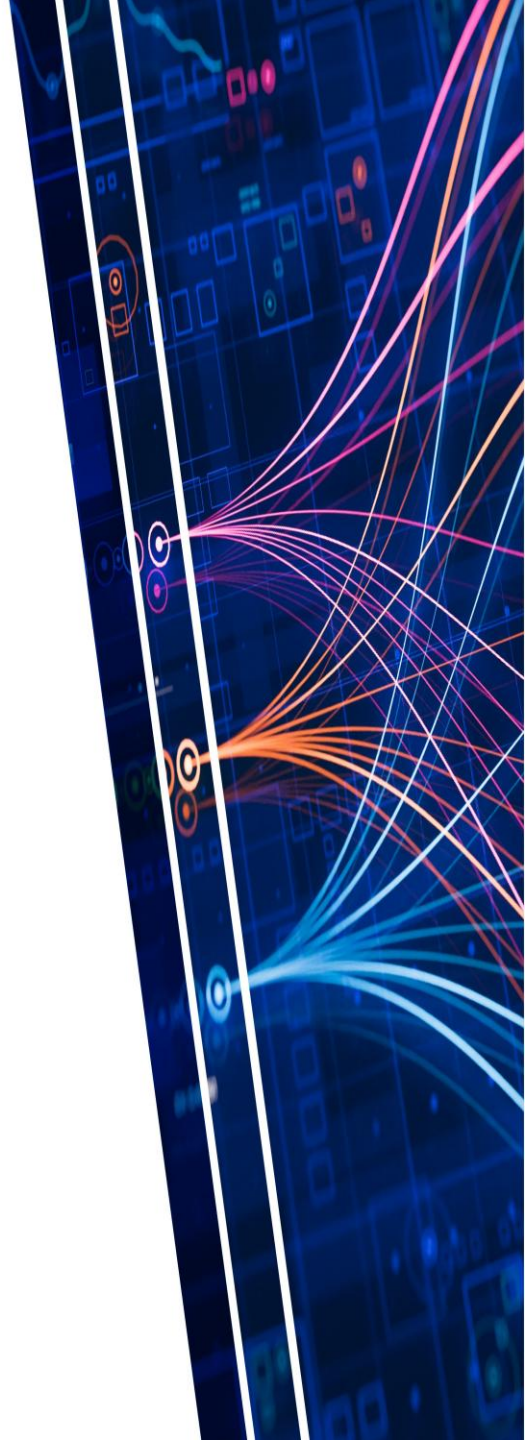


Post-Mythos vulnerability mitigation

AI won the time to exploit versus time to patch race…but you can end the race

Post-Mythos: more CVEs, weaponized faster, via more doors

10 hours

disclosure to exploit time
(average was 2 years in 2020)

- Microsoft Patch Tuesday now shatters records
- 8× increase in edge breaches in 2026
- CISA says they can no longer publish all CVEs

300 new WAN doors

per month
(due to cloud, APIs, IoT, B2B, etc.)

- 39 billion perimeter edges by 2030
- Every door is a target
- 8x increase in edge breaches in 2026

NetFoundry helps remove reachability so you patch at your own speed without costs and risks of rushed testing and fire drills, including for use cases such as 3rd party, APIs, OT and IoT.

Big 4 results from removing reachability

Shrink your exploitable backlog

Unreachable workloads exit the exploitable queue. Remediation-SLA breaches fall without a single extra patch cycle.

KPI: open exploitable criticals ↓ · SLA breach rate ↓

Decrease uptime risk Emergency changes become scheduled ones

A KEV on an unreachable workload is a normal ticket, not a war room or rushed patch. Each avoided emergency window removes labor costs and business continuity risk.

KPI: emergency changes avoided × cost per window

Gain an audit-grade compensating control

PCI DSS compensating-control worksheets, DORA/NYDFS/CIP mitigations, risk-acceptance memos. All backed by evidence a tester can verify: scan and find nothing.

KPI: findings closed with evidence · audit prep hours ↓

Reduce the un-patchable estate risk

EOL systems, legacy apps, many OT and medical devices, vendor appliances, M&A estates. In cases where no patch will ever come, unreachability is the remediation, not the stopgap.

KPI: % of unpatchable assets mitigated

NetFoundry

NetFoundry helps with the remediate part of the ecosystem

Discover & inventory	Scanners / CNAPP	EASM
Prioritize	Threat context	Risk score, attack path analysis
Validate exploitability	BAS / autonomous pen test	External scan verification
Remediate	Patch or in-path shield	Make workloads unreachable
Workflow & SLA	Remediation workflow	Orchestration
Governance	GRC & board metrics	Audit evidence

- NetFoundry makes any workload unreachable – from legacy to agentic. Includes EOL, OT, appliances, 3rd-party, site-to-site.
- Use NetFoundry to proactively make any single workload unreachable without impacting anything else.
- Choose to leverage NetFoundry to fill the gaps left behind by zero trust and microseg solutions, or to replace them.
- Choose to use NetFoundry on-prem or cloud solutions.

NetFoundry

Remediation options when the next KEV lands (or before it lands)

Patching is the permanent fix - unreachability reduces the costs and risks and puts you in control of the timelines

	Microsegmentation	ZTNA or SASE	NetFoundry unreachable
Time to mitigate	Days, weeks or months	Hours for user-facing apps	Hours for any type of workload
Uptime / change risk	High	Low	Minimal: per-app, no firewall or network surgery
Coverage	East-west for mapped workflows; gaps for others	Employee to modern app; gaps for others	All workloads include OT, IoT, legacy, AI, 3rd-party. Use NetFoundry on-prem or cloud solution.
Still reachable by attacker?	Reduced laterally; N-S remains	Hidden for users; workload paths remain	No path for unauthorized parties – human and non-human
Audit evidence	The policy	The policy	The policy and is immediately scan-verified
When it's the right choice	E-W containment, when done ahead of time, for mapped workloads	Workforce using modern apps	All workloads or specific ones (high risk, crown jewels, legacy, etc.). Get E-W microseg and N-S zero trust.

Use NetFoundry to quickly close the gaps which microseg, ZTNA and SASE leave behind.
Or use NetFoundry for all microseg and zero trust needs.

NetFoundry

Board scorecard for removing reachability

% workloads unreachable

0% → target by tier

Categorize by workload. The risk reduction RPI of removing public exposure.

Mean time to mitigate

Months → Days → Minutes

From CVE publication to no-path. The operational ROI of exiting the patch race.

Emergency changes avoided

Count × $/window

Reducing both absolute and opportunity costs of the labor and added risk

Remediation-SLA breach rate

↓ quarter over quarter

Unreachable workloads leave the exploitable queue

Findings closed as compensating control

Per framework

Audit-accepted closures with scan-verified evidence attached.

The next 9.x CVE

Priceless

A non-event for you and your customers.

NetFoundry

Triage faster, with less risk and cost

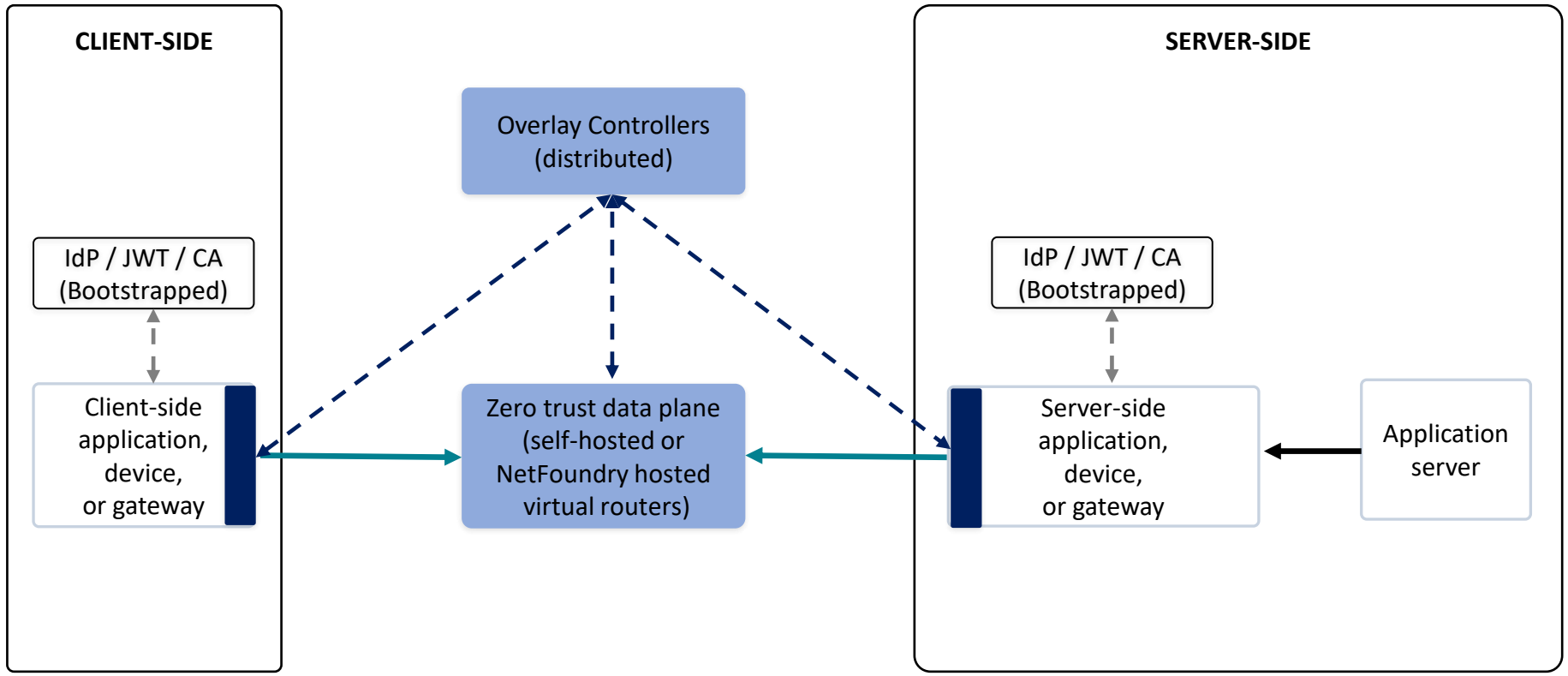
Patch on your schedule — not the Internet's

Make the next KEV a non-event

Appendix

How NetFoundry workload unreachable works

Built on OpenZiti (the open-source zero trust networking platform NetFoundry created and maintains)



Legend

Policy enforcement points (PEPs)

- Put PEP in the app (SDK), on device (connector) or gateway
- Includes multiple NHI and auth options
- Options for legacy, clientless, JIT, IPsec

Virtualized overlay

- Only accepts PEP authorized sessions
- Self-hosted, NetFoundry-hosted, hybrid
- Private and dedicated options
- Software-only, deploy as code in minutes

- Run in passive mode first. Cut over via policy change (via web console or API).
- Make single app unreachable w/o impacting anything else – proactive or after vulnerability.
- Optionally add full zero trust, microsegmentation and/or sandboxing.
- This diagram shows gateway options. SDK is a clientless option to embed the connector in the application. Connectors are available for every major OS and cloud.
- No gateways are necessary with SDK or connector option but can serve as ‘break glass’ access or inspection points.

How NetFoundry workload unreachable works

1: Identity + posture + MFA

NetFoundry provides options to match operational needs, including:

- Bootstrapped X.509 PKI, keys generated on-device
- Enterprise CA and IdP options
- MFA and posture checks
- External JWT option
- Keycloak, SPIFFE, CAC etc.
- Clientless, client, gateway, IPsec, TLS and mTLS options.
- JIT and continual auth options.
- Jira, ServiceNow, API workflow integration options.

2: Zero trust overlays

- Overlays do not allow any packets unless identity, authentication and workload access authorization are done first
- Client and server sides dial outbound to virtualized overlay – eliminate open inbound port, NAT and IP address overlap
- Overlays are spun up in minutes. Self-hosted and NetFoundry hosted options. Use for anything including server-to-server, AI agent to AI agent, OT, IoT, APIs, admin access.

3: Nothing to scan, no path to exploit

- Unauthorized parties can't discover, ping, scan or connect - the CVE has no path.
- Authorized session end-to-end encrypted with libsodium, FIPS and PQC options
- Same solution can do east-west microseg and sandboxing – with single set of controls and policies
- Identity-attributed logs and scan-verified unreachability export to SIEM, GRC, audit packs (PCI, DORA, NYDFS, CIP).

Use surgically or universally: make one workload unreachable today (live KEV, crown jewel, EOL server) without touching anything else or steadily and proactively move all to the unreachable model.

NetFoundry