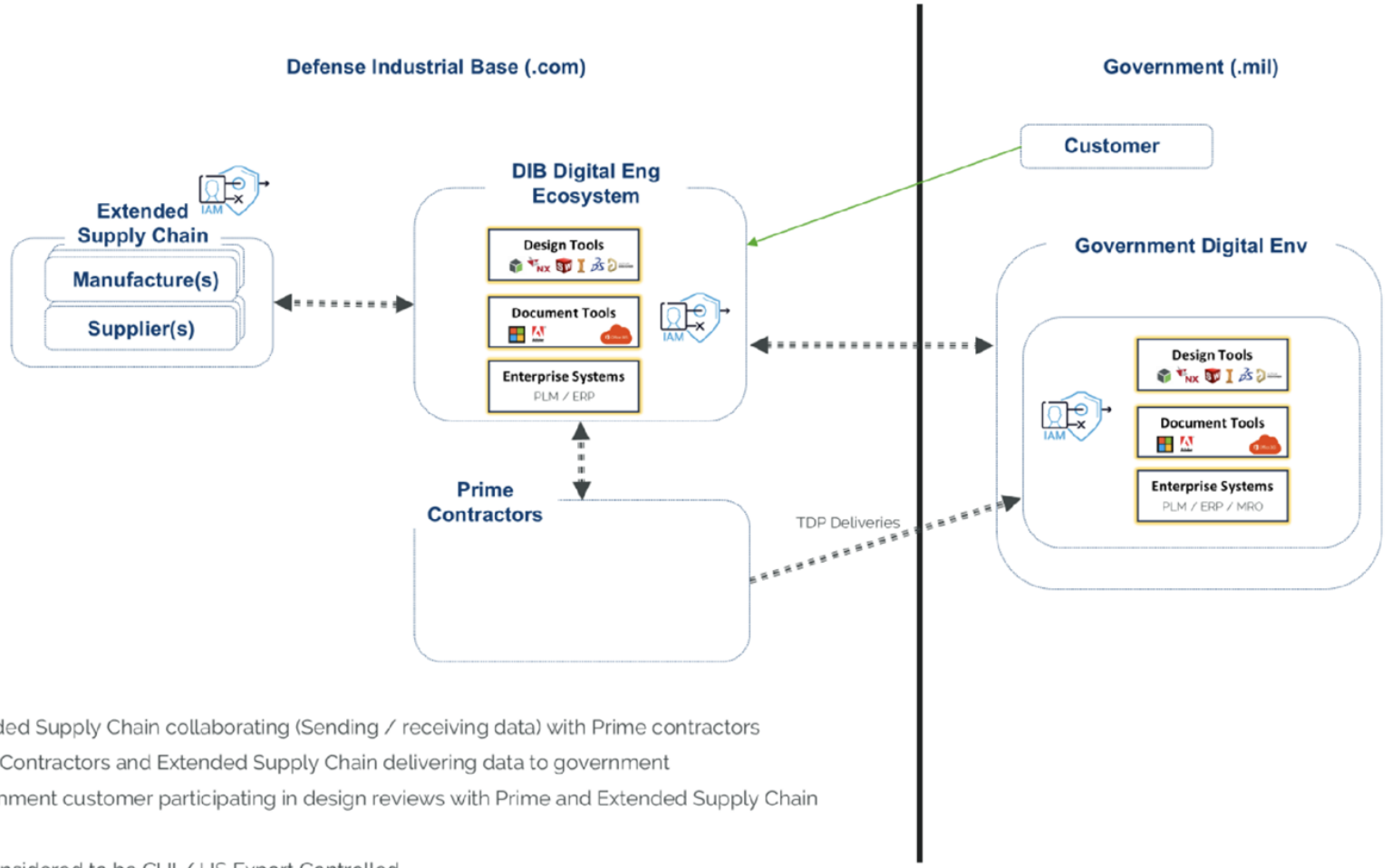
Developers of **OpenZiti**

Secure Workload Connectivity

Stop managing your attack surface. Eliminate it — with the only identity-first zero trust fabric for every AI, API, and machine interaction

DIB Digital Engineering Ecosystem

Controlled data exchange across many network boundaries



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

DIB CUI/CMMC: secure the flow, not the underlay

Practical path for ecosystem to exchange CUI without turning compliance into underlay refresh project(s)

The pressure

DIB suppliers must handle CUI/ITAR across factories, clouds, remote engineers, and partners while CMMC/FIPS expectations become a condition of doing business.

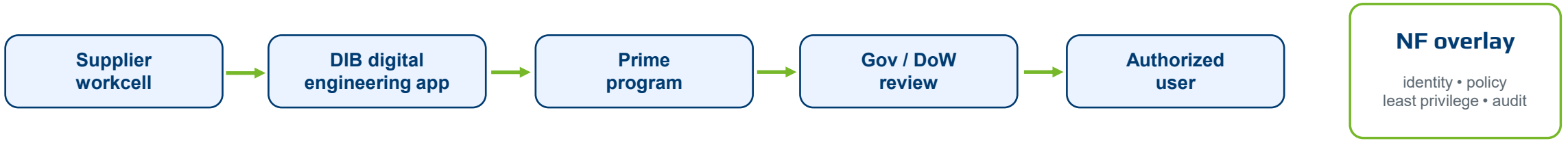
The old answer

Treat compliance as a site-by-site underlay project: FIPS routers, firewalls, VPNs, switches, segmentation, and slow OT change control.

The NetFoundry path

Secure only the sensitive operational paths as identity-defined services, using an overlay that spans edge, plant, cloud, and authorized users.

What this means for PLM / digital engineering flows

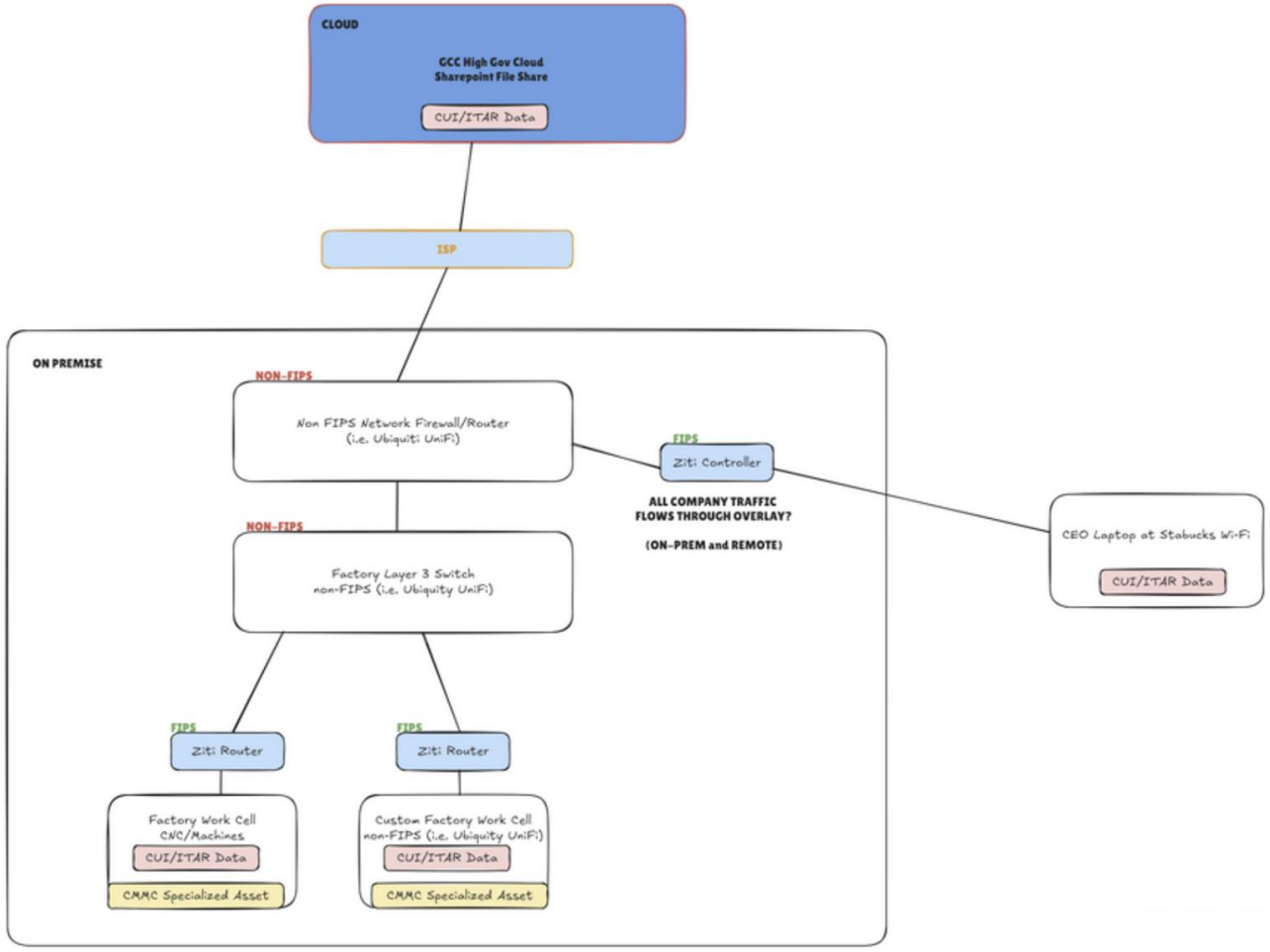


Each controlled collaboration path becomes an explicitly authorized service — not a broad network connection.

NetFoundry

Supplier deployment: secure CUI flows without rebuilding OT

A practical pattern for brownfield factories: make the CUI/ITAR paths identity-defined services.



Supplier can protect selected CUI/ITAR services without replacing existing OT switches, routers, or plant networks.

Key Takeaways

1. **Underlay stays in place**

   The existing plant network may remain non-FIPS and operationally stable; it is no longer the primary compliance boundary for each sensitive flow.

2. **Overlay protects the sensitive paths**

   NetFoundry routers/endpoints wrap the factory work cell, cloud repository, and remote user paths so CUI/ITAR traffic rides identity-first, least-privilege services.

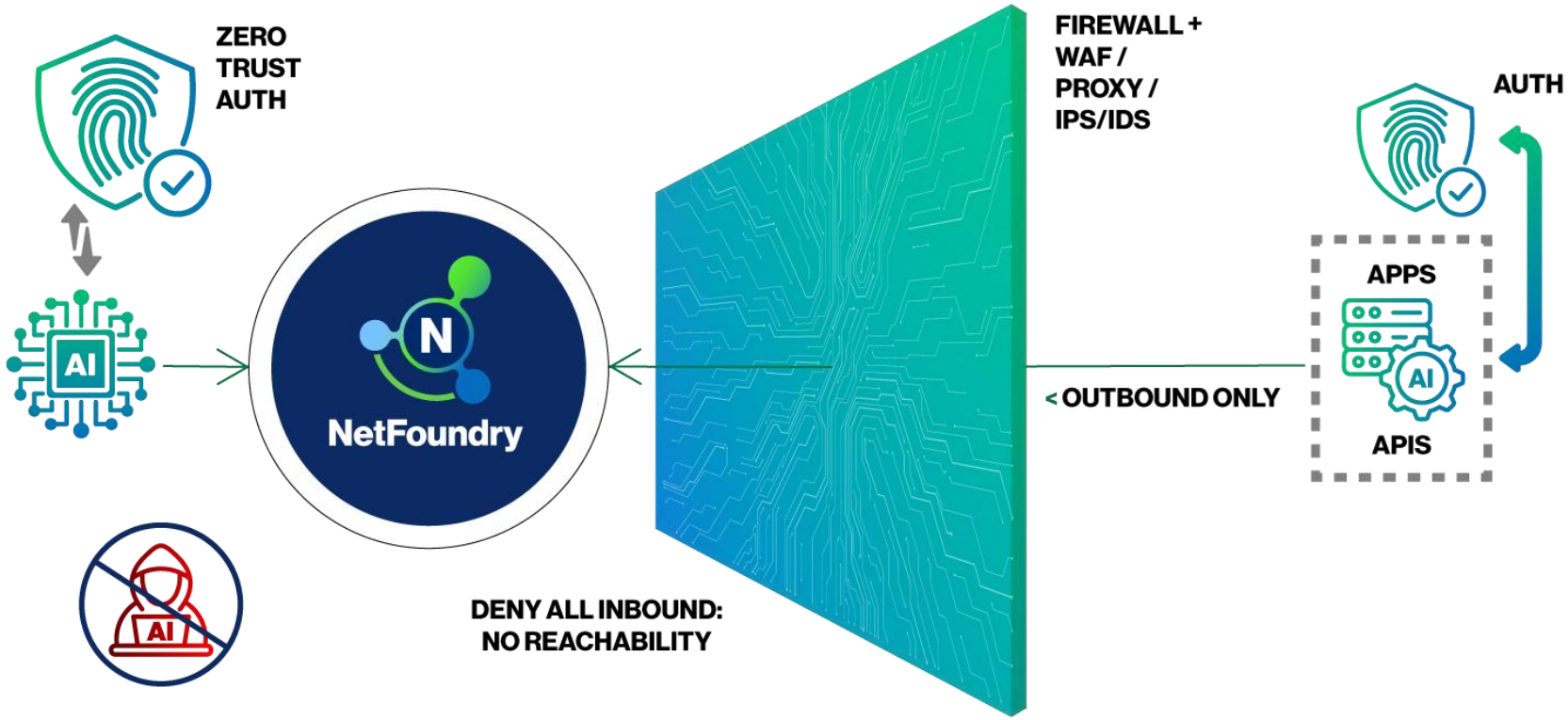
3. **Compliant collaboration scales**

   The same pattern can extend from one supplier to prime/government workflows without every participant building bespoke VPNs or refreshing site infrastructure.

NetFoundry

NetFoundry's Identity-First Reachability™

The only identity-first zero trust fabric for every AI, API, and machine interaction



- Inbound services are Deny All - All connections are outbound-only
- Reachability governed by cryptographic identities (human & non-human)

- Replaces vulnerable firewall ports with cryptographic identities
- Zero reachable ports, zero targets to exploit
- Eliminates 99.99% of threat to attack surface
- Enables least privilege access / segmentation and visibility by identity
- Eliminates operational drag on deployments

NetFoundry

NetFoundry's Software-Only, Private, Dedicated Overlay Networks

Spin up new air-gapped networks in minutes

- 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

Simplified Security Architecture Eliminates Operational Drag

Traditional architecture forces a large operational ‘tax’ across teams which slows the business

Traditional Architecture

- Constant firewall rule changes
- Reliance on configuration, reliability, and vulnerability mgmt. without room for error
- Little to no visibility - often impossible to trace activity by IP Address across networks
- SIEM noise and wasted cross-team analysis

“15–20 policies/rules across tools, teams and firewalls… two weeks to make any change”

Identity-First Reachability

- No firewall changes, no deployment delays
- Simplified and centralized policy-based governance
- Centralized visibility by identity, not IP Address
- Less logs means lower log costs, fewer alerts, and less time chasing false positives

Saves $millions/year while better managing complex, segmented, partner-rich environments

Transforms connectivity from a coordination headache to a simple policy decision

NetFoundry

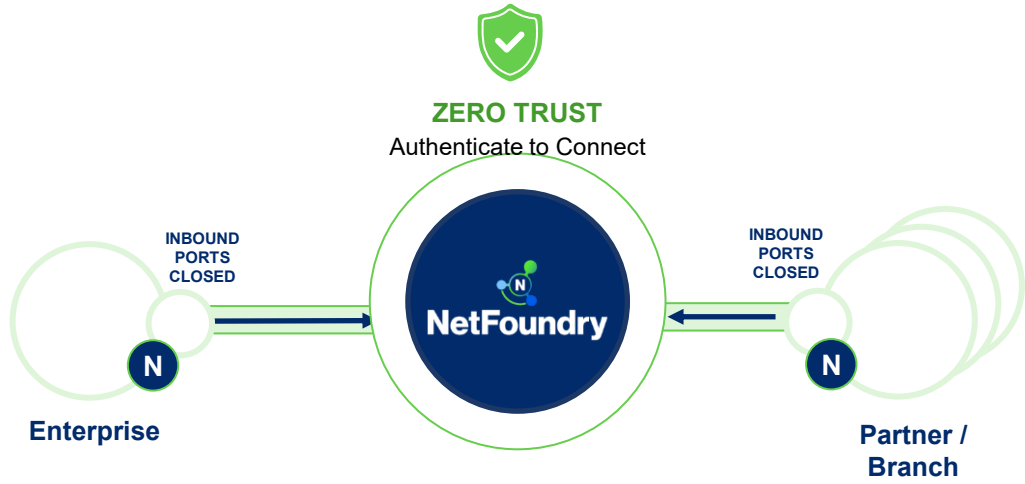
Operational Comparison: S2S VPNs

Site-to-site IPSEC VPN
Manual Complexity & Risk

1. Open inbound firewall ports
2. Configure static routing/BGP
3. Update ACLs/policy on both sides
4. Configure peer IPs & pre-shared keys
5. Setup dedicated hardware appliances
6. Negotiate IKE Phase 1 (Encryption, DH Group, Hash)
7. Define IKE Phase 2 Sas (Security associations)
8. Handle overlapping CIDR ranges (NAT)
9. Monitor tunnel health (complex)
10. Troubleshoot connectivity issues
11. Repeat for every new site (mesh mess)
12. Add ACLs on internal FWs for segmentation
13. Complex day 2 troubleshooting with Engineers on both sides
14. Visibility clouded by false positives & log correlation challenges (IPs)

Infrastructure Dependent, Network-Centric, Open Ports (Vulnerable)

NetFoundry
App-Centric Simplicity

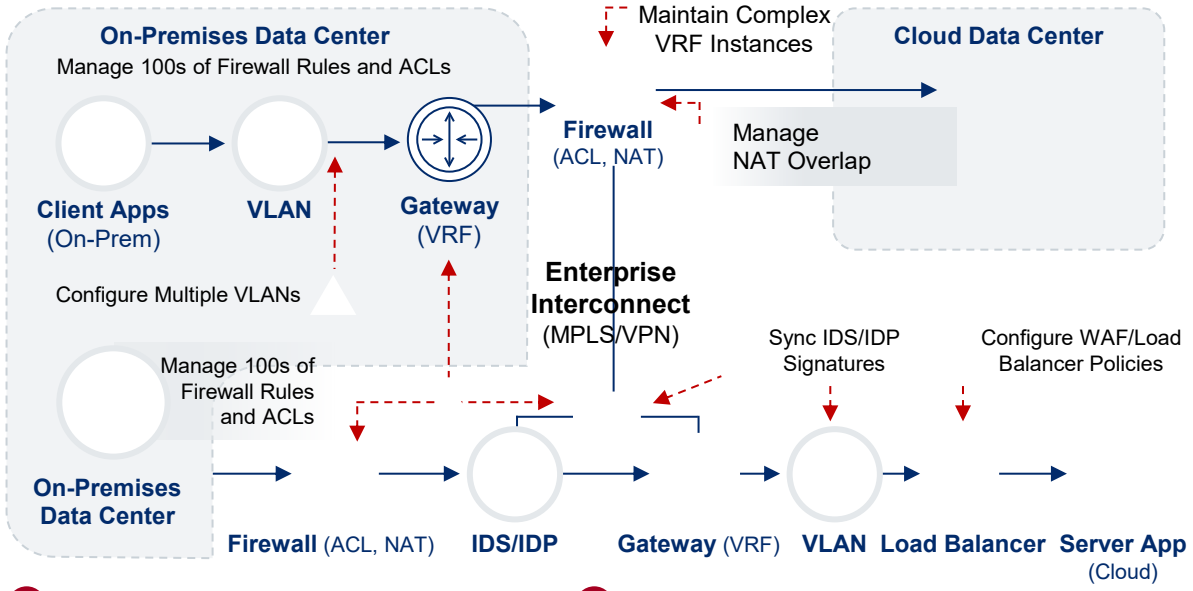


1. Deploy Edge Router on COTS HW
2. Create service and micro-segmented policies (UI/API/IAC)
3. Simple, centralized, deep operational visibility (UI, API, logs)

Hardware Agnostic, Outbound-Only mTLS Tunnels, Zero Trust Architecture, Software-Defined, Fast Scalability

Operational Comparison: Internal Microsegmentation

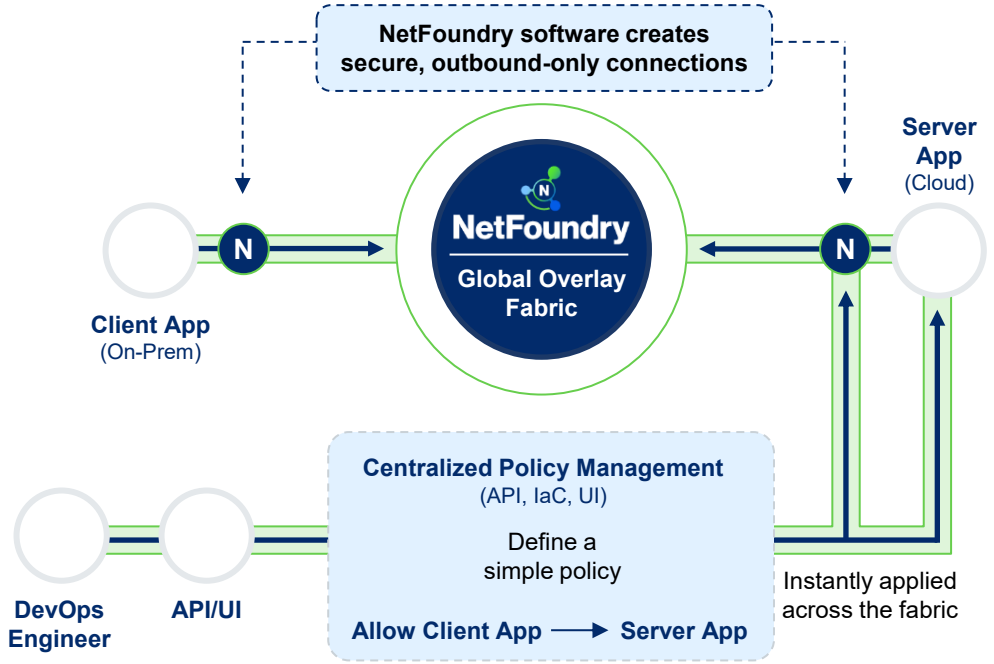
Traditional Microsegmentation
Complex Hop-by-Hop Configuration



1. Deploy and maintain agents
2. Dependency mapping and traffic flow discovery
3. Define and continuously tune segmentation policies
4. Complex integration
5. Hard to troubleshoot blocked traffic
6. Requires deep network/app expertise
7. Limited hybrid/multi-cloud visibility
8. Performance overhead from agents/inspection
9. Ongoing drift management
10. Specialized Day 2 operations

Agents everywhere, complex topology-based mapping and static rules that limit scalability and ease of operations

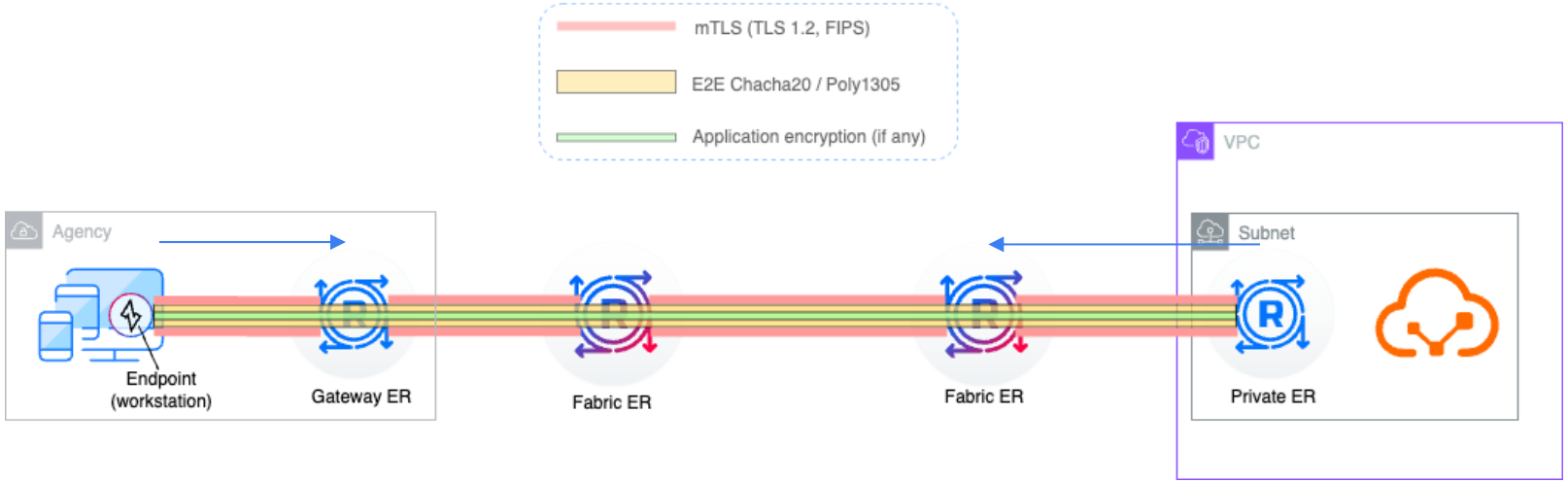
NetFoundry
Simple Identity-based Micro-segmentation



1. No agents required on workloads
2. Identity-based application access policies
3. Works across cloud, on-prem, edge
4. No network reconfiguration needed
5. No dependency mapping required

No agents, zero trust built in, software-defined, Identity and service-based policies and visibility

NetFoundry Encryption Overview & FIPS

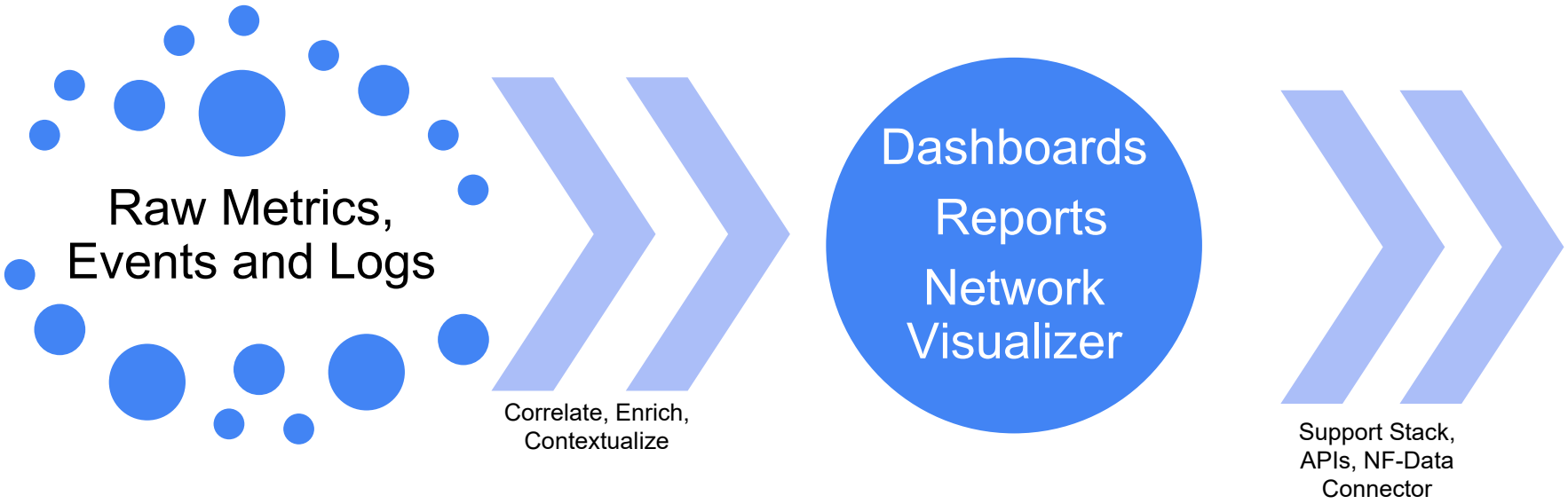


- Private/sovereign keys generated by source/destination
- Data plane is impossible to be decrypted by Private/Fabric/Gateway ERs
- Optional, FIPS compliant Mutual TLS (mTLS) on each hop and/or E2E.
- Routers have no access to payload or the payload keys.
- Enrollment and PKI/key management fully automated.

- The Edge Routers are built as container images using Ubuntu 22.04. The encryption library uses OpenSSL FIPS provider. The certificate number for the compliance is **4282**. https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4282
- The Windows Desktop Edge uses the Windows 11 native libraries, under certificate **A2004**. https://csrc.nist.gov/projects/Cryptographic-Algorithm-Validation-Program/details?source=A&number=2004
- More details at: https://netfoundry.io/products/netfoundry-platform/fips-compliance/

NetFoundry

NetFoundry Reporting



Overlay Network

NetFoundry

NetFoundry

Flexible Deployment Options

OPENZITI

Self hosted open source

Community support

Self deployed and managed (connectors, routers, controller), self orchestrated

SELF-HOSTED

Self hosted licensed

Enterprise grade support (24x7)

Self deployed and managed (connectors, routers, controller), self orchestrated

Guidance for resilient, reliable, scalable production architecture & deployment

Operations, logging, assurance and platform LCM tools

Contracted relationship (indemnification)

FIPS compliant

Use case and/or implementation documentation

CLOUD

SaaS

Enterprise grade support (24x7)

Fully managed by NetFoundry with 99.95% uptime SLA

Guidance for resilient, reliable, scalable production architecture & deployment

Fully automated LCM of hosted and LCM support for self-hosted components

Contracted relationship (indemnification)

FIPS compliant

Use case and/or implementation documentation

SOC 2 Type II compliant

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

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

Developers and Maintainers of World Renowned OpenZiti Opensource Platform

NetFoundry