

Case Study:

Beyond the “Up/Down” Ping: How Context-Aware AI Transformed Operations for a Tier-1 MSP

Executive Summary

For many Managed Service Providers (MSPs), the challenge isn't a lack of data—it's an overwhelming flood of it. **A Mid-Market Managed Service Provider** managing over 150 client sites across a multi-vendor stack (Cisco Meraki, Fortinet, and legacy SNMP devices), found themselves trapped in a cycle of reactive "firefighting."

By implementing NetOp AI, they shifted from managing thousands of disconnected alerts to resolving **Compound Incidents** with full root-cause context. The result was a 65% reduction in Mean Time to Repair (MTTR) and the ability to scale their client base by 30% without adding a single headcount.

The Client Profile

Company: A Mid-Market MSP

Focus: Managed IT and Connectivity for Healthcare and Retail

Infrastructure: Hybrid (Cloud-managed and on-premise), Multi-vendor

Challenge: Alert fatigue and high escalation costs due to lack of diagnostic context.

Challenge: The “Needle in a Haystack” Problem

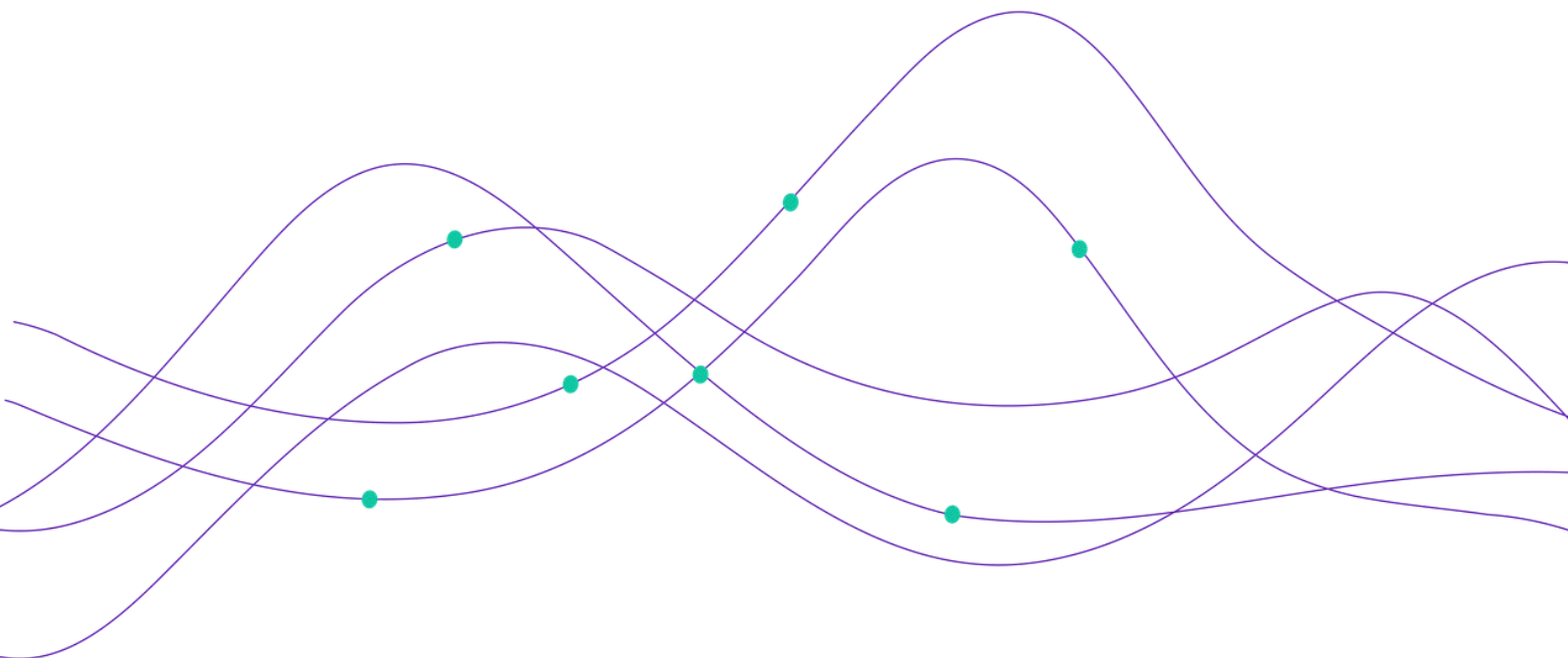
This MSP was successful, but their operational margins were thinning. Their NOC (Network Operations Center) was receiving over 2,000 alerts daily. Most of these were "pings" indicating a device was down or latency was high, but they provided no "Why."

The team faced three critical hurdles:

1. **Alert Fatigue:** Technicians spent 40% of their day filtering out "noise" (e.g., a momentary ISP blip or a scheduled reboot).
2. **Siloed Visibility:** Jumping between the Meraki Dashboard, Fortinet logs, and SNMP tools meant they couldn't see how an issue in one layer affected another.
3. **The Context Gap:** A "Device Down" alert didn't tell them if it was a bad cable, a VLAN mismatch, or a power failure. This led to "blind" onsite dispatches that were often unnecessary or lacked the right equipment.

We weren't just monitoring networks; we were drowning in data. We knew something was wrong, but we didn't know where to start until the client had already called to complain."

— **VP of Operations of Mid-Market MSP**

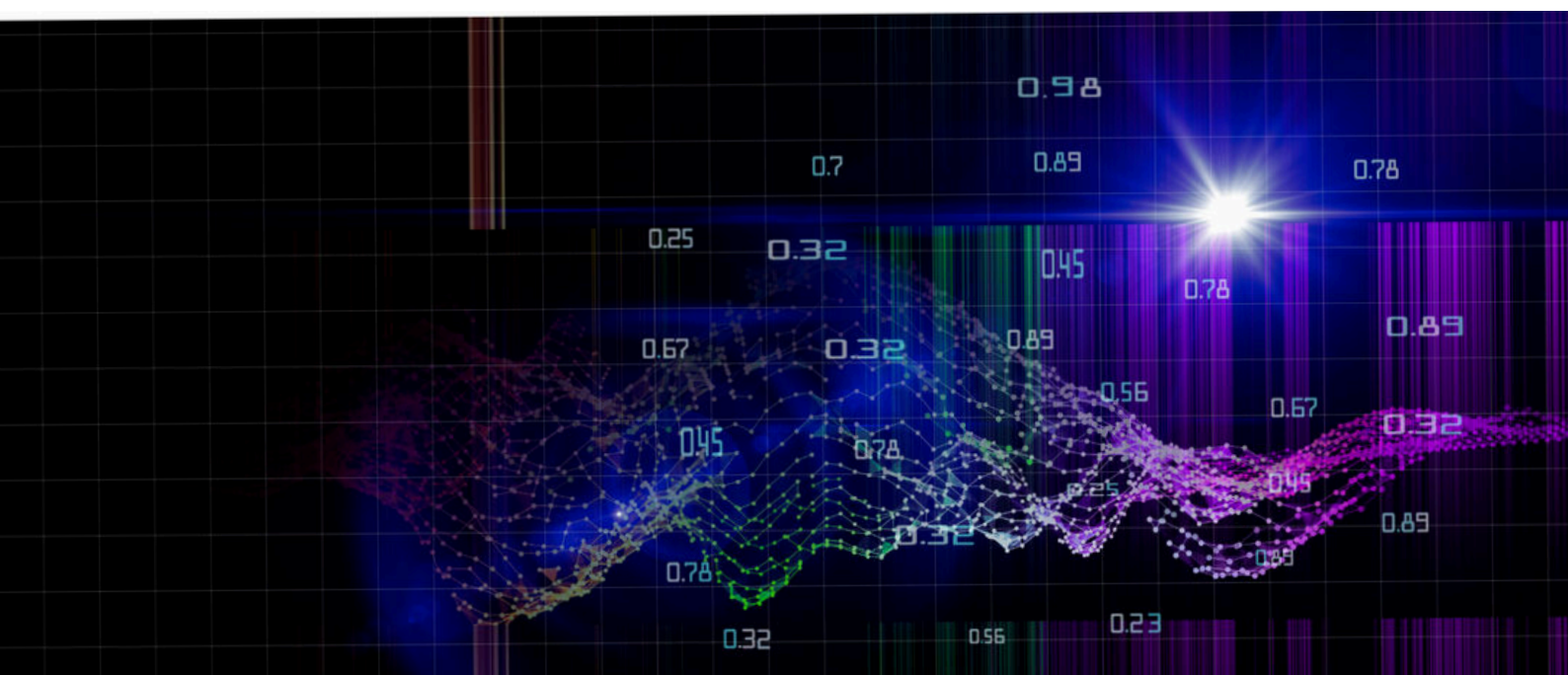


NetOp's Solution

To address these critical issues, the MSP team deployed NetOp AI to sit across their entire infrastructure. Unlike traditional NMS tools that report on individual status, NetOp's AI engine began correlating anomalies into Compound Incidents.

Key Features Implemented:

- **Automated Root Cause Analysis (RCA):** Instead of reporting "Access Point Down," NetOp identified that the underlying switch port had experienced an error, pinpointing a physical problem as the source.
- **Predictive Anomaly Detection:** NetOp identified "brownout" patterns—minor performance dips that precede a total outage—allowing the MSP to intervene during business hours before a failure occurred.
- **Cross-Vendor Correlation:** By unifying data from Meraki and Fortinet, NetOp provided a holistic topology view that showed exactly how a configuration change on a firewall was impacting Wi-Fi performance at the edge.



The Transformation: Context is the Multiplier

The "huge difference" for the MSP team came down to the context behind the alert. In one instance, a major healthcare client experienced intermittent VoIP dropping. Traditional tools showed "High Latency" but no hardware failure. NetOp AI analyzed the historical patterns and correlated the latency spikes with a specific ISP routing change and a saturated uplink on a secondary switch. NetOp provided the "Fix-It" Blueprint: Instead of a generic alert, the technician received a dashboard notification that said:

*"High Latency on VoIP VLAN 10. Cause: Uplink saturation on Switch-04.
Recommended Action: Adjust QoS tagging or move non-critical traffic to secondary WAN."*

This level of detail allowed a Tier-1 technician to solve an issue that would previously have required a high-cost Tier-3 engineer.

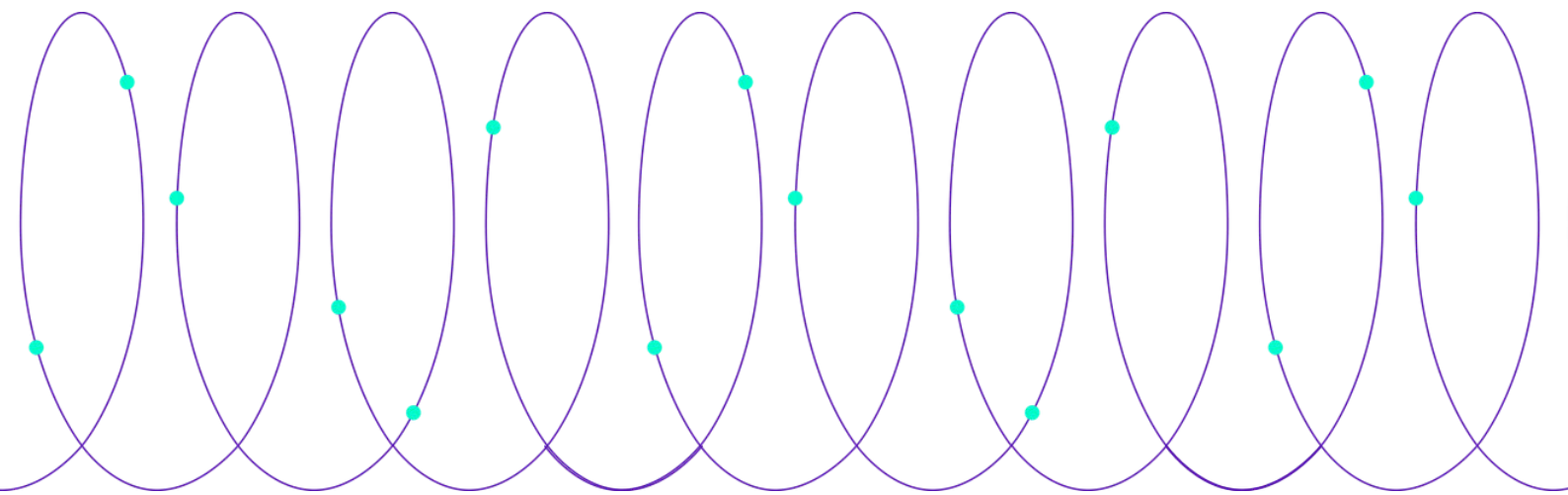
The Results: Scaling with Intelligence

Within six months of deploying NetOp AI, the MSP team saw a fundamental shift in their business health:

- **90% Noise Reduction:** By grouping hundreds of related pings into single Compound Incidents, the NOC team could focus on issues that mattered.
- **65% Faster MTTR:** With the "Why" provided upfront, troubleshooting time dropped from hours to minutes.
- **Proactive "First-to-Know":** In 85% of cases, the MSP team resolved the issue before the client even realized there was a problem, significantly boosting CSAT (Customer Satisfaction) scores.
- **Operational Efficiency:** The MSP successfully onboarded 40 new sites without hiring additional engineers, as the existing team was no longer bogged down by manual data correlation.

Conclusion

For MSPs, NetOp AI isn't just another monitoring tool—it's a force multiplier. By providing the context behind every alert, NetOp allows service providers to stop "stumbling in the dark" and start delivering the proactive, expert service their clients expect.



Why NetOp?

NetOp's AI-driven platform is purpose-built for MSPs managing complex, multi-site networks. The solution automates analysis and provides actionable intelligence, enabling MSPs like Astaris to focus on delivering exceptional service rather than manually sifting through raw data. NetOp makes network operations more accessible, scalable, and effective, helping MSPs save time, improve service quality, and unlock new business opportunities.