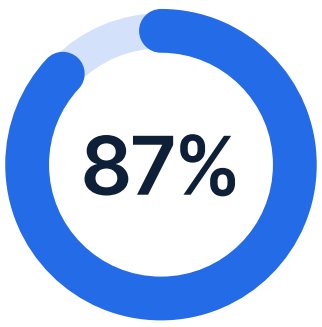
BLUECAT™

LiveNX | Explainer

Mission-ready network insight

Unified observability for defense and intelligence networks



of network operations teams use multiple network observability tools.

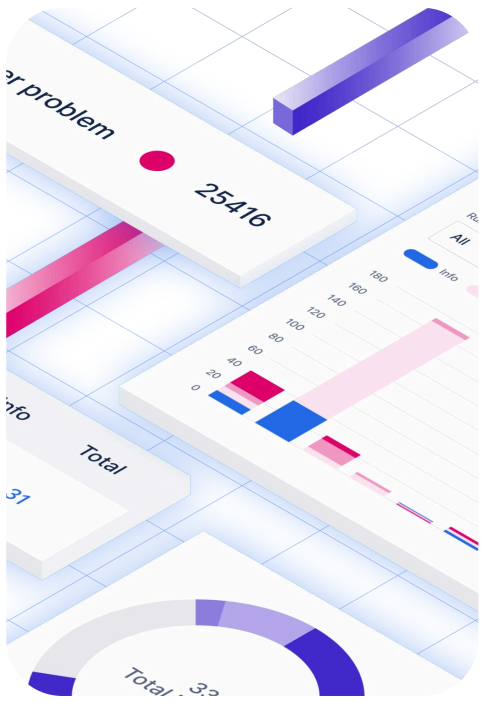
Source:
The Network Observability Maturity Model: How to Plan for NetOps Excellence, Enterprise Management Associates

Fragmented network observability puts mission-critical services at risk

U.S. defense and intelligence networks support users, applications, and mission services across distributed, multi-vendor environments. When device health, traffic flows, packet data, alerts, and change history are fragmented in separate tools, network teams lose valuable time trying to connect symptoms to root causes.

The result is slower troubleshooting, more blind spots, and higher service availability risk. Network teams may know something is wrong, but not whether the issue comes from device saturation, interface errors, traffic congestion, packet behavior, security anomalies, or a recent change.

Federal agencies need network observability solutions that consolidate operational evidence in one view, connecting device telemetry, flow analytics, packet-level insight, automated diagnostics, and AI-guided analysis. Network teams can better see what is happening, understand why, and act before issues disrupt critical missions.



BlueCat connects network observability signals

BlueCat's network observability solutions bring together complementary observability capabilities for network and security teams. This reduces tool pivoting and helps you move from reactive monitoring to proactive mission assurance. Solutions include:

- **BlueCat LiveNX,** which offers observability for traffic behavior, performance, and application paths and **Network Resource Monitoring**, an add-on to boost device visibility and telemetry
- **BlueCat LiveWire,** which provides packet-level intelligence for network forensics, and **Security Insights**, an add-on for fast packet-level anomaly detection and forensics at the network edge
- **BlueCat LiveAssist,** which applies AI to telemetry, alerts, and configuration data, giving teams natural-language access to urgent risks, potential root causes, and recommended next steps
- **BlueCat LiveAssurance,** which offers automated diagnostics, validation, and recommended remediation for critical infrastructure, including post-change verification

"LiveNX has significantly improved our organization's network performance monitoring capabilities, allowing us to promptly identify and rectify network issues, thereby minimizing downtime.

Senior technology services specialist, FedEx

Use case: How network observability solutions can help when a mission service degrades

When a mission service degrades, defense and intelligence network teams can start with LiveNX to identify affected paths and traffic patterns. You can then use Network Resource Monitoring to check device health, pivot into packet evidence with LiveWire where deeper analysis is required, and then use LiveAssist or LiveAssurance to guide root-cause analysis and remediation.

Implementing network observability solutions benefits operations in several ways, including:

- Faster diagnosis with shared operational context
- Fewer escalations caused by missing evidence
- Lower risk from undetected device, traffic, security, or change-related issues

Next steps

Discover how BlueCat can unify network observability across defense and intelligence networks.

Learn more