable exposure that authorization authorities must account for and constrains the blast radius of misconfigurations or vulnerabilities to explicitly authorized services rather than routable network segments. Microsegmentation becomes a centrally governed policy operation (identity > service) instead of a distributed underlay exercise involving firewall rules, subnets, and change windows.

From an ATO perspective, this shifts "network change" into policy change. Programs can onboard or modify individual workflows without redesigning the network or expanding routable access, supporting incremental, COA1-aligned adoption rather than high-risk, big-bang transitions. The scope of authorization becomes clearer and more bounded: which identities can access which services, under what conditions, and for what duration.

NetFoundry also improves RMF evidence and continuous monitoring by producing identity- and service-level telemetry rather than relying on IP-centric logs that are difficult to interpret in dynamic, multi-domain environments. This supports auditability, incident response, and ongoing authorization decisions with more deterministic evidence. The result is not "ATO by automation," but a network architecture that structurally reduces accreditation churn - shrinking exposure, simplifying change, and enabling Zero Trust to scale without slowing mission delivery.

6 Performance, Resilience, and Mission Assurance

Zero Trust implementation must remain operable under real mission conditions: DDIL links, variable latency, multi-transport environments, and contested networks. NetFoundry is designed as a software-only, identity-driven fabric that can use multiple underlay transports concurrently, dynamically steering traffic based on real-time link conditions and providing rapid reroute when links degrade or fail. This supports resilient operations across diverse transports (e.g., satcom, LTE, fiber, tactical radios) while keeping policy enforcement consistent at the service level.

NetFoundry's high availability approach avoids single points of failure. The control plane operates as a highly available cluster with replicated configuration/state and automatic leader election, while the data plane functions as a distributed mesh in which sessions can persist even during controller disruption; components re-sync automatically when connectivity is restored.

In addition to resilience across transports, NetFoundry improves performance and stability inside the overlay itself. It provides end-to-end flow control spanning routers and endpoints (including SDK-based applications and tunneler endpoints), which helps prevent congestion collapse and maintains predictable behavior on high-latency or variable-quality links under load. It also achieves high throughput and resilience through multiplexed streams over overlay circuits, allowing multiple service flows to share efficient encrypted circuits rather than establishing brittle per-flow tunnels—improving link utilization and reducing the operational impact of packet loss and retransmits in constrained environments.

Operationally, the platform is built to work where traditional networking assumptions break: it does not require inbound listeners, static IPs, or manual port-forwarding, and it supports nodes behind NAT/CGNAT with outbound-only enrollment. It also supports deployment on commodity hardware and constrained footprints (including small form-factor systems), with scaling achieved through horizontal distribution of routers/PEPs and published sizing guidance.

7 Priority Use Cases for DoD Leadership

Zero Trust progress accelerates when leaders can align policy objectives, mission outcomes, and technical feasibility. The following use cases reflect where identity-first, authenticate-before-connect networking delivers immediate value while directly supporting COA and DTM-25-003 objectives.

In practice, the strongest early adoption opportunities are often mission teams and program offices that must operate across networks and enclaves they do not control, rather than enterprise network owners alone.

7.1 COA-ready modernization: replace VPNs with identity-based service access

VPNs remain one of the most common, and most problematic, dependencies across the DoD. They provide broad network reachability and rely on downstream controls to limit behavior. This creates oversized trust zones, complicates audit, and introduces risk that scales with every new user, device, or integration.

A Zero Trust program benefits when VPN-style network access is replaced by *service access*: identity-scoped connectivity to specific applications or services, created only after authentication and authorization.

NetFoundry enables a phased, CO1-aligned transition:

- High-value workflows are migrated first
- No disruption to the underlay or legacy applications
- No requirement to re-IP, re-route, or refactor networks
- No new inbound ports or exposed services

For DoD leadership, this creates a practical path to:

- Reduce VPN sprawl without “big bang” migrations
- Shrink attack surface while improving auditability
- Demonstrate measurable Zero Trust progress tied to outcomes, not tools

For program owners, the benefit is simpler: access that works, without weeks of firewall changes or repeated ATO updates.

7.2 Weapon systems and the tactical edge (DDIL environments)

DTM-25-003 explicitly calls for incorporating Zero Trust into weapon systems and combined joint tactical environments. These environments challenge nearly every assumption of traditional networking:

- Intermittent or degraded connectivity
- High latency (hundreds of milliseconds or more)
- Low-power, low-footprint devices
- Non-human systems and machine-to-machine communication
- Rapid mobility and changing network conditions across mission phases

In these contexts, perimeter-centric security models and proxy-based access often break down. Heavy agents, centralized chokepoints, and constant inspection are not viable when links are constrained, platforms are resource-limited, and operational conditions change faster than networks can be reconfigured.

An identity-first overlay model addresses this by:

- Operating independently of transport type (satcom, LTE/5G, tactical radio, maritime links, fiber)
- Maintaining consistent identity and policy even as links change or degrade
- Supporting low CPU and low memory footprints suitable for embedded and edge systems
- Enforcing least privilege at the **service level**, not the subnet or VLAN level

A large U.S. defense contractor evaluating tactical 5G and unmanned systems summarized the benefit as: *"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."* This highlights two practical requirements in the tactical edge: strong Zero Trust networking outcomes (microsegmentation and end-to-end encryption) and interoperability with existing ICAM/PKI approaches - including the ability to start quickly while supporting bring-your-own trust anchors.

For constrained platforms and degraded links, NetFoundry's overlay design supports efficient use of limited bandwidth via multiplexed streams and applies end-to-end flow control across routers and endpoints—improving stability and throughput without requiring heavier inspection stacks or underlay redesign. For DoD leadership, this means Zero Trust is no longer limited to enterprise IT; it becomes applicable to the systems that deliver mission effects.

7.3 AI and agentic workflows without opening the network

AI and agentic systems fundamentally change connectivity patterns:

- Increased east–west traffic
- Explosive growth in non-human identities
- Dynamic, short-lived interactions across environments
- New high-value targets such as model endpoints, tool servers, and data pipelines

Traditional networking turns this into risk and delay. Each new integration requires firewall changes, exposed endpoints, and standing privileges that are difficult to justify—or audit.

An identity-first, default-deny overlay enables a different model:

- Each agent instance receives a cryptographic identity
- Access is granted per service, per task, and per time window
- No inbound exposure of AI services, APIs, or data stores
- Continuous attribution: which agent accessed what, and why

This allows AI initiatives to move forward without forcing network expansion or weakening Zero Trust posture. Importantly, it adds a network-enforced layer of least privilege that complements, rather than replaces, application-layer authorization.

For DoD leaders, this creates a path to scale AI adoption while maintaining governance, containment, and auditability - rather than trading speed for risk.

7.4 OT security and alignment with IEC 62443 principles

Operational technology environments introduce additional governance challenges:

- Mixed ownership between operators, OEMs, integrators, and IT teams
- Multiple overlapping remote access mechanisms
- Inconsistent identity models and audit trails
- Pressure to avoid underlay network changes

These conditions make it difficult to demonstrate compliance with IEC 62443 system requirements, particularly around least privilege, boundary protection, audit, and session control.

The ISA/IEC 62443 series of standards define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS)

An identity-first, conduit-based overlay model aligns naturally with IEC 62443 concepts:

- Per-service conduits bound to identity, protocol, and duration
- Default-deny boundary protection with zero inbound ports
- Deterministic behavior during connectivity loss
- Unified governance without modifying the underlying network

Rather than layering more point solutions onto OT environments, this approach simplifies the control plane while preserving operational sovereignty. This is why large industrial OEMs such as Siemens have already adopted NetFoundry and built it into their products.

For DoD programs operating or interfacing with industrial systems, shipboard environments, or mission-critical infrastructure, this provides a practical way to raise security maturity without introducing unacceptable operational risk.

7.5 From point solutions to a unified Zero Trust network fabric

Across these use cases (VPN replacement, OT/DDIL, and AI), the pattern is consistent: point solutions address individual gaps but increase fragmentation - separate tools for remote access, segmentation, and workload connectivity, each with its own identity, policy, and audit model. An identity-first Zero Trust network fabric replaces this sprawl with a single, policy-driven connectivity layer: identity becomes the control plane, connectivity is created only after authorization, and access is consistently enforceable, auditable, and automatable. For DoD leadership, this is the architectural shift that enables Zero Trust to scale across pillars, environments, and mission timelines without compounding complexity.

7.6 Where DoD engagement should be prioritized first: target high-acuity mission owners, not only branch-level programs

The highest-impact entry points for Zero Trust networking modernization are often not Service headquarters or enterprise network teams first; they are mission teams and program owners who must deliver outcomes across networks, enclaves, and organizations they do not control. These teams experience the limitations of traditional connectivity most acutely: VPN sprawl, firewall/routing dependencies, cross-boundary change delays, and mission impact when access to a specific service requires underlay reconfiguration.

For DoD prioritization, NetFoundry should focus first on environments that combine: (1) cross-boundary dependence, (2) mission ownership without full network ownership, (3) enclave/classification complexity, (4) high mission tempo, and (5) constrained or degraded transport conditions. In these cases, identity-first, authenticate-before-connect networking provides disproportionate value because access is defined as policy (identity-to-service) rather than broad network reachability.

Priority by branch (where pain is often most acute)

U.S. Navy
(afloat / maritime mission systems)
Enclave-dense shipboard environments, DDIL links, coalition operations, and severe space/power constraints.

USMC
(expeditionary / distributed mission support)
Secure access to systems on networks they do not own, under tight timelines and limited infrastructure margin.

USAF
(especially ACC mission defense / mission systems)
Distributed mission defense and mission-system access across installations, contractors, and mixed-classification environments.

Army (expeditionary / coalition / MPE-heavy formations)
Strongest fit in coalition and mission-partner operational contexts.

Space Force
(classified mission ops)
Strong need in contractor-integrated, high-value mission environments, typically with more fixed infrastructure.

Priority by mission-team type (often the strongest buying centers)

- Mission Defense Teams (MDTs) / weapon-system cyber defenders
- Coalition / Mission Partner operators (MPE, CJTF, combined C2, releasable enclaves)
- Shipboard/afloat mission-system operators and maintainers
- Sensor/security/OT-like mission teams operating on non-owned networks
- Distributed mission/business application owners spanning fragmented environments

The result is virtualized, zero trust native overlays, independent of networking and infrastructure. All sessions (internal and supply chain) are authorized before any communication, and no inbound underlay ports are left open. It includes true end-to-end encryption (the keys remain local to the endpoints), with every link using mTLS. Each overlay delivers authorized, microsegmented sessions, mitigating against data exfiltration. NetFoundry is consumed as cloud native NaaS or self-hosted on-premises, including air gapped. NetFoundry is an all batteries included service, with no external dependencies, but includes prebuilt integrations and APIs for the cases when integrations make sense.

This prioritization complements enterprise Zero Trust programs by creating a practical land-and-expand path: prove measurable outcomes first in high-acuity mission workflows (e.g., faster time-to-connect, reduced VPN dependence, narrower exposure, improved auditability), then replicate across adjacent programs and enclaves using the same identity-first policy model.

Publicly referenceable context supporting this prioritization includes: Air Force MDT mission complexity discussions (including multi-installation/contractor-connected mission defense), SEI mission-oriented MDT training environments, Joint Staff CIAV interoperability analysis informing CJADC2/MPE/FMN, Army MPE guidance for coalition operations, and Navy shipboard stovepipe modernization context.

8 OpenZiti: Open Source Foundation and Ecosystem Strategy

NetFoundry develops and maintains OpenZiti, an open source identity-first networking project. OpenZiti provides a transparent, auditable foundation for zero trust networking patterns and enables ecosystem adoption. For DoD, this matters: open standards reduce lock-in risk, enable independent assessment, and support broader adoption across components and partners.

Strategic position: DoD should move toward an ecosystem where VPN-style broad network access is replaced by identity-based, service-specific access. OpenZiti provides a practical technical foundation for this transition, and NetFoundry provides enterprise-grade distribution, support, and capabilities for COA-aligned deployments.

9 A Practical Adoption Plan (90 Days to Proof, Then Scale)

Zero Trust adoption succeeds when it is treated as an incremental operational change, not a network-wide rebuild. The goal of this plan is to demonstrate value quickly - within 90 days - by protecting a small number of high-impact, cross-boundary services, producing audit-ready evidence, and validating operational fit under real mission conditions. This approach aligns with COA-style deployment, allowing programs to prove outcomes, reduce risk, and build leadership confidence before scaling service by service.

9.1 Start with a small number of high-value, cross-boundary services

The most effective starting point is a mission owner - not a central network organization - who must deliver outcomes across boundaries they do not fully control. These teams feel the operational friction of VPN sprawl, firewall change queues, enclave segmentation, and partner integration delays most acutely. Selecting such a workflow ensures measurable impact within 90 days.

- Select 2–4 priority workflows that cross boundaries (cloud < > on-prem, tactical < > enterprise, partner < > single service) and require coordination across enclaves or organizations.
- Deploy the fabric in DoD-controlled infrastructure (COA-aligned) and connect boundary nodes.
- Implement default-deny and publish only the named services required for mission outcomes.

9.2 Define pilot success criteria for leadership decisioning

The most effective starting point is a mission owner - not a central network organization - who must deliver outcomes across boundaries they do not fully control. These teams feel the operational friction of VPN sprawl, firewall change queues, enclave segmentation, and partner integration delays most acutely. Selecting such a workflow ensures measurable impact within 90 days.

- Time-to-permit for a new microsegment: demonstrate policy updates without underlay change tickets.
- Reduction in exposed inbound ports and discoverable services for protected workflows.
- Audit-ready evidence: identity-based logs of service access and policy decisions.
- Operational fit in degraded transport scenarios where applicable.

9.3 Scale by repeating the pattern—service by service

The overlay approach scales by replication: onboard the next workflow, the next enclave, and the next partner, using the same policy model. This reduces complexity growth compared to subnet/rule-based segmentation.

Conclusion

DoD's FY2027 target-level Zero Trust objective requires an approach that eliminates the biggest practical blocker: network reachability and cross-boundary segmentation complexity. NetFoundry's identity-first, authenticate-before-connect network fabric provides a COA1-aligned path to accelerate Zero Trust outcomes - especially in the network and applications/workloads pillars - while integrating with existing identity, device, and data governance programs. In parallel, DoD should drive an ecosystem shift away from VPN-based network access toward service-specific, identity-based access built on open foundations such as OpenZiti.

ANNEX A

Detailed DoD Zero Trust Pillar Mapping

DoD Zero Trust implementation guidance emphasizes outcomes across seven pillars: User, Device, Network & Environment, Application & Workload, Data, Automation & Orchestration, and Visibility & Analytics. Together, these pillars define the capabilities required to reach target-level Zero Trust by FY2027 across enterprise, tactical, and weapons-associated environments.

NetFoundry's strongest value is accelerating the pillars that typically drive schedule and complexity - especially Network & Environment and Application & Workload - while integrating with existing DoD identity and endpoint tooling rather than replacing them. Just as importantly, NetFoundry's identity-first model enables the two cross-cutting pillars that determine whether Zero Trust can scale at operational tempo: Automation & Orchestration (policy-driven, just-in-time access) and Visibility & Analytics (identity- and service-based telemetry rather than IP-only narratives).

Finally, while pillar mappings are useful for capability planning, leadership ultimately cares about risk outcomes: containment, resilience, and mission continuity. For that reason, this section concludes with how NetFoundry's architecture contains blast radius—even in the presence of newly disclosed vulnerabilities.

A.1 User: enforce least privilege access to named services

NetFoundry supports the User pillar by binding access to identity and policy at the service level - so access means permission to a specific named service, not broad reachability to a network. It also integrates with enterprise identity and lifecycle systems (e.g., external IdPs via OIDC and provisioning via SCIM), supporting centralized governance while enforcing least privilege in the network fabric.

- **Service-level access policies:** users are authorized to specific services, not subnets or flat trust zones.
- **BYO PKI/CA:** issue and manage endpoint/workload identities under enterprise PKI governance, enabling interoperability with existing ICAM credentialing and audit requirements.
- **Enterprise IdP integration (OIDC):** leverage existing authentication, MFA, and conditional access patterns where applicable.
- **Lifecycle automation (SCIM):** automate provisioning/deprovisioning and group membership alignment to reduce drift and standing access.
- **Strong session attribution:** who accessed what service, when, and under what policy decision.
- **Time-bound and just-in-time patterns:** reduce standing privilege and support controlled workflows.

A.2 Device: posture-aware admission and continuous authorization

The Device pillar is achieved when device state influences access and can be used to reduce risk in real time. NetFoundry supports compliance-to-connect patterns by enforcing policy at connection time and, where configured, during the session.

- **Posture checks:** ensure only compliant endpoints participate in access paths (e.g., OS/device conditions, process or configuration signals where available).
- **Continuous re-authorization:** posture changes can revoke access without redesigning network controls.
- **Device-to-service scope:** device compliance gates access to specific services instead of granting broad network reachability.

A.3 Network & Environment: advanced maturity through identity-based segmentation

The Network & Environment pillar is where many programs stall because traditional networking is connect-first and segmentation is expressed as a growing set of brittle rules. NetFoundry delivers advanced maturity by replacing IP/location-based reachability with identity-based reachability and default-deny service access.

- **Identity-to-service microsegmentation** enforces least privilege by default.
- **Default-deny networking** reduces lateral movement and discovery opportunities.
- **Closed inbound ports** and "dark services" patterns reduce exposed attack surface.
- **Cross-boundary segmentation** (cloud < > on-prem < > edge < > partner) is expressed as policy, not underlay change requests.
- **Encrypted, identity-bound paths** treat the underlay as untrusted transport and preserve policy intent across diverse environments.

A.4 Application & Workload: adopt without breaking legacy

The Application & Workload pillar is achieved when applications and workloads can be made reachable only through explicit policy, while supporting legacy constraints and modernization. NetFoundry supports both non-invasive and embedded adoption paths.

- **Gateway mode:** front legacy applications (including constrained environments) without modifying application code.
- **SDK mode:** embed Zero Trust networking into modern apps so the app participates in identity-first access and can avoid trusting the host network.
- **Service-specific onboarding:** protect one workflow at a time, then scale - reducing disruption and accelerating ATO-friendly rollout.
- **Protocol flexibility without expanding exposure:** preserve required application protocols while avoiding broad port opening and network reachability.

A.5 Data: control access paths (data in motion) and integrate governance

The Data pillar spans governance (classification/tagging), protection (encryption, DLP), and enforcement. NetFoundry's direct impact is strongest on data in motion: it controls which identities can reach which data services and ensures encrypted transport, while complementing enterprise data governance and protection programs.

- **Identity-scoped access to data services:** only explicitly authorized identities can reach specific data endpoints.
- **Encryption in transit by default** to protect data flows across untrusted transport.
- **Complements (not replaces)** data tagging, DLP, and at-rest encryption programs managed by data and security teams.
- **Event/telemetry signals** can feed monitoring and response workflows for data access oversight.

A.6 Automation & Orchestration: policy-driven, ephemeral access at mission speed

DoD Zero Trust maturity depends on the ability to automate and orchestrate access decisions—not just document them. Traditional networking makes automation hard because access is expressed through routes, ports, and firewall changes that require ticketing and change windows.

An identity-first overlay enables access to be ephemeral and driven by business rules: who/what may access which named service, under what conditions, for what duration.

- **Just-in-time and time-boxed access** for users, systems, OEMs, and automated workflows.
- **Event-driven policy:** posture changes or mission conditions can grant, narrow, or revoke access without underlay changes.
- **Repeatable rollout patterns:** apply the same policy model across enclaves and environments without re-plumbing networks.
- **Safer change management:** access changes become policy updates, not broad rule stacks and exposed ports.

A.7 Visibility & Analytics: identity-and-service telemetry, not IP-only narratives

Visibility in traditional networks often collapses to IP addresses, NAT artifacts, and fragmented logs across routers, firewalls, VPN concentrators, and proxies. In dynamic or constrained environments, this limits attribution and slows investigation.

NetFoundry improves visibility by aligning telemetry to identity and named services.

- **Who accessed what service, when, and for how long** - expressed as identity-to-service activity.
- **Policy decision context:** what rule allowed or denied access and what conditions influenced it.
- **Operationally meaningful blast-radius views:** scope of access per identity and per service by design.
- **Telemetry export patterns** support SOC/SIEM integration and audit readiness.

A.8 Containment, resilience, and Zero Trust in the presence of vulnerabilities

Zero Trust does not assume perfect software. It assumes failure is inevitable and focuses on limiting impact when failures occur. A common concern for security and accreditation authorities is whether a newly disclosed vulnerability (e.g., a CVE) in any component could undermine the environment. In traditional networking models, this concern is valid: once connected, trust is often transitive, and compromise of one component can enable lateral movement.

An identity-first, authenticate-before-connect network fabric behaves differently. Even if a vulnerability exists, access to any service is protected by multiple independent layers that must be defeated before an attacker can reach a single service. These layers include hop-by-hop authentication, identity validation, private service resolution, per-service encryption, and application-layer authorization.

Critically, there is no network-level trust collapse:

- Services are not routable or discoverable without explicit authorization.
- Compromise of one service does not expose others.
- Lateral movement is structurally prevented by default-deny reachability.
- Blast radius is constrained to a single, explicitly authorized service.

Even in the unlikely scenario where every protection layer is bypassed, the impact is limited to one service, never the network itself. This model aligns directly with Zero Trust's assume breach philosophy and with DoD objectives around containment, resilience, and mission continuity. It also simplifies accreditation discussions by replacing broad trust zones with narrowly scoped, auditable access paths.

ANNEX B

DoD Zero Trust Activities & Capabilities Mapping (Overview)

B.1 Purpose and scope

This annex provides a DoD Zero Trust Activities & Capabilities alignment overview for NetFoundry's identity-first Zero Trust Connectivity Fabric (built on OpenZiti). It is designed for enterprise ZT leadership and compliance stakeholders who need a concise mapping that supports planning, governance, and program-level decision-making.

This annex is intentionally summary-level. Annex A contains detailed pillar mapping and implementation notes. A full activity-by-activity crosswalk is maintained in the accompanying spreadsheet and is available upon request for traceability and engineering planning.

B.2 How to read this mapping

NetFoundry's contribution is described as:

- **Native (N):** NetFoundry provides the capability directly in the fabric.
- **Integrates/Enforces (I/E):** NetFoundry relies on an authoritative enterprise system (ICAM/IdP, PKI/CA, EDR/MDM, SIEM/SOAR) but enforces outcomes at the connectivity layer.
- **Out of Scope (OOS):** Requirements primarily owned by other programs/tools (e.g., at-rest encryption, data labeling, UEBA), which can proceed in parallel and integrate with NetFoundry.

B.3 One-page snapshot: Alignment by DoD ZT pillar

Legend: N = Native | I/E = Integrates/Enforces | OOS = Out of Scope

Note: The "Activities/Capabilities covered" column lists representative items covered within the pillar, not an exhaustive restatement of the full DoD rubric.

Key Components Benefits	What DoD measures (outcome focus)	NetFoundry support (N / I/E / OOS)	Activities / capabilities covered (representative)	Operational evidence / artifacts (examples)
User	Access is identity-governed, least privilege, attributable	**I/E**: BYO IdP (OIDC); **I/E**: BYO PKI/CA; **N**: per-service authorization & attribution	Federated identity integration; strong identity binding to access decisions; least privilege access to named services; session attribution; JIT/time-bound access patterns	Identity-to-service access logs; policy decision records; identity provider integration configuration; certificate/ trust-anchor configuration
Device	Device posture influences access; compliance-to-connect	**I/E**: EDR/MDM/CDM signals; **N**: service-scoped admission; **N/I**: re-authorization patterns	Posture-aware access; device compliance gating; continuous/periodic re-authorization; rapid revoke without network change	Posture check results; deny/ allow decision events; per-service policy conditions; access revocation events
Network & Environment	Default deny reachability; microsegmentation; reduced discovery; cross-boundary segmentation	**N**: default deny / dark services; **N**: identity > service microsegmentation; **N**: closed inbound exposure; **N**: encrypted overlay	East-west and north-south microsegmentation; eliminate broad network reachability; reduce exposed attack surface; cross-boundary segmentation (cloud/on-prem/edge/ partner) as policy	Service inventory (named services); segmentation policies; logs showing denied discovery; evidence of “no inbound listeners” posture; encrypted tunnel/ circuit telemetry
Application & Workload	Apps/workloads protected without breaking legacy; supports non-human identities	**N**: gateway patterns; **N**: SDK patterns; **N/I**: workload/service identities	Protect legacy apps without refactor; embed ZT in modern apps; workload-to-workload access controls; incremental service-by-service onboarding	Service onboarding records; app/workload identity artifacts; policy-to-service binding; deployment pattern documentation (gateway vs SDK)

Key Components Benefits	What DoD measures (outcome focus)	NetFoundry support (N / I/E / OOS)	Activities / capabilities covered (representative)	Operational evidence / artifacts (examples)
Data	Data access is governed; data in motion protected	**N**: access-path control; **N**: encrypt in motion; **OOS**: labeling/DLP/at-rest	Identity-scoped access to data services; encrypted transport for data flows; enforce which identities can reach which data endpoints	Identity-to-data-service access logs; encryption evidence; policy mappings to data services; integration hooks for DLP/governance tools (where used)
Automation & Orchestration	Policy adapts at mission tempo; ephemeral access reduces operational friction	**N**: ephemeral/JIT access; **I/E**: event inputs from enterprise tools	Business-rule-driven access; time-boxed access; automated grant/revoke patterns; repeatable onboarding workflows	Policy change/audit trail; time-boxed session controls; automated enrollment/provisioning records; approval workflow integration evidence (where used)
Visibility & Analytics	Visibility answers ZT questions; integrates with SOC tooling	**N**: identity+service telemetry; **I**: export to SIEM/SOAR; **OOS**: UEBA engines	Identity-centric telemetry (who/what/when/decision); service-level activity; evidence for audits; SOC integration	Event/telemetry exports; SIEM/SOAR integration configs; dashboards/queries based on identity > service narratives; audit reports

Key takeaways

- NetFoundry provides strong **native** coverage for the pillars that most often determine timeline and operational risk: **Network & Environment** and **Application & Workload**.
- For pillars dominated by enterprise programs (User/Device/Visibility/Automation), NetFoundry **integrates and enforces** outcomes using ICAM (OIDC + PKI/CA), posture signals, and SOC tooling—without replacing them.
- For **Data**, NetFoundry's primary impact is **governing and protecting access paths in motion**; labeling/DLP/at-rest encryption remain owned by data platforms and governance programs.

B.4 Dependencies and "does not replace" clarity

NetFoundry is a connectivity fabric that makes Zero Trust enforceable at the service edge. It does not replace:

- **ICAM/IdP/MFA** programs and systems (it consumes identity assertions and enforces access).
- **PKI programs** (it supports BYO PKI/CA and enterprise trust anchors).
- **EDR/MDM/CDM** (it consumes posture/health signals and enforces policy).
- **SIEM/SOAR/UEBA** platforms (it exports identity-and-service telemetry; analytics/response occur in those platforms).
- **Data labeling/DLP/at-rest encryption** (owned by data governance and storage platforms).

This separation of duties is intentional: it allows DoD Components to adopt NetFoundry per use case and scale consistently across environments without displacing enterprise tooling.

B.5 Traceability statement

This annex provides an overview aligned to the DoD ZT Activities & Capabilities framework. The complete activity-by-activity crosswalk is maintained in the supporting spreadsheet and is available upon request for compliance traceability, implementation planning, and audit support.