Solutions Brief

Network Observability

AI-Driven Intelligence for Network Operations

June 2026

The Challenge: Network Observability Hasn't Kept Pace with Network Complexity

Modern networks no longer look anything like the architectures legacy monitoring tools were built for. Today's environments span on-premises infrastructure, multi-cloud services, SD-WAN, WiFi, optical transport, and edge devices — all generating metrics, logs, flows, and events around the clock. Operations teams are expected to keep all of it running smoothly, but most are working with tools that were never designed for this level of scale or complexity.

The result is a familiar and costly pattern:

- **Tool sprawl and siloed data:** Network, infrastructure, and application teams each rely on their own monitoring stack, leaving no single, correlated view of what's actually happening across the environment.
- **Alert fatigue:** Thousands of disconnected, duplicate, or low-value alerts bury the handful that actually matter, and on-call engineers spend more time triaging noise than fixing problems.
- **Manual root cause analysis**: When something breaks, engineers are pulled into war rooms to manually cross-reference dashboards, logs, and tickets across multiple tools just to find where a problem started.
- **Reactive operations**: Without predictive insight or historical context, teams are stuck responding to outages after customers are already affected, rather than catching the early signals beforehand.
- **Rising MTTR and operational cost:** Every hour spent hunting for root cause is an hour of degraded service, lost productivity, and mounting pressure on already-stretched operations teams.

These challenges compound as environments grow. Traditional, rules-based monitoring platforms require thousands of static thresholds and manual correlation logic just to keep up — an approach that breaks down the moment network and application architectures evolve faster than the rules written to monitor them.

How Selector Helps

Selector is an AI-driven observability and event intelligence platform purpose-built for complex, modern IT environments. Rather than adding another siloed monitoring tool to the stack, Selector unifies telemetry, metrics, logs, flow data, and events from across the entire network and IT ecosystem, correlates them in real time using AI and machine learning, and surfaces the insights that actually matter.

Selector acts as a force multiplier for network and IT operations teams — helping them detect, diagnose, and resolve incidents in minutes rather than hours, while proactively identifying risk before it becomes downtime. Critically, Selector is designed to enhance existing workflows and tool investments rather than replace them, meeting teams where they already work.

Unify

Bring metrics, logs, flows, topology, and events from across the full stack into a unified operational data layer.

Correlate

Apply AI/ML to connect related signals across domains, time, and topology — automatically.

Prioritize

Deduplicate and rank events by impact, cutting through alert noise to surface what matters.

Resolve

Accelerate root cause analysis and remediation with GenAI Copilot and automated workflows.

Selector vs. Legacy Monitoring and the Competition

Legacy monitoring tools and many point observability solutions — including the SolarWinds, LogicMonitor, and BigPanda-style platforms common in enterprise environments — were built for a previous generation of static, siloed architectures. They typically rely on rule-based thresholds, manual dashboard correlation, and narrow, single-domain visibility. Selector takes a fundamentally different approach:

AI-native, not rules-based

Where legacy platforms require thousands of manually written and maintained regex patterns and static thresholds, Selector uses machine learning to automatically baseline normal behavior (accounting for time-of-day and seasonal cyclicity), detect anomalies, and extract meaning from unstructured logs — without an army of engineers tuning rules.

Automated correlation vs. manual triage

Incident investigation with legacy tools relies heavily on engineers manually cross-referencing dashboards across multiple systems to confirm anomalies. Selector's correlation engine runs continuously in the background, connecting metrics, logs, events, and topology — temporally and contextually — to tell the story of what happened, when, and why, automatically.

True full-stack visibility, not point solutions

Many competing tools specialize in a single domain — network, application, or infrastructure — forcing teams to stitch together visibility themselves. Selector delivers correlated visibility across the full operational path, spanning network, infrastructure, applications, SD-WAN, WiFi, optical, and cloud in one platform.

A living Digital Twin and historical DVR, not static diagrams

Legacy topology views are typically static and manually maintained. Selector continuously builds and updates a live Digital Twin of the environment, paired with Network DVR — the ability to rewind and replay historical network and device states for deep post-incident analysis.

Conversational AI, not rigid query languages

Rather than requiring engineers to learn proprietary query syntax, Selector's GenAI Copilot — powered by a purpose-built Network Language Model (NLM) — lets anyone ask questions in plain language and get expert-level answers, visualizations, and guided remediation steps.

Open and extensible, not closed

Selector is designed to plug into the tools organizations already use — ServiceNow, Splunk, PagerDuty, Slack, AWS, and hundreds of others — enhancing existing workflows rather than forcing a rip-and-replace.

Capability	Legacy Monitoring Tools	Selector
Data sources	Siloed, single-domain tools	Unified ingestion across network, infra, cloud, apps, and logs
Stack coverage	Partial visibility — typically one OSI layer or domain	True full-stack visibility from L1 to L7, including SD-WAN, WiFi, and optical
Detection method	Static, manually-tuned thresholds and rules	ML-driven baselining that learns time-of-day and seasonal patterns automatically
Root cause analysis	Manual correlation across multiple dashboards and tools	Automated, AI-driven RCA that pinpoints the source in seconds
Alert handling	Alert storms with high noise and duplication	Correlated, prioritized incidents that cut noise and surface what matters
Event correlation	Limited or rule-based; struggles across domains	Temporal, contextual, and topology-aware correlation across all domains
Log analysis	Search and regex patterns that must be hand-maintained	ML-based log mining that clusters and extracts entities without regex rules
Topology awareness	Static diagrams, manually updated and quickly stale	Live Operational Twin, continuously updated from real-time telemetry
Historical analysis	Limited retention or no replay capability	Network DVR with historical replay of states, alerts, and topology.
User experience	Dashboards, queries, and manual investigation across tools	Natural language GenAI Copilot, powered by a purpose-built Network LLM
Predictive insight	Reactive; issues surface only after impact	Predictive 'what-if' analytics and forecasting that flag risk early
Remediation	Manual hand-offs and runbooks	Guided remediation with auto-create / auto-resolve ticketing workflows
Extensibility	Closed or narrow, vendor-locked integration sets	Open, API-first ecosystem with broad, vendor-agnostic integrations
Deployment	Lengthy, appliance-bound rollouts	Kubernetes-native, deployable on-prem, in your cloud, or as SaaS

Key Use Cases

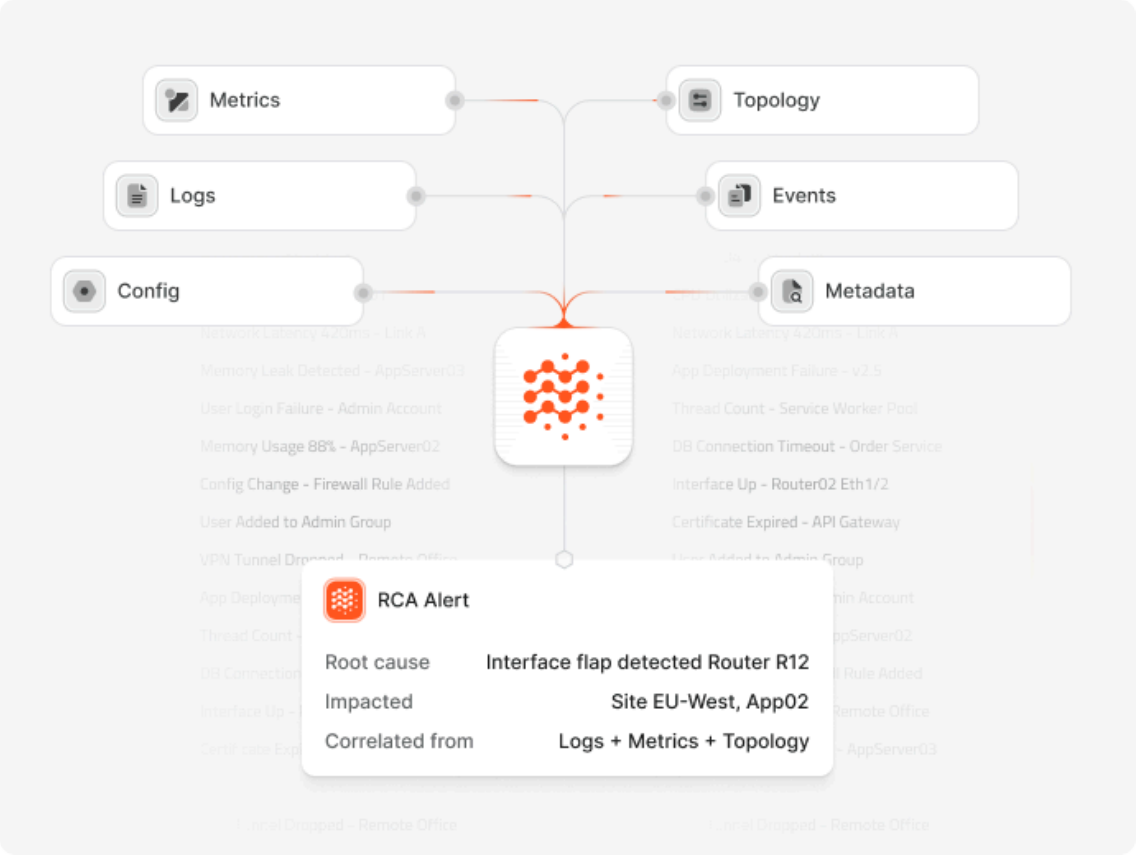
Selector supports a broad range of operational use cases across the network and IT stack — all built on the same unified data and correlation foundation.

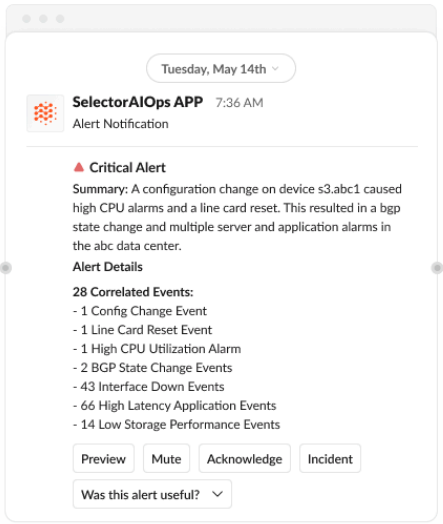
Incident Management & Noise Reduction	Correlates multi-domain alerts and events into deduplicated, ranked, actionable incidents, and automatically syncs them with ITSM and ticketing platforms.
Full Stack OSI Visibility (L1–L7)	Delivers observability from physical links to applications, with KPI tracking for availability, latency, error rates, and throughput.
Digital Twin	Maintains a continuously updated, real-time model of the network and infrastructure stack for accurate operational awareness.
Network DVR — Historical Playback	Provides timeline-based, interactive playback of historical device states, alerts, and telemetry for deep post-incident root cause analysis.
AI-Driven Troubleshooting with GenAI Copilot	Enables natural language queries, ad-hoc visualizations, and guided remediation through Selector's Network Language Model (NLM).
Control Plane, Routing & Topology Analytics	Provides real-time and historical visibility into BGP, IGP, and other routing protocols, with topology-aware anomaly detection.
Performance Synthetics & Analytics	Simulates real-world user interactions and validates end-to-end service health and SLA performance.
Device Health Analytics	Monitors routers, firewalls, switches, wireless devices, load balancers, and more, with auto-discovery and anomaly detection.
ITSM Integration, Ticketing & Analytics	Automates ticket creation, enrichment, and resolution through ServiceNow and CMDB integrations, with full workflow analytics.
SD-WAN Analytics	Correlates overlay and underlay telemetry across vendor-agnostic SD-WAN deployments to surface performance anomalies.
WiFi Analytics	Tracks wireless performance and signal strength, correlating user-facing issues with underlying WiFi or WAN conditions.
CPE & Optical Analytics	Monitors customer-premises equipment and optical network health, mapping systemic failures and flagging early degradation signals.

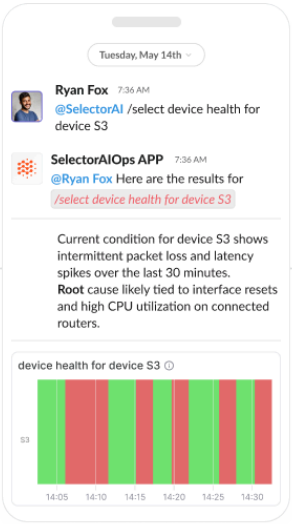
Key Capabilities & Features

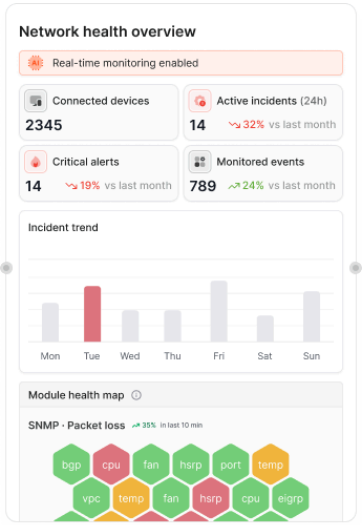
AI-Powered Incident Management

- Multi-domain event correlation that connects alerts and events across systems into contextualized, actionable incidents.
- Intelligent prioritization that deduplicates, enriches, and ranks events by business impact to cut alert fatigue.
- Knowledge graph analysis that computes correlation graphs and clusters incidents to reveal hidden relationships.
- Automated incident resolution for recurring issues, with auto-create and auto-resolve ticketing workflows.



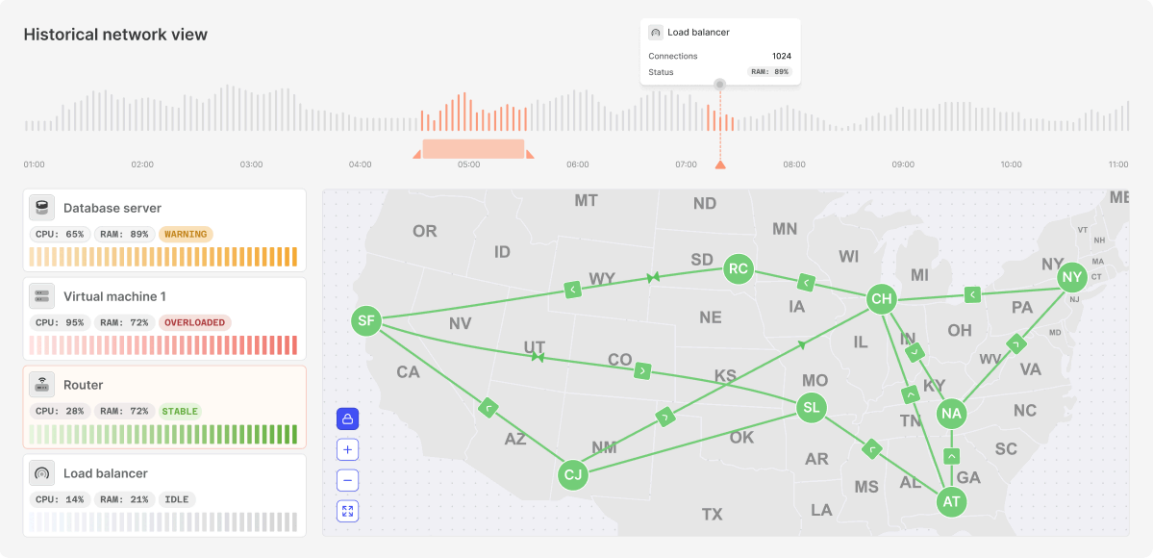






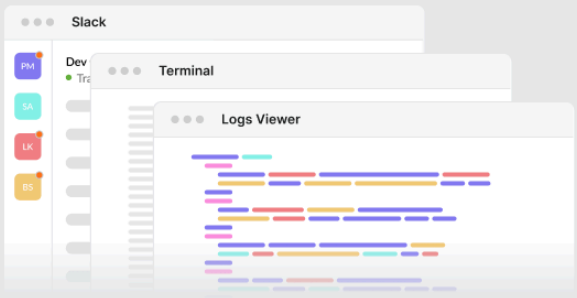
Operational Twin & Network DVR

- Continuous, real-time topology mapping enriched with live telemetry from every layer of the stack.
- Interactive drill-downs into infrastructure, network, and service layers.
- Time-slider navigation to step back in time and replay historical device states and conditions.
- Timeline-based root cause analysis to pinpoint and diagnose recurring issues.



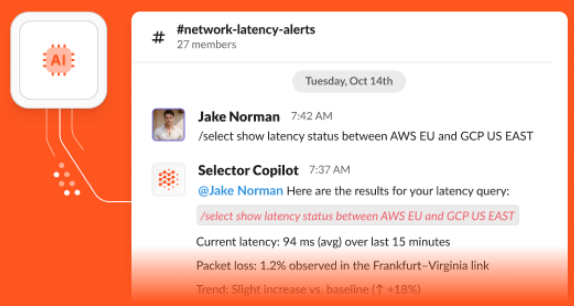
GenAI Copilot & Network Language Model

- Natural language interface for ad-hoc queries against telemetry, logs, and alerts.
- Expert-level guidance and analysis powered by Selector's proprietary Network LLM (NLM).
- On-demand, ad-hoc visualization generation for faster troubleshooting.
- AI-powered guided remediation recommendations that accelerate resolution.



Without Copilot

Manually search logs, switch between tools, and waste time piecing together symptoms and causes.

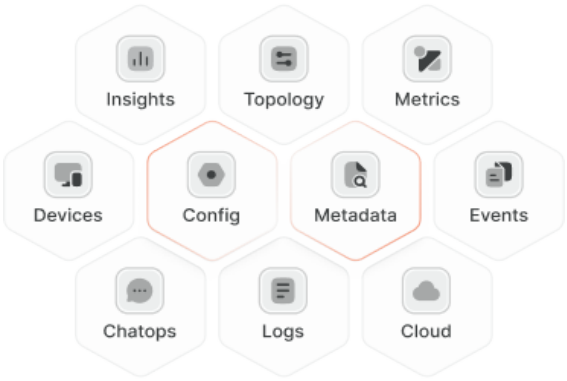


With Copilot

Ask one question and instantly get root cause, timeline insights, and recommended actions — all in one view.

Full-Stack Data Collection & Correlation

- Protocol-agnostic telemetry collection via SNMP, gNMI/gRPC, NetFlow/IPFIX, BGP, Syslog, streaming telemetry, and more.
- Device auto-discovery with customizable collection profiles and CMDB/inventory integration.
- ML-driven log mining that clusters and extracts structured meaning from raw logs without manual regex rules.
- ML-driven baselining that accounts for time-of-day and seasonal patterns to flag genuine anomalies.



Open, Extensible Integration Ecosystem

- **Operational data from network equipment**: Routers & switches (Juniper, Cisco, Arista, Ciena), infrastructure (VMware, Kubernetes), CMDB (Netbox, Nautobot, Infoblox), SD-WAN (Cisco Meraki, Palo Alto CloudGenix), and WLAN (Cisco Prime).
- **Real-time traffic insights & synthetic probes:** Cisco ThousandEyes, Pingmesh, Traceroute, and custom synthetic probes.
- **Logs**: Splunk, native Syslog, TACACS logs, and Logstash.
- **Automation & workflow:** ServiceNow, RunDeck, PagerDuty, Bitbucket, Jira, Itential, and SolarWinds.
- **Alerting & collaboration:** BigPanda, ScienceLogic, PagerDuty, Opsgenie, Slack, and Microsoft Teams.
- **Public cloud & application monitoring**: AWS SQS, AWS CloudWatch, and Dynatrace.
- **Identity & event streaming**: Okta, Ping Identity, Azure AD, Kafka, and file-based ingest (CSV, Excel, Google Sheets).

Key Benefits & Outcomes

Organizations that adopt Selector see measurable improvements in how quickly they detect, diagnose, and resolve issues — and in how much operational burden their teams carry day to day.

Faster MTTR

Automated correlation and root cause analysis collapse alert storms into clear, actionable insights — cutting mean time to detect, identify, and repair.

Fewer, Better Alerts

Deduplication and intelligent prioritization mean engineers see the incidents that matter, not thousands of disconnected notifications.

Proactive Operations

Anomaly detection and predictive 'what-if' analytics help teams catch and address risk before it affects end users.

Reduced Operator Fatigue

Less time spent triaging noise across siloed tools means more time spent on optimization and strategic work.

Tool & Vendor Consolidation

A single, correlated platform reduces the need for multiple overlapping monitoring tools — and the cost that comes with them.

Faster Time to Value

Open, API-first integrations mean Selector plugs into existing workflows and tools quickly, without operational disruption.

The Bottom Line

Network observability shouldn't mean stitching together a dozen siloed tools and hoping an engineer can connect the dots before customers feel the impact. Selector brings full-stack visibility, AI-driven correlation, and natural language troubleshooting into a single platform so operations teams spend less time hunting through dashboards and more time keeping services healthy.

Unlike legacy monitoring and point observability tools, Selector is AI-native from the ground up: it learns what normal looks like, surfaces the few incidents that matter out of thousands of raw signals, and points teams straight to root cause. And because it's open and extensible, it enhances the tools and workflows you already rely on rather than forcing a rip-and-replace.

85%	95%	10x	70%
Lower MTTR	Noise reduction	Faster RCA	Fewer incidents

See how Selector delivers AI-driven operational intelligence across your network

Request a Demo

www.selector.ai | sales@selector.ai