KORE-TEK STRATEGIC PERSPECTIVES, NO. 3

The Outsourcing Inflection:

Why Network Operations Is Becoming a Service Category

A market analysis of the forces reshaping enterprise NOC sourcing decisions

Kore-Tek Insights | kore-tek.com/insights
Kore Technologies, LLC | 225 South 6th Street, Suite 3900, Minneapolis, MN 55402

Kore-Tek Strategic Perspectives, No. 3 in an ongoing series

Executive Summary

Network operations is undergoing a category-formation moment. What was for decades treated as discretionary in-house function, staffed, tooled, and operated by organization on their own terms, is becoming a defined service category with measurable economics, professionalized delivery models, and external benchmarks. The shift is not architectural. It is operational and financial.

The market data is unambiguous. Independent analysts project the global NOC-as-a-Service market to expand from approximately $3.73 billion in 2025 to $6.14 billion by 2030, at a compound annual growth rate of 10.5 percent[1]. Within that growth, hybrid delivery models (onsite + remote) are the fastest-growing segment, reflecting how regulated industries are reconciling compliance requirements with the operational economics of outsourced delivery[1]. These are not the growth dynamics of a feature. They are the growth dynamics of a category.

Five forces are driving the inflection: rising infrastructure complexity across multi-cloud, edge, and IoT estates; the operational drag of tool sprawl and alert fatigue; the escalating cost of downtime in always-on environments; intensifying compliance and auditability requirements; and a structural shortage of network operations talent. Each driver in isolation could be addressed through hiring, tooling investment, or process change. Taken together, they describe a sourcing environment where the in-house operational baseline is no longer the lowest-cost or lowest-risk option for most organizations. Network operations is moving from a discretionary internal function to a sourced service category, and the move is being driven by economics, complexity, and labor-market conditions that are unlikely to reverse.

> *“More organizations are moving to outsourced or hybrid NOC models not because architecture has failed, but because operations have outgrown the org chart.”*
> Ryan Young, CEO, Kore-Tek

The Market Trajectory

The most consequential signal in the NOC services market is not its absolute size. It is the composition of the growth.

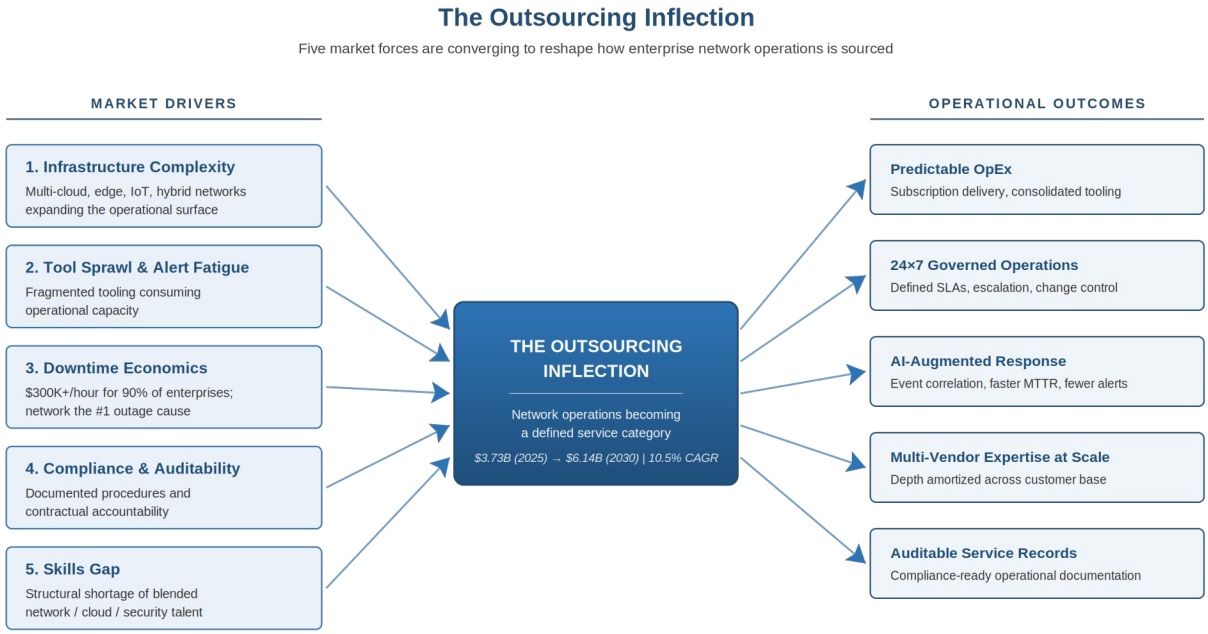
The headline number is straightforward. The global NOC-as-a-Service market is projected to reach approximately $6.14 billion by 2030, expanding from $3.73 billion in 2025 at a compound annual growth rate of 10.5 percent[1]. Independent market research firms produce variant numbers depending on segment definition and geographic scope, but the directional consensus is consistent: this is a market growing at roughly double the rate of overall IT services spend[2].

Two structural patterns within the growth matter more than the topline. First, offsite delivery, fully external NOC operations, continues to hold the largest share of the market, driven primarily by cost efficiency[1]. Second, hybrid delivery models, in which operational responsibility is shared between an internal team and an external partner, with workload distribution varying by capability domain, are the fastest-growing segment[1]. The hybrid pattern reflects a specific buyer profile: organizations in regulated industries, organizations with data residency requirements, and organizations that have invested heavily enough in internal capability that wholesale outsourcing would be operationally disruptive. These buyers are not choosing between in-house and outsourced. They are choosing how to distribute responsibility across both.

This composition has a clear strategic implication. The category is not maturing toward a single dominant delivery model. It is maturing toward an established set of sourcing choices that each carry their own economics, their own governance requirements, and their own operational dependencies. The previous paper in this series, *The Co-Managed NOC: Rethinking the Sourcing Spectrum for Enterprise Network Operations*, examines this sourcing structure in detail. The growth data confirms what that paper described: the spectrum is no longer theoretical. It is where buyer demand is concentrating.

The Outsourcing Inflection at a Glance

The diagram below summarizes the five market drivers reshaping enterprise network operations sourcing decisions and the operational outcomes that mature managed and hybrid delivery models produce. Each driver is examined in detail in the sections that follow.



Sources: MarketsandMarkets (NOCaaS Market Forecast); ITIC 2024 Hourly Cost of Downtime; Uptime Institute 2024 Data Center Resiliency; WEF Future of Jobs 2025; Linux Foundation 2025 State of Tech Talent. See Sources section for full citations.

Kore-Tek Strategic Perspectives, No. 3

The Five Forces Driving the Inflection

Driver 1: Multi-Cloud, Edge, and the Complexity Surface

Networks have changed shape. For most organizations, the operational estate now spans on-premises infrastructure, two or more public clouds, edge locations, branch networks, and a growing population of IoT and operational technology endpoints. Each layer brings its own telemetry, its own management interface, and its own failure modes.

The operational consequence is not merely that there are more components to monitor. It is that the relationships between components are increasingly opaque. A performance degradation observed in a cloud-hosted application may originate in an on-premises firewall configuration, a third-party transit provider, an SD-WAN policy change, or an edge device firmware update. Each of those domains is typically instrumented by a different team, with different tooling, and different alerting thresholds. The diagnostic work that was once contained within a single team and a single console now requires coordination across multiple operational silos to resolve a single incident.

Independent analyst commentary on this shift converges on a common observation: **network operations is the layer of the IT stack where complexity is compounding fastest, and where the gap between observable telemetry and actionable insight is widening**[3]**.** This is not a problem that more tooling will solve. It is a category-level shift in what the operational function is being asked to do.

Driver 2: Tool Sprawl, Alert Fatigue, and Operational Drag

The instinctive response to complexity has been to add tools. Most IT organizations now operate a portfolio of monitoring, observability, alerting, ticketing, automation, and analytics platforms, often dozens of them, each acquired to address a specific gap and each generating its own signal stream.

The cumulative effect of this layering is well-documented. Operational teams spend an increasing percentage of their working hours triaging and de-duplicating alerts rather than executing on incidents. Independent research on monitoring and event management consistently finds that alert volume far exceeds operator capacity, and that the majority of alerts generated by enterprise monitoring stacks are either redundant, low-priority, or actionable only after correlation with other signals[4]. Gartner’s Market Guide for Event Intelligence Solutions describes this dynamic as the central problem that event intelligence and AIOps platforms exist to solve[5].

The relevant metric is not the alert count. It is the share of operational capacity consumed by signal processing relative to the share spent on resolution and improvement. Organizations operating mature monitoring stacks without an aggregation and correlation layer above them typically find this ratio inverted, most of the team’s time is being spent on signal management, with resolution work fitted into whatever time remains. The first paper in this series,

The AIOps and Managed NOC Convergence, examines this pattern and the architectural response in detail.

A related and underappreciated dynamic is reporting and budget fragmentation. The tool portfolio described above is typically acquired piecemeal, often across capital and operating budget cycles, and rarely consolidated into a single line of accountability. The result is that the true cost of operational tooling is opaque even to the CIOs and CFOs accountable for it. This reporting gap is one of the most consistent observations from buyer-side conversations about the move toward managed and hybrid delivery models: the financial reset is often more attractive than the operational one.

Driver 3: The Economics of Downtime

The financial case for operational investment is often based on mitigating loss due to downtime.

ITIC's 2024 Hourly Cost of Downtime Survey, based on more than 1,000 responses worldwide, found that a single hour of unplanned downtime now costs over $300,000 for more than 90 percent of mid-size and large enterprises, and that 41 percent of enterprises report hourly downtime costs in the $1 million to $5 million range or higher[6]. These figures exclude regulatory penalties and litigation exposure.

The Uptime Institute's 2024 Data Center Resiliency Survey adds a critical operational detail: network-related issues have become the single largest cause of IT service outages, with 31 percent of respondents identifying networking and connectivity as the primary cause. Among network-driven outages specifically, the top underlying causes are configuration and change management failures (45 percent of respondents) and third-party provider failures (39 percent) [7]. The implication is that the operational disciplines most directly responsible for preventing outages, change management, configuration governance, and partner coordination, sit squarely inside the NOC function.

Total cost of ownership reinforces this. Meter's IT Total Cost of Ownership guide lays out the full set of costs an in-house operation has to carry: hardware, software licensing, labor, ongoing maintenance, energy, and the cost of downtime[8]. The key point is how those costs behave over time. Across a three- to five-year horizon, the recurring costs, not the upfront purchase, become the largest part of the total, often two to three times the size of the initial capital outlay.

This is where managed delivery changes the math. ACG Research's published business cases report total cost of ownership reductions of roughly 79 percent for managed WAN and 84 percent for managed Internet and security services in representative mid-market scenarios[9]. Those figures call for some caution, since savings of that size reflect specific use cases and specific starting costs and will not hold for every organization. But the underlying pattern is consistent across independent analysis. **Once the full recurring cost of running operations in-house is counted, including the loaded cost of dedicated staff, the licensing and renewal burden of monitoring tools, and the financial exposure of unplanned downtime, the comparison with a subscription-based managed model is rarely close.**

Driver 4: Compliance, Auditability, and the Case for Hybrid Delivery

Compliance and audit pressure has changed the conversation about outsourced operations in regulated industries.

A decade ago, the dominant compliance objection to outsourced NOC services was data residency and access control: regulated buyers required their operational data to remain within defined geographic and access boundaries, and few external providers could credibly meet those requirements. The market has substantially adapted to that constraint. Hybrid delivery models, in which sensitive workloads and tier-one infrastructure remain under direct internal control while routine monitoring, after-hours coverage, and standardized incident handling are delivered externally, have emerged as the preferred sourcing pattern in healthcare, financial services, public sector, and education[1].

The compliance case for hybrid delivery is not merely about meeting residency and access requirements. It is about auditability. A formal managed services relationship, with documented service-level commitments, recorded operational procedures, defined escalation paths, and contractual accountability, produces an auditable operational record that in-house teams often cannot match. **For organizations subject to SOX, HIPAA, PCI-DSS, FedRAMP, or sector-specific regulatory frameworks, the documentation produced as a byproduct of a managed services relationship is itself a compliance asset.** This is one of the less-publicized reasons that regulated buyers are moving toward hybrid models even when their internal operations are technically capable of meeting performance requirements without external support.

Driver 5: The Skills Gap

The labor market for senior network operations talent is structurally tight, and the trend is intensifying.

The World Economic Forum's Future of Jobs Report 2025 identifies skills gaps as the single largest barrier to business transformation through 2030, with 63 percent of surveyed employers citing them as a major obstacle[10]. The Linux Foundation's 2025 State of Tech Talent report, based on responses from more than 500 global hiring leaders, finds that 65 percent of organizations report being understaffed in cybersecurity and compliance, 59 percent in cloud computing, and 56 percent in platform engineering, each of which is foundational to modern network operations[11]. **IDC has projected that the IT skills shortage will affect 9 out of 10 organizations by 2026, with a cumulative cost of approximately $5.5 trillion attributable to delays, quality issues, and lost revenue[12].**

The labor-market signal is reinforced by what hiring organizations are paying for. Compensation premiums for senior network engineers with cloud, security, and automation depth have moved sharply upward, and the pattern of "blended skills" demand, engineers who can credibly cover networking, cloud, and security simultaneously, has compressed the available labor pool further[2].

The strategic implication for sourcing decisions is straightforward. Building an in-house NOC function at the scale required to staff a true 24×7 operation typically requires between eight and twelve full-time engineers, accounting for shift coverage, vacation rotation, escalation depth, and specialty expertise across vendor platforms. Filling that headcount with engineers who carry the necessary blended skill profile, retaining them against compensation pressure from larger employers, and absorbing the institutional cost when they leave is a labor-market exposure that most organizations are reassessing. The economic case for distributing this labor exposure across a multi-tenant provider, where staffing depth is amortized across a customer base, is not new. What is new is the size of the gap, the cost of the gap, and the rate at which the gap is widening.

What the Inflection Produces

The five drivers above describe why the market is moving. The operational outcomes that follow describe what buyers receive in return.

The most significant operational shift accompanying the move toward outsourced and hybrid NOC delivery is the integration of AIOps and event intelligence platforms into operational workflows. AIOps adoption is consistently identified by independent analysts as a primary growth driver for the broader NOC services category, both because it amplifies the productivity of operational staff and because it enables a class of proactive and predictive operational behaviors that manual workflows cannot support at scale[5]. Event intelligence and alarm-correlation platforms compress the gap between signal generation and meaningful operational action, which is precisely the gap that consumed the disproportionate share of in-house operational time described earlier.

The outcomes that mature managed and hybrid NOC delivery models produce are well-defined and measurable: faster mean time to detection and resolution, sustained reduction in alarm volume reaching human operators, formal change governance with auditable records, expansion of effective coverage from business hours to true 24×7, and access to a depth of multi-vendor expertise that few in-house teams can credibly maintain. The previous papers in this series, *The AIOps and Managed NOC Convergence* and *The Co-Managed NOC*, examine the architectural and sourcing dimensions of these outcomes in detail. This paper addresses the market context that is causing them to be in demand.

The Outsourcing Inflection

The category-formation moment described in this paper is not a forecast. It is a description of buyer behavior already underway. Independent market data, third-party operational research, and the structural pressures observable across enterprise IT all point to the same **conclusion: network operations is moving from a discretionary internal function to a sourced service category, and the move is being driven by economics, complexity, and labor-market conditions that are unlikely to reverse.**

The implication for senior infrastructure leaders is not that an outsourcing decision is now mandatory. It is that the default sourcing baseline has changed. A decade ago, the in-house NOC was the assumed starting point, and outsourcing was the alternative that had to justify itself. The current market environment has inverted that relationship. The outsourced or hybrid baseline now sets the operational and financial reference point, and an in-house function, particularly one operating without an aggregation and correlation layer above it, increasingly carries the burden of justification.

For organizations evaluating their position against this baseline, the relevant questions are not architectural. They are operational: what share of operational capacity is being consumed by signal processing rather than resolution? What is the true loaded cost of the existing operational stack, including downtime exposure? What is the labor-market exposure of the current staffing

model? And what does the available evidence suggest the answers to those questions will look like three years from now? Kore-Tek is positioned to help senior infrastructure leaders work through those questions on terms that match the substance of the decisions involved.

About This Paper

This paper is a Kore-Tek Strategic Perspective, part of an ongoing series intended as framework-level reference material for senior infrastructure leaders. The series is published in our Insights library at kore-tek.com/insights, alongside earlier papers including *The AIOps and Managed NOC Convergence* (No. 1) and *The Co-Managed NOC: Rethinking the Sourcing Spectrum for Enterprise Network Operations* (No. 2).

Kore Technologies, LLC (Kore-Tek) is an optical engineering, network infrastructure, and managed NOC services firm based in Minneapolis, Minnesota. The firm partners with leading equipment manufacturers and integrators to deliver network operations capabilities to enterprise, education, public sector, and service provider customers.

For additional information about our NOC services or to request a briefing, visit kore-tek.com or contact marketing@kore-tek.com.

Sources

1. MarketsandMarkets, *NOC-as-a-Service Market, Global Forecast to 2030*. marketsandmarkets.com

2. TechTarget and Network World coverage of the network operations labor market, including the Linux Foundation's 2025 State of Tech Talent findings on blended-skills demand and Skillsoft survey data on the most difficult roles to fill. techtarget.com; networkworld.com

3. EMA Research, network monitoring and observability market analysis, as cited in *The AIOps and Managed NOC Convergence* (Kore-Tek Strategic Perspectives, No. 1). ema-research.com

4. Independent observability and event-management research on alert volume and operational drag, including BigPanda 2024 downtime cost analysis and EMA Research observability findings. bigpanda.com; ema-research.com

5. Gartner, *Market Guide for Event Intelligence Solutions*, March 2025. gartner.com

6. ITIC (Information Technology Intelligence Consulting), *2024 Hourly Cost of Downtime Survey*. itic-corp.com

7. Uptime Institute, *2024 Data Center Resiliency Survey*. uptimeinstitute.com

8. Meter, *IT Total Cost of Ownership* guide. meter.com

9. ACG Research, managed services business case analyses on TCO reductions for managed WAN and managed Internet/security services. acgcc.com

10. World Economic Forum, *Future of Jobs Report 2025*. weforum.org

11. The Linux Foundation, *2025 State of Tech Talent Report*. linuxfoundation.org

12. IDC, projections on the impact of the IT skills shortage on enterprise organizations through 2026, as referenced in published analyses by Tecla and Xantrion. idc.com