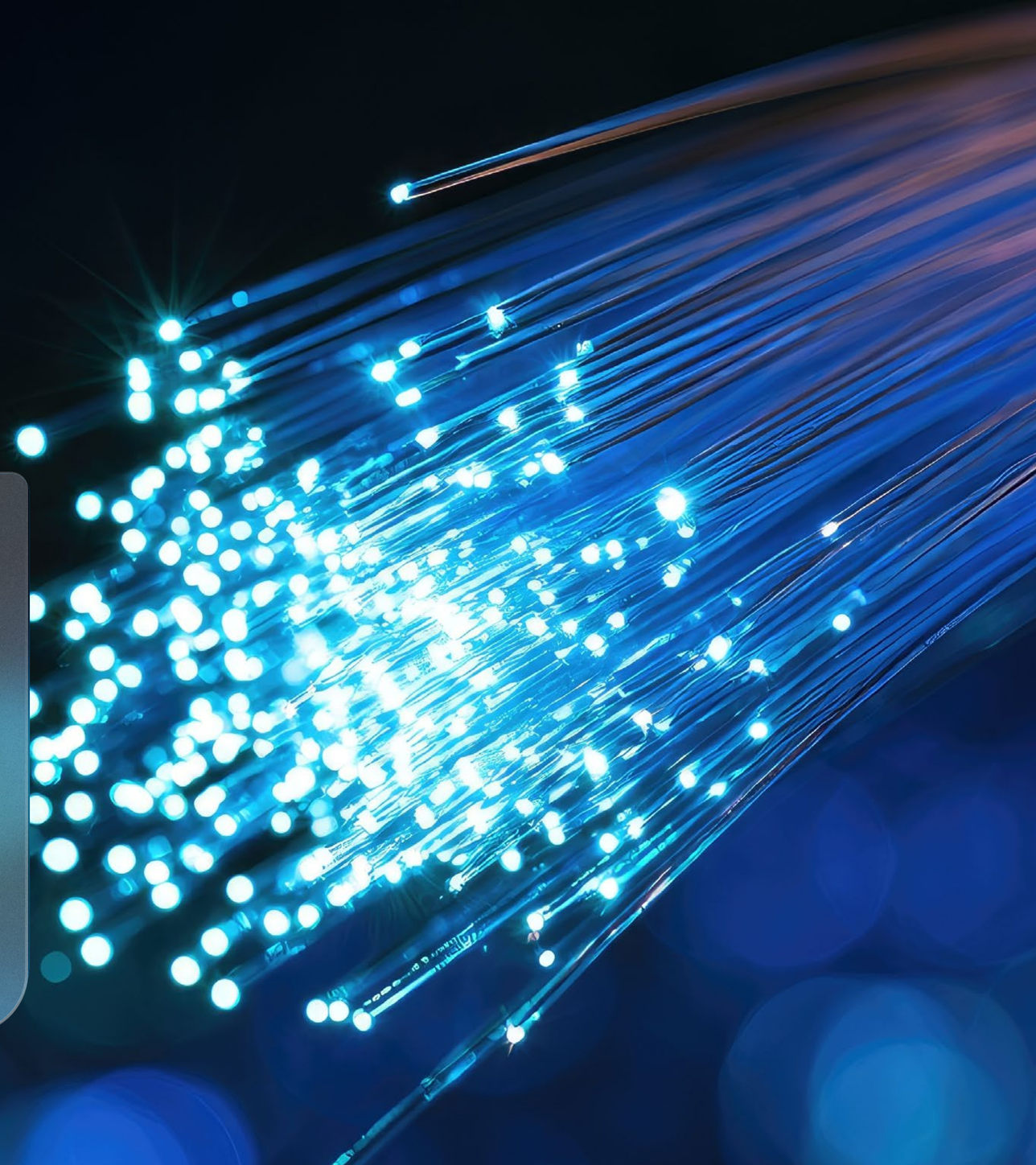
SUTHERLAND®

What Happens When Operational Visibility Isn’t Enough?

How an agentic model can turn enterprise NOC insights into better operational decisions



Identifying the Problem Is Only the Beginning

It’s the early hours of Wednesday morning, and a routine infrastructure change has just completed during the overnight maintenance window. Minutes later, monitoring systems are flashing alerts across network, application, and service layers. Performance has degraded across multiple workloads, with symptoms appearing in systems that don’t immediately seem connected.

The timing makes the change the obvious place to look. But is it the root cause, a contributing factor, or simply a coincidence?

This is an all-too-familiar challenge for enterprise NOCs (Network Operations Center). And that’s despite years of investment in monitoring, automation and AIOps that lets operations teams see more of their environment than ever and spot the first signs of trouble faster.

Yet, spotting those signs is just one step on the road to recovery after an incident. Truly understanding what’s happened and working out what to do next is a far more complex task.

The reason for this – and one of the hardest steps in the overall process – is connecting the dots between different signals and data points. Operations teams must establish which alerts share a common cause, what might have changed immediately beforehand, which business services depend on the affected infrastructure, and what can be restored safely.

Building that picture takes considerably longer than initially detecting the problem. And even after the originating issue has been resolved, downstream services might remain degraded while dependencies, backlogs, or other residual effects are addressed.

Two-thirds (67%) of network observability alerts are deemed to be noise, while the typical network operations professional spends 29% of their day firefighting.[1]

1 https://www.enterprisemanagement.com/product/network-management-megatrends-2026-automation-hybrid-and-multi-cloud-networks-and-ai-transformation/

 © 2026, Sutherland Global Services, Inc. All rights reserved

The Current Response Model Is Reaching Its Limits

As enterprise environments become increasingly interconnected, this challenge becomes more pronounced. A single digital service might span network infrastructure, cloud platforms, applications, third-party services, and multiple operational teams, meaning an incident can quickly become a coordination problem that extends well beyond the technology domain where it was first detected.

When disruption reaches critical services, the financial stakes can be high. In an Uptime Institute survey, 57% of respondents estimated **the cost of their most recent major data center outage was above $100,000.**[2]

The challenge then isn't visibility. **What's missing is a way to carry context from detection through investigation and prioritization to decision, action, and recovery,** ensuring the response reflects what the incident means for the services the business depends on.



2 https://datacenter.uptimeinstitute.com/rs/711-RIA-145/images/2026.AnnualOutageAnalysis.pdf

 © 2026, Sutherland Global Services, Inc. All rights reserved

Where the Response Starts To Break Down

Large enterprises aren’t starting from scratch when it comes to NOC modernization. Many already have monitoring, ITSM, automation, observability, and AIOps capabilities in place.

The challenge is that the evidence needed to understand an incident can be scattered across multiple places: telemetry and logs, topology and configuration data, service maps, tickets, change records, and more.

This creates friction at the exact point where speed matters most. An anomaly might appear in one tool while the relevant change history sits in another, leaving teams to piece together the incident context. According to EMA research, 75% of IT professionals reportedly use four to 12 observability tools across network, cloud infrastructure, and service environments, with 55% having to switch tools three to five times per incident.[3]

This fragmentation is difficult to tackle because the barriers are not purely technical. Different teams may own different parts of the incident lifecycle, leading to manual handoffs, repeated interpretation, and people rebuilding context as the incident evolves. Data quality and service mappings can vary. Integrations need to work across legacy and multi-vendor environments. And governance requirements can limit what can be automated.



3 https://www.enterprisemanagement.com/press_release/new-ema-research-finds-observability-unification-remains-a-challenge-for-most-enterprises/transformation/

 © 2026, Sutherland Global Services, Inc. All rights reserved



The Answer Isn’t Another Point Solution

Because the problem spans tools, data, workflows and organizational ownership, adding another isolated capability only addresses part of it. A point solution may improve monitoring, correlation or automation within a specific domain or stage, but it won't carry context across the tools, teams and workflows involved in the wider response.

By contrast, an agentic operating layer uses AI agents to coordinate incident response across the operational tools and workflows already in place. It maintains context from detection through investigation, decision and action, while the underlying monitoring, ITSM, observability and automation platforms continue doing the jobs they were built for.

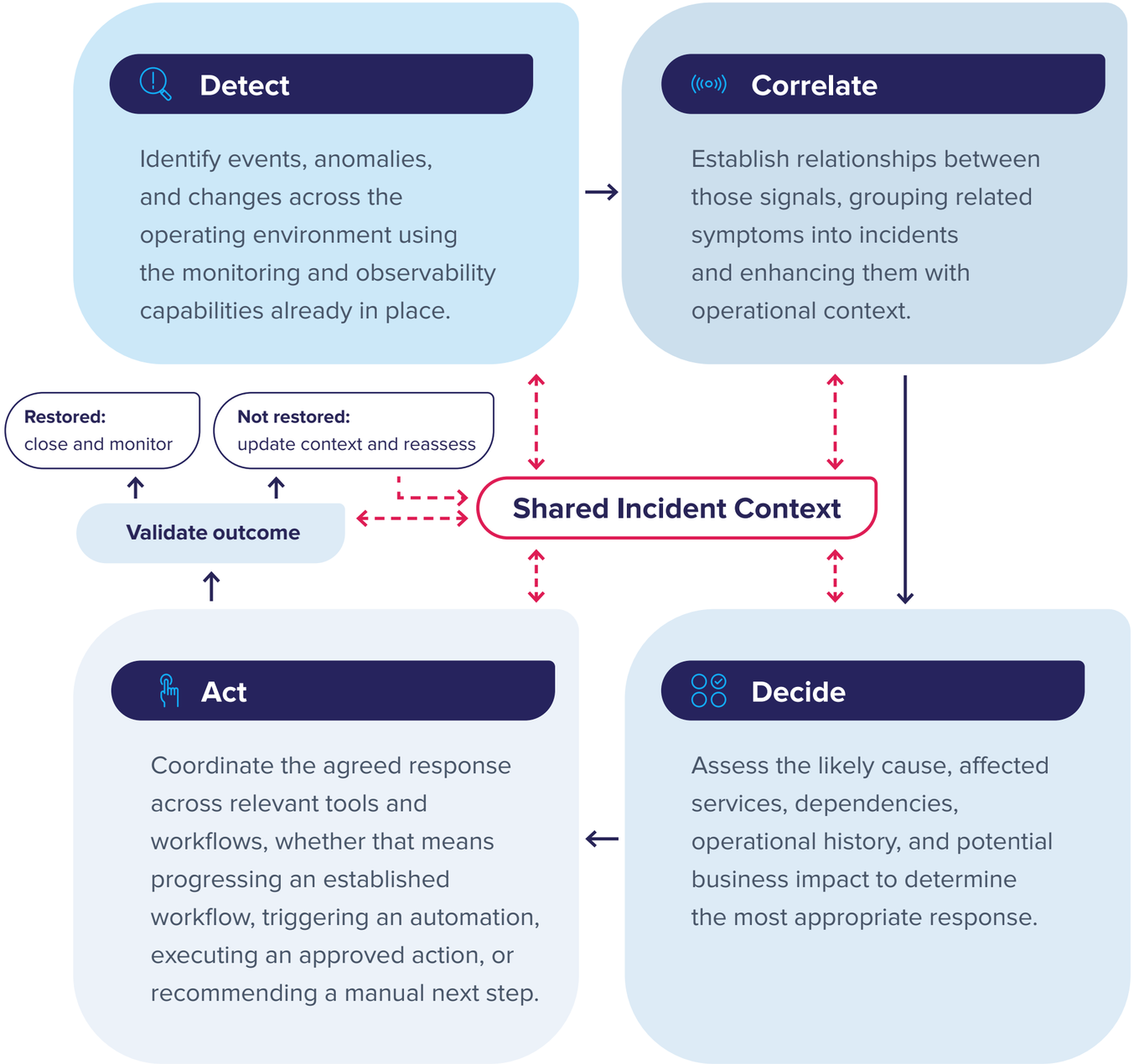
In a **connected manufacturing plant**, the network alert, application dependency, and production schedule may sit in different systems, owned by different teams. Until those views are connected, the NOC may see a network fault without being able to fully recognize the production downtime at risk.

This is the operating model shift at the heart of the agentic NOC.

Moving From Operational Noise to Business Context

An agentic NOC changes how intelligence is applied across the operations environment. Through a multi-agent, multi-step orchestration model, it brings together signals, operational knowledge, service context, and workflows so the NOC can build and maintain a more complete picture as an incident develops.

At a high level, this creates a four-stage operating loop where each stage enhances the same incident record:



POV-1106 | © 2026, Sutherland Global Services, Inc. All rights reserved

The agentic layer extends existing automation by interpreting developing context, selecting from approved tools and APIs, and coordinating a response across multiple steps. So rather than executing a pre-defined task in isolation, it can use new insight across each stage to determine what should happen next. In turn, this means hundreds of disconnected alerts can be narrowed into a smaller number of contextualized incidents, with the likely cause, affected service, business significance, and recommended response brought together in a shared incident record.

Validation then takes the response beyond execution to verified recovery – i.e., did the action restore the affected service? If it didn't, that execution becomes additional evidence, allowing the NOC to reassess without restarting the investigation from scratch and supporting further self-improvement and optimization over time.

The added context this loop creates also provides a better basis for prioritization. An incident doesn't necessarily become the highest business priority because it generates the most alerts or carries the highest technical severity. The response can instead reflect what the incident actually means for the business.

A network incident affects both an internal reporting tool and the payment service of a **national bank.** By connecting the fault to service dependencies and transaction failures, Agentic NOC can prioritize payment recovery based on the disruption to customers' ability to transact.

Retail Example: The Four-Stage Loop in Practice

An online checkout service slows during a busy holiday period. An agent correlates network and application alerts to identify the likely cause. With access to order-processing data, it flags purchases at risk and raises the priority of the incident.

The agent then recommends a tested recovery action for human approval and checks whether checkout performance recovers after the change.



Trust the Action, Not Just the Decision

An agentic NOC improves how incidents are understood, prioritized, and acted on. But the ability to make a better decision does not automatically mean an agent should be allowed to execute it. The key question is how much authority agents should have in different situations.

This will depend on factors such as the potential business impact, the confidence behind the decision, and the nature of the action itself. A low-risk, well understood workflow can be treated very differently from one involving a critical service where the consequences of getting it wrong are much greater.



The goal, therefore, is not full autonomy everywhere. It's the right level of autonomy for each situation.

Autonomy Sits on a Spectrum

An agent might investigate an incident and recommend the next step, leaving the final decision with the operations team. In another workflow, it might coordinate the response across several tools but wait for human approval before execution. And in a lower-risk, higher-confidence scenario, an agent could be allowed to carry out a predefined action automatically.

For a **healthcare provider,** the agentic NOC can connect a network fault to disruption in clinicians' access to patient records. An agent can immediately undertake pre-approved diagnostic checks, while changes that could further affect access to critical clinical services remain subject to human approval.

Making that spectrum work depends on policy guardrails, confidence and risk thresholds, and human oversight being built into the operating architecture from the outset. The controls around each workflow need to determine what agents can do independently, what requires approval, and when an issue should be escalated.

Modernize Around the Services That Matter Most

Implementing an agentic NOC does not mean transforming the entire operating environment at once. For most enterprises, a more practical starting point is to identify the services and workflows where manual effort, fragmented processes, or slow decision-making create the clearest operational risk or cost.

That does not necessarily mean starting with the most critical service in the business. The strongest candidates are those where the potential value is meaningful, but the data, integrations, processes, and controls are mature enough to introduce agentic capabilities in a controlled way.



© 2026, Sutherland Global Services, Inc. All rights reserved

Start With Where You Are Today

Sutherland's assessment-led approach starts by establishing that baseline. How connected is your operational data? How much context can already be brought together? Where are decisions still dependent on manual investigation? And which incident management workflows are mature enough to support greater levels of orchestration or autonomy?

From there, the journey can be mapped against five stages of operational maturity:

1 Observe



Connect signals and operational data from across the existing environment to create a clearer and more consistent view of what is happening.

2 Understand



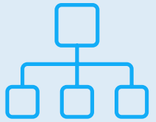
Correlate events and enrich them with topology, dependencies, and operational context to identify likely causes and affected services.

3 Recommend



Prioritize incidents and recommend the most appropriate response, while keeping the final decision with the human in the loop.

4 Orchestrate



Coordinate workflows and actions across tools and teams, with agents initiating and progressing the response within defined controls.

5 Operate Autonomously



Allow agents to execute certain actions independently within predefined guardrails, validate outcomes, and escalate exceptions.

POV-1106 | © 2026, Sutherland Global Services, Inc. All rights reserved

Different services can sit at different maturity stages depending on their complexity, risk, and operational maturity. A workflow may remain at ‘recommend’ because human judgment is essential for it, while another can progress to autonomous execution once the evidence and controls justify doing so.

Measuring What the Agentic NOC Protects

Success in this environment should be measured against the same business priorities that guide modernization. Traditional NOC metrics such as MTTR, incident volumes, and productivity still matter, but they only tell part of the story.

A more meaningful measure is what improvements in those areas protect: service availability, reduced disruption, operational continuity, SLA performance, and the smooth running of business processes that depend on the underlying technology layer.

Framing the agentic NOC in this way creates a repeatable path to scale. Enterprises can prove the model around a smaller number of high-value services or workflows, learn from the results, strengthen the underlying operating foundations, and then extend the agentic NOC across a wider range of use cases and levels of autonomy over time.

A cloud infrastructure fault has been resolved, but customers are still struggling to use a **SaaS platform**. By connecting infrastructure status with application performance and failed user requests, the agentic NOC can check whether the customer-facing service has recovered, giving teams a clearer measure of restored availability.



From NOC Metrics to Business Resilience

Ultimately, the agentic NOC isn't about seeing more, automating every step, or removing people from the process. Its true value lies in helping operations teams make better operational decisions faster, with a clearer understanding of what is happening, why it matters to the business, and what needs to happen next.

Adopting this model doesn't require wholesale replacement. Sutherland combines unrivaled engineering expertise and agentic NOC capabilities with an open, standards-based architecture built on the TM Forum ODA framework to provide a route to modernize around the technology and operational investments you've already got in place.

Sutherland's agentic NOC is already delivering significant operational impact across live enterprise deployments. Results have included:

18 > 1
raw alarms correlated into a single root cause incident

40-60%
MTTR reduction on average

6,180+
outage minutes saved per month for a global enterprise client

The result is a shift away from fragmented, reactive operations towards a model that **allows for faster, more trusted decisions based on what matters most to the business.**

POV-1106 | © 2026, Sutherland Global Services, Inc. All rights reserved

Ready to evolve your NOC?

Learn more about how we can help you build a phased roadmap towards greater orchestration and autonomy.

Explore Your NOC Roadmap

Sutherland is an AI-driven business transformation partner to enterprises, including several Fortune 500 clients. We design, run, and automate business operations at scale, helping clients improve efficiency, strengthen customer experiences, and deliver measurable outcomes.

Most companies either build AI-led capabilities or run operations. Sutherland does both. We run complex, mission-critical processes while engineering the AI-led solutions that sit within them. This closed loop helps clients move beyond AI pilots to reliable, governed outcomes that improve and scale over time.

With deep operational expertise, advanced products, platforms, and engineering, we help clients modernize operations and build future-ready businesses.

SUTHERLAND®
driving outcomes.

sutherlandglobal.com

POV-1106 | © 2026, Sutherland Global Services, Inc. All rights reserved