WHITE PAPER

# Killing the Alarms

## Moving from reactive noise to autonomous action

An architectural argument for why the human-in-the-loop NOC stopped scaling, and what an AI-native alternative actually looks like — including what is running today and what is not.

**Shawn Ennis**

Founder, Rapax — a Citus Technologies company

sales@rapax.app · rapax.app · cal.com/shawn-ennis

Written for: CTO, COO, VP of Network Operations, NOC Director

Version 2.0 · July 2026

### WHAT THIS PAPER CLAIMS, AND WHAT IT DOES NOT

This paper describes an operating model and the architecture behind it. Where a capability is available today, it is listed in the "Available today" table. Where it is planned, it is listed in the "On the roadmap" table and described as design intent.

Performance figures for unreleased capabilities are not published here, because they have not been measured. Industry figures cited in the text are attributed in the Sources section, and where a widely repeated number could not be traced to a primary source, it has been left out rather than restated.

# 1. The end of reactive operations

Your best engineers are working as network janitors. They watch dashboards, correlate alarms by hand, and clean up configuration errors that a machine should never have allowed in the first place. None of that is the work you hired them for, and none of it gets easier as the network grows.

The economics underneath this are the real problem. Bandwidth demand rises on an exponential curve. Revenue per bit does not. Every operator therefore faces the same question: how do you cover a materially larger network without a proportionally larger operations team?

The conventional answers have run out. You can buy another monitoring tool, but tool count is already part of the problem. You can hire, but the workforce that understands both legacy transport and modern fiber plant is retiring faster than it is being replaced. You can accept longer restoration times, but that shows up in churn.

The remaining answer is to change what a human is for. That is what this paper is about.

### The scissors effect

Two lines are moving in opposite directions. Network complexity is climbing — 5G, XGS-PON, virtualized cores, more vendors, more device types, more telemetry per device. Available operational expertise is falling, as experienced staff retire and the pipeline behind them is thinner than the one that fed it.

Traditional OSS/BSS platforms cannot close that gap, because they were built for a world where a human read the output. They are reactive by design: they detect, they display, and they wait. Every minute a person spends deciding which of forty alarms matters is a minute of restoration time you are paying for twice — once in labor and once in service credits.

# 2. The foundation: from data lakes to data activation

Most operators are drowning in telemetry and starving for action. The usual architecture routes everything into a data lake — which, in practice, is where telemetry goes to die. Query latency measured in seconds to minutes is fine for a quarterly capacity review and useless for an event in progress.

Rapax separates the two workloads instead of forcing one store to serve both.

### Hot path — Redis Streams

The nervous system. Streaming telemetry and alerts are processed as they arrive, so correlation happens while the event is still unfolding rather than after someone opens a dashboard.

### Cold path — OpenSearch

The memory. Historical data is retained for trend analysis, capacity modeling, and audit — the work that benefits from depth rather than speed, and that would otherwise compete with real-time processing for the same resources.

## Deployment freedom

The platform is a Kubernetes-based microservices architecture. It runs on AWS, Azure, or GCP, and it can be deployed entirely on-premise using open-weight models where data sovereignty requires it. For operators whose network topology and subscriber metadata cannot leave their perimeter, that is not a preference — it is a procurement gate.

## Elastic scale

A storm or a mass-outage event floods a monitoring system with alarms at exactly the moment it can least afford to slow down. The platform uses KEDA to scale collection and analysis workers against real-time demand, so processing capacity tracks the event rather than the average.

## 3. The fleet: what a digital employee actually is

Rapax is not a monolith with an AI feature bolted to the side. It is a set of specialized agents, each with a defined operational mandate, each pre-trained on carrier network protocols and operational practice, and each continuing to learn the specifics of the network it is deployed into.

The distinction that matters commercially — and the one most AI-in-the-NOC material blurs — is between what you can deploy this quarter and what is on a roadmap. Both tables below are real. Only the first one is purchasable.

### Available today

| Agent | Operational mandate |
|---|---|
| **Frank** | Frontline Response And Knowledge Navigator. Handles Tier 1 support interaction: classifies inbound tickets, answers from the knowledge base, closes what it can resolve, and routes what it cannot with the diagnostic context already attached. |
| **Wade** | Diagnostic engine. Executes troubleshooting procedures and remediation workflows for Tier 2 incidents, so that remote diagnosis happens before a truck is scheduled rather than after it returns. |
| **Grace** | Configuration compliance and alert communication. Tracks configuration state against policy and handles automated stakeholder notification during an event. |
| **Bruce** | Business Rules Upgrade Customization Engineer. Builds and deploys new device and system integrations, so adding a device type is a configuration task rather than a professional services engagement. |
| **Oscar** | NOC supervisor briefing. Summarizes the current operational picture — what is open, what changed, what needs a human decision — for shift handover and management reporting. |

### On the roadmap

The following are designed and specified but not released. They are described here so that the operating model is legible end to end. Nothing in this section should be read as currently deployable, and no performance figures are attached to it.

| Agent | Operational mandate |
|---|---|
| **Victor** | Incident controller. Detects the parent fault beneath a cluster of symptoms, determines the corrective action, and executes remediation or dispatch. |
| **Otto** | Network engineer. Interprets intended network changes and prepares scripts |

| Agent | Operational mandate |
|---|---|
| | for human-approved remote execution. |
| **Sheila** | Security and audit. Monitors the configuration and actions of both humans and agents against compliance frameworks. |
| **Ernie** | Energy optimization. Analyzes utilization and models cost against risk to suspend idle infrastructure. |
| **Richie** | Revenue integrity. Monitors the buy-to-bill cycle to detect and escalate provisioning and delivery errors. |

## 4. What a fiber cut looks like

The following is the designed response sequence. It describes how the platform is architected to behave, at full roadmap deployment. It is a design, not a measurement, and it is included because the shape of the workflow is the argument — not the stopwatch.

- Detection. The hot path receives the alarm burst as it arrives, rather than on a polling interval.
- Correlation. Symptomatic alarms from downstream elements collapse into a single service-affecting event with an identified parent cause, so the queue shows one incident rather than forty.
- Diagnosis. Remote diagnostics run against the affected path before any dispatch decision is made.
- Communication. Affected customers and internal stakeholders are notified from the correlated event, without a separate manual step.
- Briefing. The supervisor view reflects the current state continuously, so shift handover does not require reconstruction.

Under a manual triage model, the same sequence is serialized through one or more humans, and typically consumes 30 to 60 minutes before a dispatch decision is made. That range is drawn from operator practice, not from a controlled study — treat it as a planning figure, not a benchmark.

## 5. Carrier-grade resilience

An assurance platform that goes down during a mass-outage event is worse than no platform, because the operations team has by then reorganized around it. Rapax is built on an Active-Active multi-datacenter architecture: if one datacenter fails, the second maintains surveillance and automation without a failover gap.

The architecture is designed to a 99.999% availability target. That is a design target, stated as such. Availability achieved in any given deployment depends on the environment it is deployed into, and Rapax does not publish an availability figure it has not measured in that environment.

## 6. The honest counterpoint

There is a real case against everything above, and it is worth stating plainly.

- **Autonomy has a blast radius** — Autonomous remediation is a trust problem before it is a technology problem. An agent that can execute a change can execute a bad one. This is why the roadmap deliberately puts script preparation under human approval rather than autonomous execution, and it is a legitimate reason to phase adoption slowly.
- **Headcount does not move on software timelines** — The labor argument is often oversold. Reassigning operations staff is a multi-year organizational change, not a line item you realize in the first quarter. Any model that shows headcount savings arriving on the same schedule as the software is a model to distrust — including one presented by a vendor.
- **Garbage topology, garbage correlation** — Correlation quality depends on topology quality. If your inventory is wrong, the parent-cause identification will be wrong in exactly the same places. Operators with poor topology data should expect a data remediation phase, and should budget for it.
- **Vendor risk is real** — Rapax is a young platform from a small company. The counterweight is that the team has built and sold assurance software before — Assure1, acquired by Oracle in 2021 — but that is track record, not scale. An operator evaluating this should weight the try-and-buy accordingly and structure the evaluation to answer its own questions rather than ours.

## 7. What to do next

Whether or not Rapax is the answer, the underlying shift is not optional. Three actions are worth taking regardless of vendor:

1. Audit where the time actually goes. Instrument how many operator-hours per week are spent on correlation, triage, and status communication. Most operators are surprised, and the number is the business case.
2. Challenge each manual step. For every recurring operational task, ask what specifically requires a human — judgment, authority, or nothing but habit. The third category is larger than it looks.
3. Fix topology first. Automation amplifies data quality in both directions. Inventory accuracy is the prerequisite for every other item on this list.

### EVALUATE IT AGAINST YOUR OWN NETWORK

Rapax offers a fixed-price try-and-buy at $25,000 — a scoped deployment against your environment, so the questions above get answered with your data rather than a reference architecture.

sales@rapax.app · Book 15 minutes: cal.com/shawn-ennis

# Sources and notes

## Cited

- GSMA Intelligence, The State of Mobile — for the divergence between bandwidth demand and revenue per bit described in Section 1.
- AICPA Trust Services Criteria (SOC 2 Type II); NERC Critical Infrastructure Protection Standards; ISO/IEC 27001 — the compliance frameworks referenced in the roadmap description of Sheila.
- Cloud Native Computing Foundation — Kubernetes as the basis for horizontal scaling and self-healing described in Section 2.

## Deliberately omitted

An earlier version of this paper cited several industry statistics that could not be traced to a retrievable primary source, and attached measured performance figures to capabilities that have not shipped. Both have been removed. Where this version states a number, it is either an architectural target labeled as a target, or a planning range labeled as a range.

## Terminology

FRANK: Frontline Response And Knowledge Navigator. BRUCE: Business Rules Upgrade Customization Engineer.

Rapax is a business unit of Citus Technologies, LLC. Version 2.0, July 2026.