KORE-TEK PERSPECTIVE

The AIOps and Managed NOC Convergence

Why the smartest enterprises and service providers are pairing customer-owned AIOps with managed network operations, and retiring the tool sprawl that drains budgets and attention alike.

Executive Summary

AIOps has been marketed to the enterprise and service providers as a replacement technology for monitoring platforms, operations teams, and, increasingly, managed service providers. That framing is wrong, and it is costing CIOs and CTOs real money while delivering disappointing results.

The honest strategic picture is this: AIOps is a powerful aggregation, correlation, and insight layer. A managed Network Operations Center is a 24x7 execution arm. These two capabilities are complementary, not competitive. The enterprises that get the most leverage from both have stopped asking "AIOps or NOC?" and started asking "How do we architect these to reinforce each other?"

This paper presents a C-suite view of that convergence. We address three realities that every technology leader is grappling with right now: the operational drag caused by a decade of tool sprawl and alert noise; the sunk-cost trap that keeps organizations paying for overlapping capex and opex across homegrown and vendor-specific monitoring stacks; and the SLA blind spot that leaves customers dependent on their provider's performance reporting.

Our position is direct. A customer-owned AIOps layer, built on top of, not instead of, a mature managed NOC relationship, produces better uptime, faster mean time to

resolution, a defensible TCO story, and something most enterprises have never had before: genuine leverage over their own operational data.

The Architecture, at a Glance

Before getting into the operational realities and the financial case, it helps to see the architecture. The diagram below shows the three tiers: the existing monitoring stack at the bottom, a customer-owned AIOps aggregation layer in the middle, and the two parallel outputs above it, customer insight and managed NOC execution, feeding each other rather than competing.

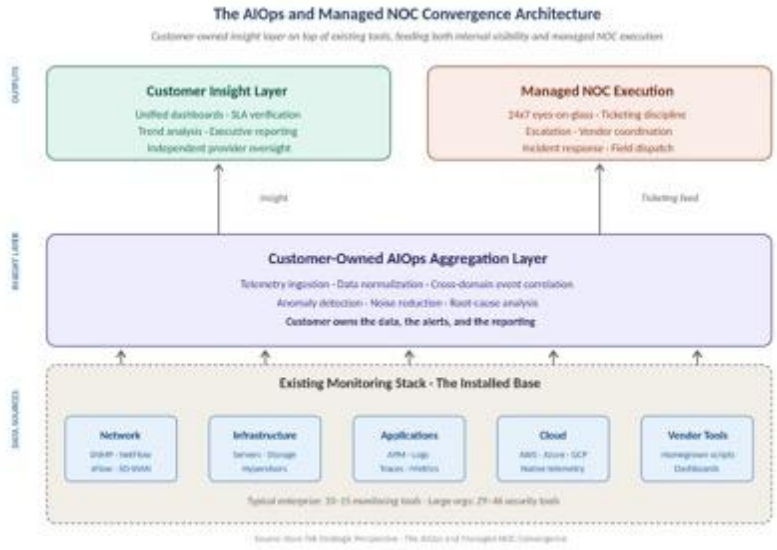

Figure 1. *The AIOps and managed NOC convergence architecture. The customer-owned insight layer sits on top of the existing tool stack and feeds both internal visibility and managed NOC execution.*

Part One: The Operational Reality in the Network

Tool sprawl has quietly become a balance-sheet problem

Ask most CIOs how many monitoring and observability tools run in their environment, and the honest answer is "we're not sure." Industry data tells a consistent story. The average network now operates 10 to 15 separate monitoring solutions spanning networks, servers, applications, cloud resources, and databases. In larger organizations, the number of security monitoring tools alone can reach 46(1). Each tool has its own license, alerting logic, incident definition, and dashboard(2).

None of those decisions was bad in isolation. Each tool was purchased for a reason: a vendor recommendation, a compliance requirement, a gap exposed by a specific outage, or a capability added through acquisition. Over ten years, however, these individual decisions have created an environment in which no single team, and often no single platform, can answer a basic question: what is actually happening across our network right now?

Alert fatigue is a symptom, not the disease

The volume of alerts in a modern enterprise environment has reached a point where human triage is mathematically impossible. Research from multiple industry sources estimates the daily alert volume for an enterprise or service provider SOC at roughly 3,000 to 4,500 events, with 63 to 67 percent going unaddressed(3). Observability research tells a parallel story on the operations side: 73 percent of organizations still lack full-stack observability, and 41 percent of IT leaders first learn about service interruptions through customer complaints, incident tickets, or manual checks, rather than from their monitoring stack(4).

The root cause is not that alerts are too loud. It is that they lack context. Each tool sees only a narrow slice of the environment. When a network event triggers an application failure, engineers must switch between dashboards, manually correlate timestamps, and reconstruct a timeline across systems that were never designed to communicate.

The first 30 minutes of every significant incident are typically spent assembling a picture of what happened rather than fixing the issue.

> *The real cost of tool sprawl does not appear on any licensing invoice. It appears in the half-hour your on-call engineer spends figuring out which of twelve dashboards holds the signal.*

The NOC alerting and reporting gap

Enterprises and service providers that have outsourced NOC operations face a related but distinct problem. A managed NOC provides the 24x7 eyes-on-glass, ticketing discipline, and escalation structure that are uneconomical to staff internally. But the visibility a customer has into that provider's performance is almost entirely mediated by the provider.

Monthly SLA reports arrive as PDFs. Where they exist, dashboards are read-only windows into the provider's ticketing system. Key operational realities, such as whether alerts were suppressed, how tickets were classified, and whether recurring issues are being root-caused or just repeatedly closed, are difficult to verify independently(5). This is not a matter of provider integrity. It is a structural problem: the customer does not own the data layer that would let them answer these questions for themselves.

The result is a relationship built on trust rather than on evidence. That works until it doesn't.

The CapEx and OpEx trap

Beneath all of this lies a financial reality that most technology leaders recognize but few have solved. Capital expenditures in network monitoring tend to be sticky. Hardware appliances, perpetual licenses, and integration projects depreciate over three to five years, and organizations are reluctant to write off investments before they are fully amortized. Operating expenditures add up: support contracts, SaaS subscriptions, internal engineering labor for maintenance, and training on multiple query languages and interfaces.

The incentive structure this creates is almost perfectly designed to preserve the status quo. New tools are added to the stack because removing old ones triggers write-downs, retraining costs, and political battles. Meanwhile, the operational insight the CIO needs, a unified view of what is happening across the environment, remains out of reach because the data is fragmented across tools that the organization cannot afford to fully use or fully retire.

Part Two: AIOps Is Not a Replacement. It Is an Aggregation Layer[6].

Most AIOps vendors market their technology to reduce or replace human operations work. That framing sells platforms, but it leads buyers to the wrong architectural decisions.

A more accurate way to think about AIOps, particularly for enterprises that already have or are evaluating a managed NOC relationship, is as a layer that sits above the existing operational stack. It ingests telemetry from the tools the organization already owns. It normalizes data formats, deduplicates alerts, and applies correlation logic across domains that traditional point tools cannot span. It produces insights, trend analysis, and context. It does not, by itself, resolve tickets, dispatch engineers, or manage vendor escalations at three in the morning.

What AIOps does well

- Aggregation across existing monitoring tools produces a unified telemetry layer without requiring the organization to rip and replace what it already owns.
- Alert correlation and noise reduction, collapsing symptom-level alerts from multiple tools into a single root-cause incident with relevant context.
- Anomaly detection against learned baselines catches subtle degradations that static thresholds miss.
- Trend and capacity analysis, providing leadership with a data-driven view of where the environment is heading rather than where it has been.

- Independent verification of provider performance is necessary because the data used to measure SLA adherence is owned by the customer, not the provider.

What AIOps does poorly

- Judgment on novel incidents. AIOps platforms pattern-match against known signatures; they struggle with genuinely new failure modes, where human experience and vendor relationships matter.
- Vendor escalation and coordination. Driving a carrier, a hardware vendor, or a cloud provider to resolution is relationship work, not algorithmic work.
- 24x7 human accountability. An AIOps platform does not carry a pager, does not have a named engineer, and does not sit on a bridge call at 2 a.m.
- Hands-on remediation. Physical dispatch, on-site support, and field engineering are operational realities that software does not solve.

> *AIOps replaces neither the NOC nor the operator. It replaces the tolerance for operating without a unified view of your own data.*

This framing matters because it shapes the buying decision. An organization choosing between an AIOps platform and a managed NOC is solving the wrong problem. An organization choosing how to layer customer-owned AIOps on top of a mature managed NOC relationship, with clear ownership of data, alerts, and reporting, is building a scalable operations architecture.

Part Three: The Consolidation Argument, in Financial Terms

For the C-suite, the most compelling case for reorganizing around an AIOps-plus-NOC architecture is financial. The argument breaks down into three parts.

The cost of fragmented tooling is understated

Licensing and subscription costs for monitoring tools are visible and easy to measure. The hidden costs are larger. They include: engineering time spent pivoting between dashboards during incidents; institutional knowledge that walks out the door with every engineer who leaves, taking with it the context for why specific thresholds were set in specific tools; integration and maintenance labor to keep homegrown scripts running; and training overhead for onboarding engineers into an environment where they must learn five different query languages and interfaces to do their job.

When these costs are modeled honestly over a three- to five-year horizon, the TCO of "keeping what we have" often exceeds the TCO of consolidating into an AIOps aggregation layer, even when the AIOps platform's cost is included. Outage economics reinforce the point: New Relic's 2025 Observability Forecast places the median cost of a high-impact outage at $2 million per hour, dropping to $1 million per hour for organizations with full-stack observability(7).

CapEx-to-OpEx shift as a strategic lever

The broader financial trend in enterprise infrastructure has been a deliberate shift from capital-intensive ownership models to operating-expense service models. The rationale is well understood at the CFO level: capex ties up balance sheet capacity, depreciates on a fixed schedule regardless of whether the asset delivers value, and exposes the organization to technology obsolescence risk.

Applying the same logic to network operations yields a clear path. Customer-owned AIOps, typically consumed as SaaS, is OpEx. A managed NOC, delivered as a subscription service, is OpEx. The capital investment in perpetual-license monitoring appliances and vendor-specific tools, which created the tool sprawl in the first place, is the capex being displaced. For CFOs focused on capital efficiency, this is a defensible and increasingly common reallocation.

The sunk-cost trap is real, and it must be named

The single largest barrier to this transition is not technology. It is the psychological and political weight of existing investments. Organizations that have spent seven figures on monitoring tools over the past five years are understandably reluctant to label those investments as replaceable.

The intellectually honest answer for the C-suite is this: sunk costs are sunk. Every future dollar of CapEx or OpEx committed to tools that do not produce unified insight is a dollar not available for the aggregation layer that would. The relevant question is not "what have we already spent?" but "what is the forward-looking TCO of the current architecture compared with a consolidated architecture over the next 36 months?"

When that question is answered honestly, the economics almost always favor consolidation.

Part Four: What SLA Management Looks Like When You Own the Data

The operational dividend of a customer-owned AIOps layer is the most tangible and most underappreciated benefit of this architecture. It shifts the nature of the NOC relationship from dependency to collaboration.

In a traditional outsourced NOC model, the customer relies on provider-generated reports to assess performance. Monthly reviews cover SLA adherence, ticket volumes, and aggregate metrics. The data is accurate but curated. Patterns that might be inconvenient for the provider, such as recurring issues closed rather than root-caused, alerts suppressed to meet response-time targets, and tickets reclassified at the boundary between severity tiers, are effectively invisible to the customer.

A customer-owned AIOps layer changes that dynamic. Because the customer owns the telemetry, they can independently verify:

- Whether alerts that fired in the environment were ticketed by the provider and how quickly.
- Whether mean time to resolution is improving, degrading, or masking recurring issues through fast closures.
- Whether specific classes of incidents cluster in ways that suggest deeper architectural problems, the provider has an incentive not to flag them.
- Whether provider performance varies by shift, by engineer tier, or by time of day in ways the monthly report aggregates.

This is not adversarial. Mature managed NOC providers welcome this transparency because it shifts the quarterly business review from a report-reading exercise to a strategic conversation. The customer arrives with data, and the provider can address specific patterns with targeted improvements. Both sides benefit from the clarity.

> *A managed NOC you can independently measure is one you can genuinely partner with. One you cannot measure is a black box you pay to trust.*

For enterprises whose boards and audit committees increasingly ask tough questions about vendor accountability, particularly in regulated industries, the ability to produce independent evidence of provider performance is no longer a nice-to-have. It is a governance requirement.

Part Five: A C-Suite Framework for Moving Forward

The path from a fragmented tooling environment to an AIOps-plus-NOC architecture is neither fast nor glamorous, but it is straightforward when treated as a strategic initiative rather than a technology project. Four steps define the work.

1. Conduct an honest tooling inventory

Most organizations cannot produce an accurate list of every monitoring, observability, and alerting tool in their environment. The first step is to know what you have, what it

costs in licensing and labor, what it monitors, what it duplicates, and what it fails to cover. This is unglamorous work, but it is the foundation for every subsequent decision.

2. Define the insight layer before choosing the platform

Avoid the trap of evaluating AIOps platforms before defining what you need from one. The right sequence is to first articulate the operational questions leadership needs answered, including uptime, SLA performance, capacity, and risk, and then evaluate platforms based on their ability to produce those answers from the data the organization already owns. Starting with platform evaluation tends to produce a tool that does what the vendor is best at, rather than what the enterprise most needs.

3. Restructure the NOC relationship around shared data

Existing NOC contracts can almost always be renegotiated to include bidirectional data integration with a customer-owned AIOps layer. Mature providers not only permit this; they often prefer it because it reduces ambiguity in the relationship and surfaces operational patterns neither party could see alone. Contracts should explicitly address data ownership, telemetry access, ticketing integration, and joint review of correlated incidents.

4. Commit to a retirement schedule

Consolidation delivers TCO benefits only if legacy tools are retired. Every organization that embarks on this transition and then fails to execute the retirement phase ends up paying for both the old and new stacks, the worst possible outcome. Executive sponsorship of a retirement schedule, with named tool owners and dates, is what separates successful consolidations from expensive parallel environments.

The maturity curve

Organizations typically progress through this architecture in three stages. The first stage is reactive: multiple tools, no aggregation, provider-reported SLAs taken at face value, and incident response driven by whoever notices first. The second stage is

consolidated: a customer-owned AIOps layer in place, a meaningful reduction in alert noise, independent visibility into provider performance, and TCO conversations moving in the right direction. The third stage is collaborative: AIOps and NOC operating as a designed system, with the provider's execution capability and the customer's insight layer reinforcing each other, and SLAs becoming a conversation about continuous improvement rather than a compliance check.

Closing Thought

The most common mistake we see in the market right now is framing AIOps as a way to do more with less, using fewer tools, fewer people, and lower spend. That framing is narrow and usually disappointing in practice.

A more useful framing is that AIOps and a managed NOC, when properly architected, enable an enterprise to do something genuinely different: operate a complex environment with insight and accountability that neither capability alone could provide. The financial case is strong. The operational case is even stronger. The governance case, in a regulatory environment that continues to tighten, may turn out to be the most important of the three.

For technology leaders, the question is not whether this convergence will happen. It will. The question is whether to architect it deliberately or inherit it by accident.

About this paper. This paper presents Kore-Tek's strategic perspective on the convergence of AIOps and managed network operations. Kore-Tek delivers optical engineering, network infrastructure, and managed NOC services to enterprise and service provider end users seeking consolidated, measurable, and operationally mature network environments. To discuss how this framework applies to your organization's infrastructure, visit sales@kore-tek.com.

Sources and References

[1] Paessler GmbH, press release, "Tool Sprawl Has Become a Security and Operational Risk as IT Teams Waste Over a Quarter of Their Time on False Positives," March 2026. Paessler's survey of enterprise IT environments found that the average organization operates between 10 and 15 separate monitoring solutions covering networks, servers, applications, cloud resources, and databases.

[2] Trend Micro International, "Cybersecurity Tool Sprawl" research, cited in Cybersecurity Dive. Survey of 2,303 IT security decision-makers across 21 countries found global organizations employ an average of 29 security monitoring tools, rising to an average of 46 tools in organizations with more than 10,000 employees.

[3] Vectra AI, "2026 State of Threat Detection Report," and IBM SOC research referenced in the CybelAngel analysis of tool sprawl, December 2025. Vectra AI reports an average of 2,992 daily alerts (down from 3,832 in 2025 and 4,484 in 2023); Cybersecurity Insiders 2025 research indicates 63 percent of those alerts go unaddressed, with IBM-referenced data citing 67 percent noise rates.

[4] New Relic, "2025 Observability Forecast," and BlueCat / Enterprise Management Associates (EMA), "The Network Observability Maturity Model," both covered in Network World (December 2025). New Relic's report is based on a global survey of 1,700 IT and engineering leaders; the EMA study surveyed 250 IT stakeholders.

[5] INOC, "NOC Service Level Reporting: Basics, Best Practices and Examples" (February 2026) and Pomeroy, "Building Trust through Measurable Outcomes: NOC as a Service SLAs, SLOs and KPIs" (November 2025). Both sources discuss the structural asymmetry in traditional outsourced NOC relationships where the provider owns the reporting layer.

[6] Gartner, "Market Guide for Event Intelligence Solutions" (Matt Crossley, Gregg Siegfried, March 2025). Gartner's rebranding of the AIOps market under the Event Intelligence Solutions category explicitly emphasizes aggregation, correlation, and noise reduction capabilities rather than operator replacement.

[7] New Relic, "2025 Observability Forecast." The report places the median cost of a high-impact outage at approximately $2 million per hour across the surveyed organizations, with organizations that have achieved full-stack observability experiencing roughly half that median cost. Seventy-five percent of respondents reported positive ROI from observability investments, with 18 percent reporting three- to ten-fold returns.

Additional analyst and industry research consulted: Gartner "Hype Cycle for I&O Automation, 2024" on network automation trends; Gartner press release, "30% of Enterprises Will Automate More Than Half of Their Network Activities by 2026" (September 2024); and industry research from LogicMonitor, Optiv, and IDC on alert fatigue patterns. All statistics presented in this paper reflect publicly available research as of Q1 2026.