

Network Resource Monitoring

Observability add-on combining network device health data, telemetry, and flow analytics for end-to-end visibility



Challenge

Enterprises face fragmented visibility across hybrid networks. Traditional device monitoring tools operate in silos, leaving network teams blind to the connection between device health and performance. As a result, troubleshooting is reactive and inefficient.



Solution

Network Resource Monitoring, an add-on to BlueCat LiveNX, extends LiveNX's traffic analysis capabilities with real-time telemetry from switches, routers, and wireless infrastructure. By combining device health data with flow analytics, NetOps teams gain end-to-end visibility for data-driven decision-making.



Benefits

- Faster troubleshooting and reduced downtime
- Proactive performance and capacity management
- Simplified operations across hybrid, multi-vendor environments
- Centralized and accurate device inventory

[Learn more](#)

Extending network observability with unified device visibility

Modern enterprise networks are increasingly complex, spanning hybrid cloud, SD-WAN, and wireless environments managed through siloed tools and data sources. This fragmentation creates significant visibility gaps, making it difficult for network teams to understand the network's true health and performance.

As a result, network teams often struggle to determine where issues originate. Without correlated insights across infrastructure, traffic, and performance data, troubleshooting is reactive, manual, and slow—requiring engineers to pivot between dashboards and export data and rely on experienced guesswork. SNMP-based monitoring also offers limited insight into real-time conditions, traffic patterns, and emerging bottlenecks, leaving teams blind to early warning signs of performance degradation.

Network operations teams need a consolidated, intelligent view of their entire infrastructure—one that spans routers, switches, and wireless controllers and access points across multi-vendor environments. They need continuous visibility that links device health to telemetry and flow data, enabling better root cause analysis, accountability, and decision-making. They also need tools that reduce operational overhead and eliminate the need to manually correlate data from multiple systems.

This solution brief explains how Network Resource Monitoring—an add-on capability to LiveNX, BlueCat's network observability and intelligence solution—unifies device health, network telemetry, and flow analytics into a single view. Use case examples show how NetOps teams can use Network Resource Monitoring across multi-vendor environments to detect bottlenecks, accelerate troubleshooting, and optimize capacity. It also highlights key differentiators from other solutions and outlines primary benefits.

Solution overview

Network Resource Monitoring continuously collects, normalizes, and enriches operational data from across the enterprise network, creating a comprehensive, real-time representation of infrastructure health, operational state, and service availability.

Rather than simply monitoring devices, Network Resource Monitoring builds operational context across every major infrastructure domain, including routing, switching, wireless, security, and application delivery. This data includes infrastructure telemetry, routing tables, ARP tables, wireless infrastructure, firewall state, load balancer services, operational alerts, and log events.

Working alongside LiveNX—which provides flow analytics, topology intelligence, and application traffic visibility—Network Resource Monitoring helps create a unified operational dataset that describes both how the infrastructure is operating and how the network is behaving. Together, they turn raw metrics into insights that reduce mean time to resolution (MTTR), prevent performance degradation, and improve user

experience.

With Network Resource Monitoring, network operations teams can:

- Monitor device health across multi-vendor environments—including Cisco, Arista, Aruba, Nokia, F5, Palo Alto Networks, Fortinet, and other supported platforms
- Identify and resolve performance bottlenecks faster
- Forecast capacity needs and prevent bandwidth saturation

How it works

Network Resource Monitoring extends network observability to the device and resource layer by continuously collecting and correlating device and resource-level telemetry with traffic and topology intelligence. It uses SNMP polling and vendor APIs to collect real-time and historical network infrastructure telemetry across Cisco, Arista, Aruba, Nokia, F5, Palo Alto Networks, and Fortinet environments.

The following table details the types of telemetry data collected:

Device category	Telemetry data collected	
Network infrastructure	• CPU and memory utilization • Interface utilization, errors, and discards • Environmental health (temperature, fans, power) • Routing tables • ARP tables	• Neighbor relationships (CDP and LLDP protocols) • VLANs • Interface operational state • Device inventory • Configuration status
Wireless infrastructure	• Wireless controllers • Access points • Radios • SSIDs • Wireless clients	• Radio Frequency utilization • Channel utilization • Signal quality • Client connectivity and health
Firewalls	• High availability status • VPN tunnel health • Interface status	• Session statistics • Operational state
Load balancers	• Virtual IPs • Pools • Pool members	• Service availability • Health monitoring • Traffic distribution
Operational events	• Infrastructure alerts • Syslog and log events • Configuration changes	• Device state transitions • Operational anomalies

Use cases

This section outlines five real-world scenarios that demonstrate the benefits of using Network Resource Monitoring with LiveNX.

Use case 1: Boosting operational efficiency through automation

Maintaining accurate device inventories and manually collecting telemetry are time consuming and error-prone. In fast-

changing environments—where devices are constantly added, reconfigured, or retired—manual updates quickly fall out of sync. Network Resource Monitoring automates both discovery and telemetry collection, continuously scanning the network to identify connected devices, classify their roles, and capture key metrics in real time. All data flows directly into LiveNX's unified model, keeping visibility up to date without manual effort. This automation saves time, reduces the risk of misconfiguration, improves compliance readiness, and ensures that monitoring scales as networks grow.

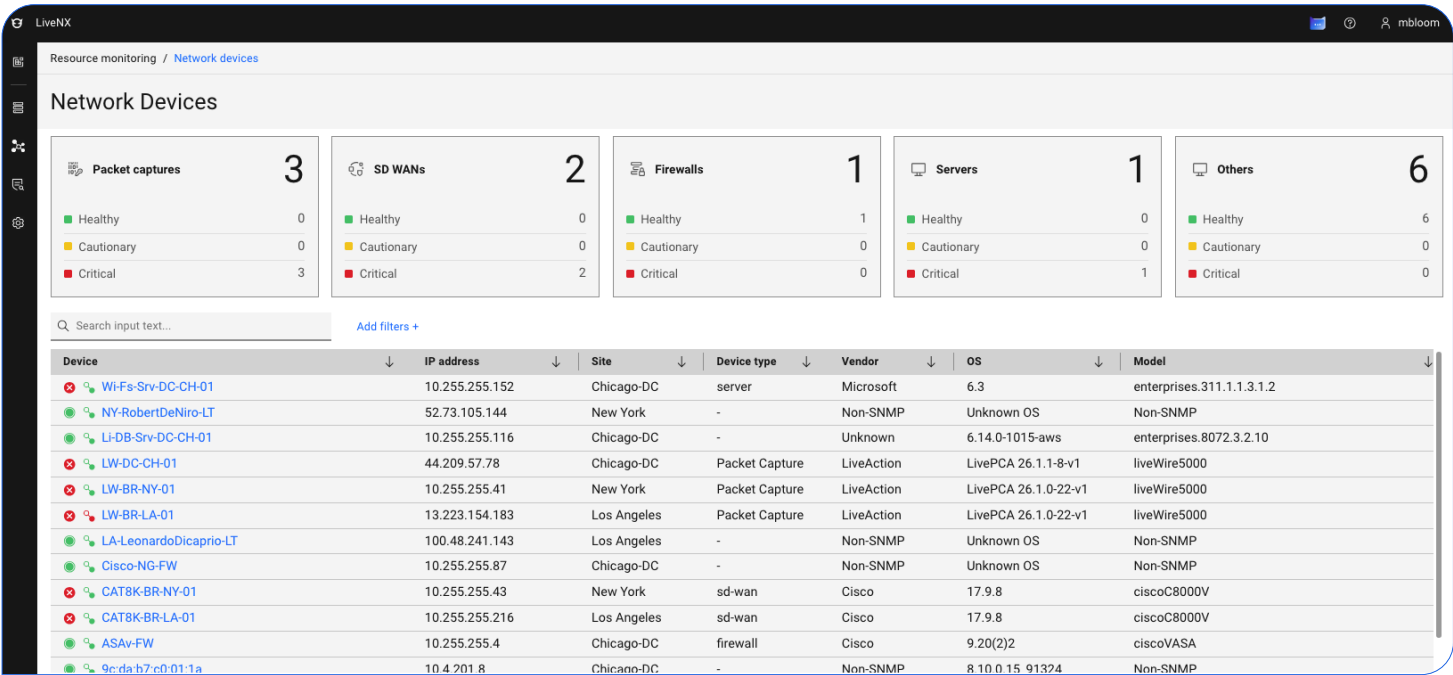


Figure 1. Network Resource Monitoring network devices dashboard

Outcome: Significant gains in productivity, reduced manual overhead, and accurate, up-to-date network intelligence. Network teams can reallocate resources to higher-value initiatives such as optimization, capacity planning, and strategic modernization.

Use case 2: Proactive outage prevention

Most network teams still operate in a reactive mode, responding to alerts only after users report performance degradation. Network Resource Monitoring changes this by continuously monitoring key device health metrics, including CPU, memory, temperature, and interface utilization. When anomalies arise, Network Resource Monitoring automatically correlates them with network performance trends in LiveNX, highlighting at-risk components before they fail. Instead of chasing complaints, NetOps teams can proactively remediate issues—from overworked switches to unstable access points—before they escalate into outages.

Outcome: Reduced downtime, faster detection of emerging problems, and improved end-user experiences. Enterprises can move from reactive firefighting to preventive operations that protect uptime and service quality.

Use case 3: Smarter capacity planning

Without visibility into device utilization and performance trends, many organizations either over-provision resources or experience unexpected bottlenecks. Network Resource Monitoring feeds continuous telemetry data into LiveNX's traffic analysis feature. The AI capabilities of LiveAssist, a separate AI-powered analytics add-on for LiveNX, correlates data for trend analysis. This allows teams to forecast demand, identify capacity risks, and confidently plan upgrades. Historical data helps predict when a router's throughput will reach its limit or when a wireless controller will need to be expanded.

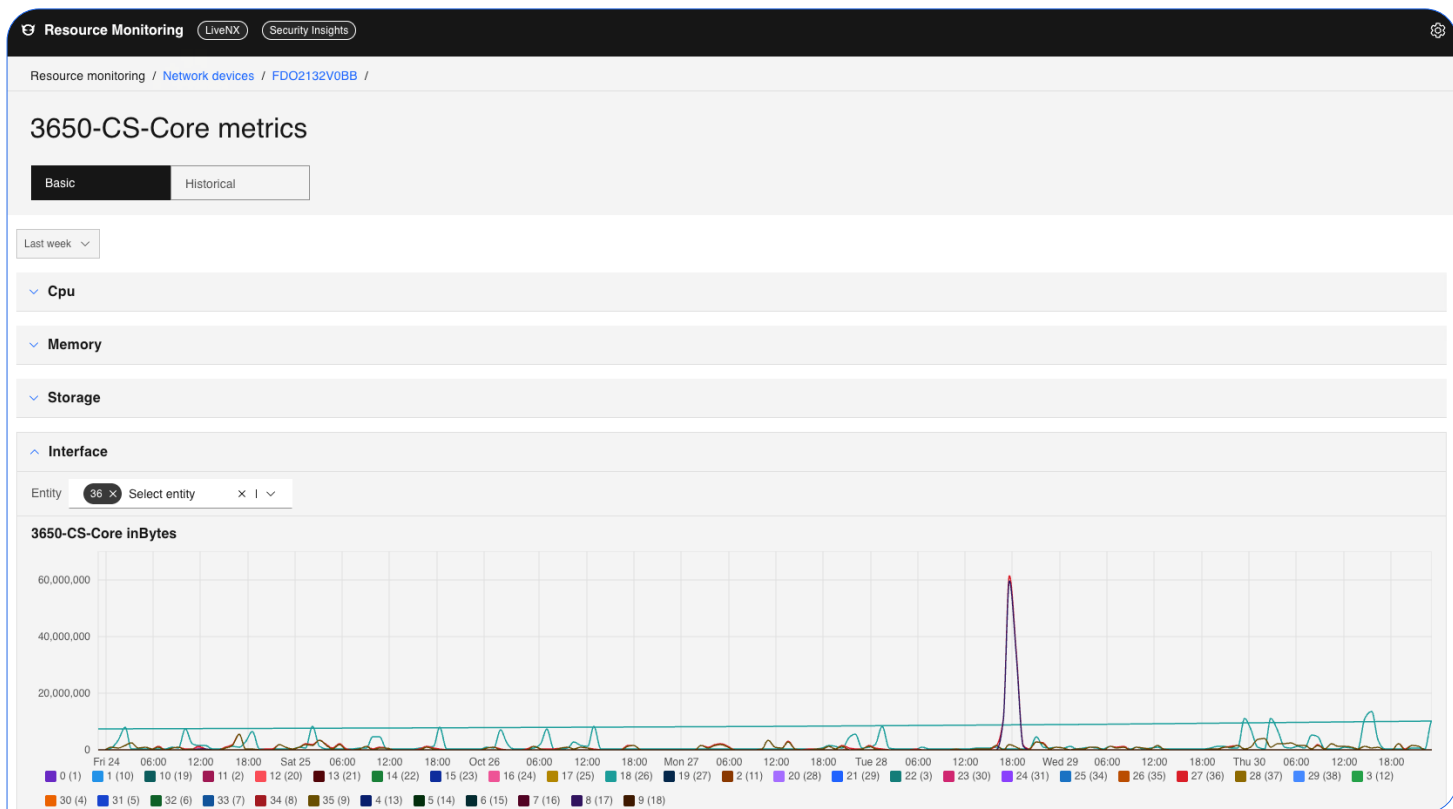


Figure 2. Network Resource Monitoring device metrics dashboard

These insights also feed into budget and resource planning, ensuring investments are data-driven rather than reactive.

Outcome: Optimized capacity and cost management. Network teams avoid overspending on unnecessary infrastructure while preventing performance degradation from under-provisioned resources.

Use case 4: Unified device and flow visibility

Enterprises managing complex hybrid environments often rely on multiple disconnected tools: one for device health, another for traffic analysis, and a third for application performance. This fragmentation creates blind spots and slows troubleshooting. With Network Resource Monitoring, LiveNX becomes the single pane of glass for both network and infrastructure insight. Device telemetry collected through SNMP and APIs is automatically correlated with LiveNX's flow analytics and topology views. Teams can instantly see how a failing router interface or overloaded switch affects traffic paths and application delivery.

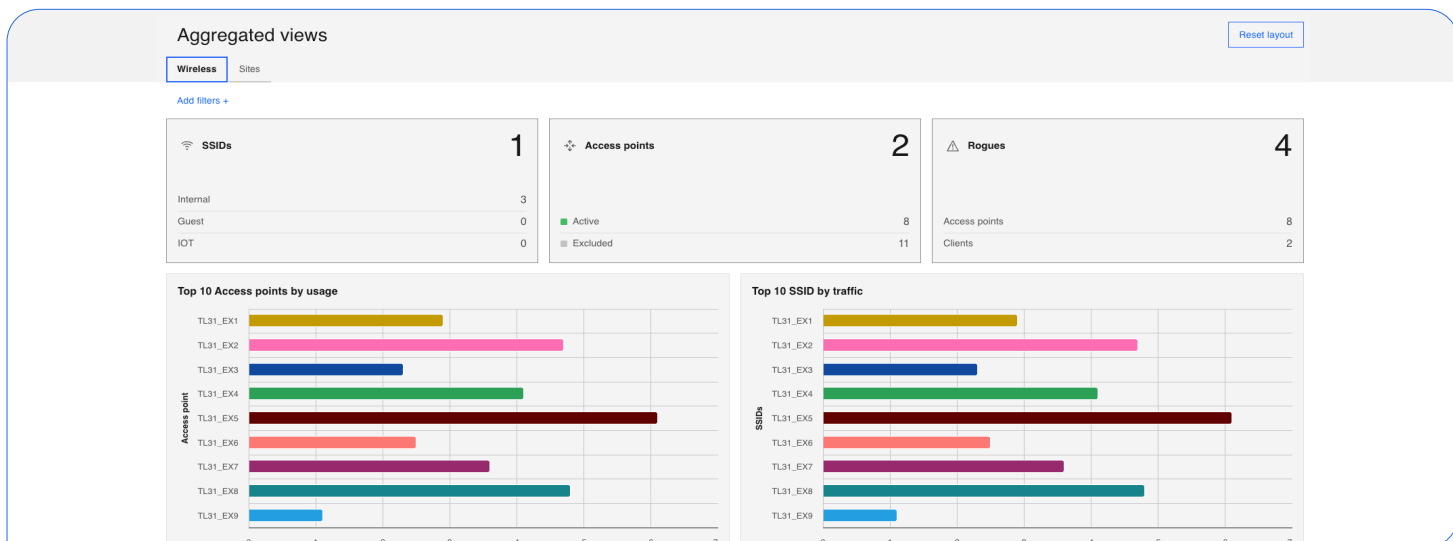


Figure 3. LiveNX dashboard showing unified device flow and visibility between network and infrastructure

Outcome: End-to-end visibility that bridges the gap between devices, flows, and applications. By consolidating toolsets, teams reduce MTTR, eliminate redundant systems, and operate from a unified, trustworthy source of truth.

Use case 5: Simplified multi-vendor operations

Large enterprises rarely operate in single-vendor environments. A typical hybrid network might include Cisco and Arista switches, Aruba wireless infrastructure, and Nokia service aggregation routers. Each vendor’s tools produce data in different formats, leading to inconsistent visibility and analysis. Network Resource Monitoring unifies multi-vendor telemetry on a single platform, normalizes SNMP and API data from diverse sources, and correlates it with flow and topology intelligence in LiveNX. This ensures teams can compare device performance side by side and apply consistent monitoring policies across environments.

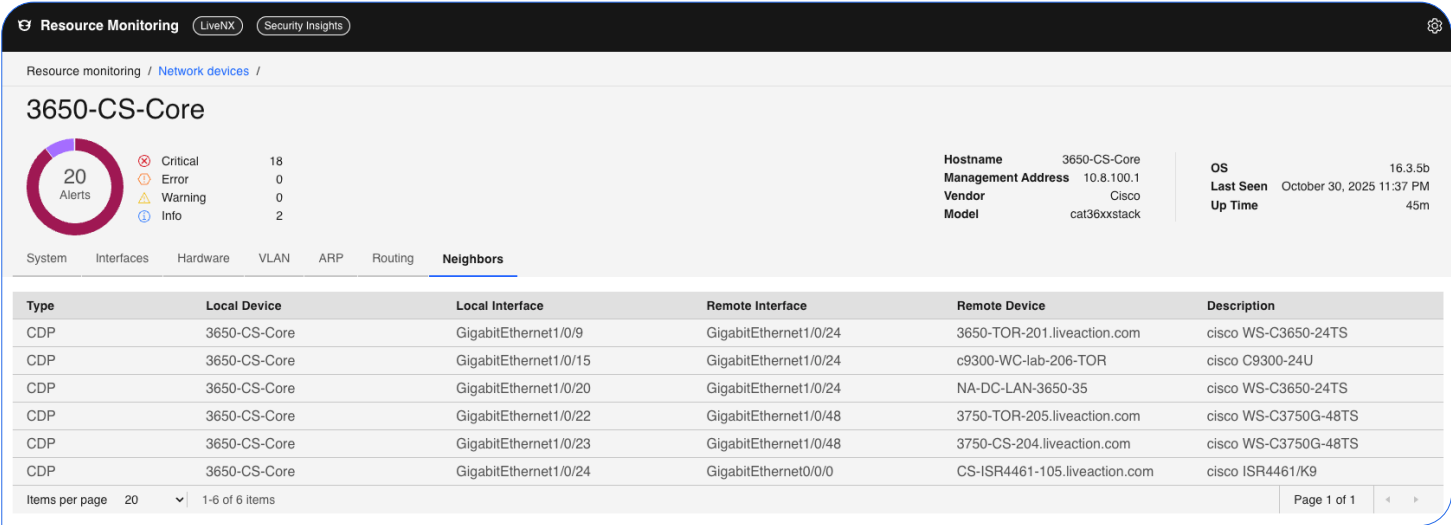


Figure 4. Network Resource Monitoring dashboard showing neighboring Cisco network devices

Outcome: Seamless cross-vendor visibility and operational consistency. Teams spend less time reconciling data across systems and more time optimizing performance and reliability.

Key differentiators

Network Resource Monitoring isn’t just another SNMP polling tool—it’s a device observability engine built to extend LiveNX’s full-stack intelligence. It stands apart due to its unique combination of:

- Operational data foundation:** Network Resource Monitoring serves as the primary source of operational infrastructure data for BlueCat’s network observability platform, continuously collecting rich operational information across routing, switching, wireless, firewalls, load balancers, alerts, logs, and operational state.
- Rich operational context:** Network Resource Monitoring captures far more than infrastructure health. It continuously builds operational context describing infrastructure state, service health, routing behavior, wireless connectivity, and critical network services.
- AI-powered:** Leveraging Network Resource Monitoring’s rich operational context, LiveAssist helps engineers investigate issues using natural language, identify root causes, and accelerate troubleshooting through AI-assisted recommendations.
- Intelligent alerting:** Infrastructure alerts become significantly more valuable when viewed alongside operational state, routing information, network traffic, and topology. This contextual approach reduces alert fatigue and accelerates troubleshooting.
- Open multi-vendor architecture:** Network Resource Monitoring provides consistent operational visibility across heterogeneous environments, including Cisco, Arista, Aruba, Nokia, F5, Palo Alto Networks, Fortinet, and other supported platforms.

Solution benefits

Network resource monitoring enables IT teams to ensure availability, reduce risk, control costs, and deliver better user experiences by providing continuous, actionable insight into infrastructure health and utilization. Key benefits include:

- ✓ **Improved performance and availability**
Monitoring of core devices and key performance metrics complements LiveNX's network-centric observability, enabling proactive detection of bottlenecks and ensuring higher uptime.
- ✓ **Optimized capacity and cost management**
LiveAssist's trend analysis of device information that is sent from Network Resource Monitoring to LiveNX supports capacity planning, bandwidth optimization, and over-provisioning prevention—reducing both outages and unnecessary spending.
- ✓ **Operational efficiency**
Automated discovery, telemetry collection, and alerting minimize manual effort, allowing teams to focus on strategic initiatives and boost productivity.
- ✓ **Proactive operations**
Detection and prevention of device-level failures before users are impacted.
- ✓ **Hybrid and multi-vendor visibility**
Unified monitoring across on-premises, SD-WAN, wireless, and cloud devices from multiple vendors—including switches, routers, and wireless access controllers from Arista, Cisco, Aruba, and Nokia—ensures consistent visibility across complex environments.
- ✓ **AI-powered intelligence**
Every metric collected by Network Resource Monitoring is sent to LiveNX. There, with the help of LiveAssist, you can ask natural-language questions and receive real-time insights, intelligent alerts, and root cause assistance to streamline troubleshooting and optimize performance.

BlueCat's Intelligent Network Operations (NetOps) solutions provide the analytics and intelligence needed to enable, optimize, and secure the network to achieve business goals. With an Intelligent NetOps suite, organizations can more easily change and modernize the network as business requirements demand.

Headquarters

4100 Yonge St. 3rd Floor, Toronto, ON, M2P 2B5
Phone: 1-416-646-8400 | 1-866-895-6931

bluecat.com

Next steps

Learn how you can combine device health data with flow analytics to create end-to-end network visibility.

[Contact us](#)