

Defending the Network: DevSecOps in Modern Telecommunications

The backbone of global connectivity cannot afford a single unpatched vulnerability.

Dave Hoon
Chief Technology Officer, Norseman Defense Technologies · February 2026

Telecommunications providers don't just build networks — **they build the infrastructure that everything else depends on.** Every financial transaction, every military communication, every emergency call, every enterprise cloud connection rides on telecom infrastructure. That makes telecom networks the highest-value targets in any adversary's playbook — nation-state or criminal.

And yet, the pressure to ship new services has never been more intense. **5G rollouts, edge computing, network slicing, IoT onboarding, virtualized network functions** — the pace of innovation is relentless. The carriers that win are the ones that ship fast *and* ship secure. The ones that choose one over the other will learn — painfully — that **speed without security is just accelerated exposure.**

DevSecOps: Security as a Continuous Operation

In defense, we don't bolt security on after the mission is planned. **Security is embedded in every phase of the operation — from concept to execution to sustainment.** DevSecOps applies that same principle to software delivery.

For telecom providers, this means fundamentally rethinking how code moves from development to production:

- **Security integrated at commit, not at release.** Every code push triggers automated static analysis (SAST), dependency scanning, and container image validation. Vulnerabilities are caught in minutes — not discovered in post-deployment penetration tests weeks later. *The cost of fixing a vulnerability in development is orders of magnitude less than fixing it in production.*
- **Infrastructure as Code with policy guardrails.** Network configurations, virtual network functions, and cloud-native infrastructure are defined in code — versioned, reviewed, and validated against security policies before deployment. No manual configuration drift. No undocumented changes. **Every environment is reproducible and auditable.**
- **Automated compliance gates.** Regulatory requirements — FCC, NIST, 3GPP security standards, GDPR — are encoded as policy-as-code and enforced in the CI/CD pipeline. Builds that don't meet compliance thresholds don't deploy. Period. *Compliance becomes a continuous state, not a periodic audit.*

Continuous Release Testing: Proving Resilience Before Deployment

In telecom, a bad software release doesn't just cause downtime — **it can take down emergency services, disrupt financial markets, or create security vulnerabilities across millions of connected devices.** Continuous release testing is how you prevent that.

- **Automated regression and performance testing.** Every release candidate is subjected to full regression suites and performance benchmarks — automatically, in CI/CD, before any human reviewer sees it. Load tests simulate peak traffic conditions, failover scenarios, and degraded-mode operations.
- **Chaos engineering for network resilience.** Deliberately injecting failures into staging environments — node outages, latency spikes, configuration corruption — to validate that the system degrades gracefully. *If your network hasn't been tested against failure, it hasn't been tested at all.*
- **Canary and blue-green deployments.** New releases are rolled out to a fraction of production traffic first, monitored against real-world telemetry, and automatically rolled back if anomaly detection triggers. **Zero-downtime deployments aren't a luxury in telecom — they're a requirement.**

Automated Threat Mitigation: Defending at Machine Speed

Nation-state adversaries don't attack on human timescales. **They attack at machine speed — and your defenses must operate at the same tempo.**

- **Real-time threat intelligence integration.** CI/CD pipelines that automatically check new dependencies, container images, and third-party components against live threat intelligence feeds. Known-vulnerable components are blocked from entering the build — *before they ever touch production infrastructure.*
- **Runtime application self-protection (RASP).** Deployed services that monitor their own behavior in real time, detecting and blocking exploitation attempts — SQL injection, API abuse, privilege escalation — without waiting for a SOC analyst to respond.
- **Software Bill of Materials (SBOM) enforcement.** Every deployed component has a complete, machine-readable inventory of its dependencies. When a new CVE is published, **automated scanning identifies every affected service in the network within minutes** — not the days or weeks that manual inventory processes require.

- **Zero trust for the CI/CD pipeline itself.** The build and deployment infrastructure is often the most valuable target in the enterprise. Norseman applies the same zero trust principles to pipeline security — *signed commits, verified build environments, immutable artifacts, and least-privilege service accounts* — that we apply to classified defense systems.

5G and Network Virtualization: The New Attack Surface

The shift to **5G, software-defined networking (SDN), and network function virtualization (NFV)** has fundamentally changed the telecom security landscape. The network is no longer hardware — it's software. And software has vulnerabilities.

- **Containerized network functions** require container security scanning, runtime monitoring, and orchestration-layer hardening that traditional network security tools were never designed to provide.
- **Network slicing** introduces multi-tenancy at the network layer — requiring isolation guarantees that must be validated continuously, not assumed.
- **Edge compute nodes** deployed at cell sites and aggregation points create a distributed attack surface that demands the same edge security discipline Norseman applies to forward-deployed military systems.
- **API-first architectures** expose service interfaces that must be authenticated, rate-limited, and monitored against abuse — *because every API is a door, and adversaries are testing every handle.*

Why Norseman for Telecommunications

We built our DevSecOps practice defending networks where the adversary is a nation-state with unlimited resources and patience. **That's the standard we bring to telecom.**

- **DevSecOps and Platform Engineering** — our core DevSecOps practice, purpose-built for organizations where security and speed are both non-negotiable.
- **Cyber Resilience and Zero Trust** — network security architectures designed for environments where the perimeter doesn't exist and every component must prove its identity continuously.
- **Cleared engineering staff** experienced in classified network environments — bringing security clearance-grade discipline to commercial telecom infrastructure.
- **Odin's Edge** — our autonomous edge platform, directly applicable to securing and managing distributed telecom edge infrastructure in locations where centralized management isn't an option.

Decisive Network Superiority

In warfare, communications superiority is the prerequisite for every other advantage. The same is true in business. The telecom providers that embed security into their development DNA — not as a gate, but as a *continuous, automated, machine-speed operation* — are the ones that will maintain network superiority as threats evolve.

We deliver the engineering discipline required to keep communications resilient against sophisticated, ever-evolving threats. Because the network is the mission — and the mission doesn't tolerate downtime.

Explore our **DevSecOps and Platform Engineering** practice, **Cyber Resilience and Zero Trust** solutions, or **contact our team** to discuss how Norseman can harden your telecom operations.

Published at norseman.com/insights/defending-the-network-devsecops-telecommunications. To talk with Norseman Defense Technologies, call 410.579.8600 or email sales@norseman.com.