

— YOUR AI TEAMMATE FOR ITOPS

Stop watching dashboards. Work with a coworker that fixes them.

It reads your telemetry, tickets, Slack and email, works the incident end to end, and hands you the fix — or applies it itself. Infra issues resolve in minutes, and your engineers get **4x more done**.

Watch

Diagnose

Fix

Resolve

— THE PROBLEM

Another dashboard won't cover the night shift

More tools just mean more tabs. Your team still drowns in alerts while the real incident hides in the noise — and someone still gets paged at 3am. **You don't need more visibility. You need someone to do the work.**



Alerts arrive faster than anyone can read them

Every layer of the stack throws its own alerts for the same underlying fault. Nobody has time to work out that they are one problem before starting to solve it.



The real incident hides in the noise

Dashboards show you everything and prioritise nothing. The signal that matters is one line among thousands, and finding it is still a human task.



Someone still gets paged at 3am

More tooling has not changed who answers the phone. Visibility improved; the work of triage, diagnosis and fix still lands on a person.



Fragmented tools, fragmented ownership

Compute, storage, database and network each have their own console and their own on-call. An incident that crosses layers becomes a coordination problem before it becomes a fix.

— A DIFFERENT SIGNAL-TO-RESOLUTION PATH



— WHAT IT REPLACES

Grepping runbooks at 3am

Cross-team Slack pings

Dashboard hopping

Copy-pasting log excerpts into tickets

Waking the one person who knows this system

THE SHIFT

You don't need another dashboard. You need a coworker that reads what you already have and does the work.

— MEET THE CREW

Four specialists. Always on.

Each one owns a layer of your stack and knows exactly how to fix it. Every coworker runs at the resolution mode you set — autonomous, human-in-the-loop, or advisory — per pattern.

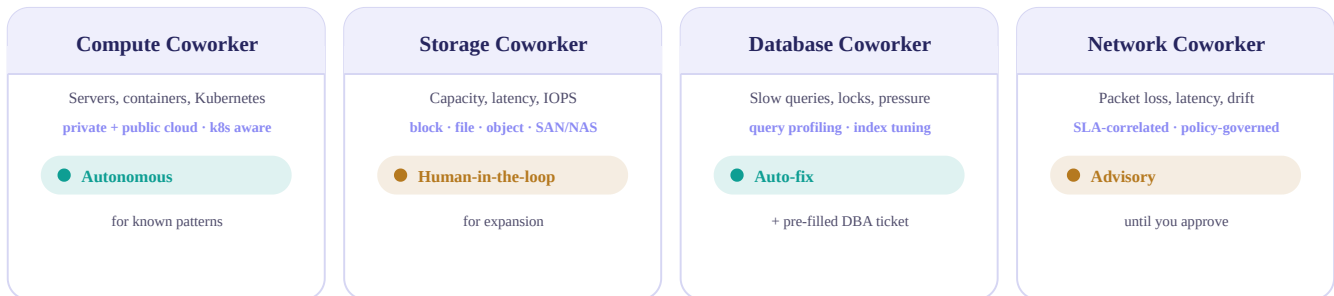
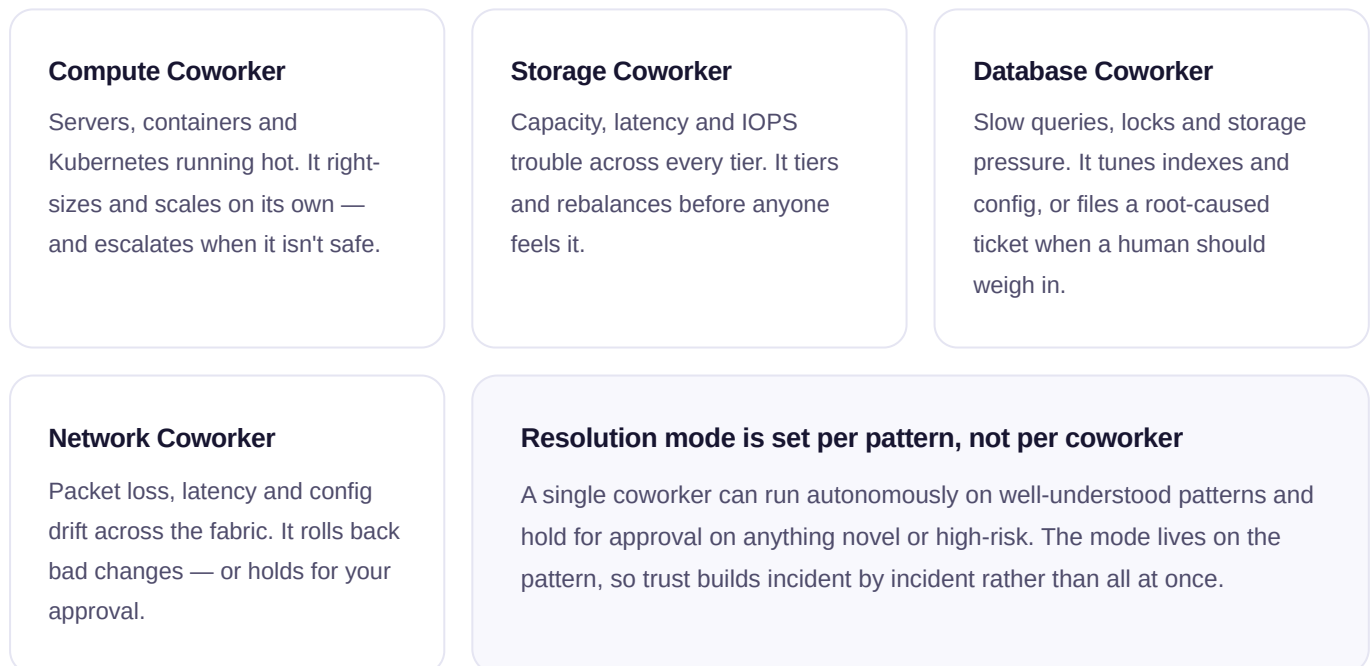


FIGURE — FOUR SPECIALISTS, ALWAYS ON



A generic agent knows a little about everything. A crew of specialists knows exactly what to do the moment it sees the signal — because it has seen this exact pattern before.

— ORCHESTRATION

The Lumi Orchestrator

Lumi turns fragmented signals into coordinated action. It ingests signals across the environment, correlates them into a single incident, determines the resolution path, and hands the fix to the right ITOps Coworker — coordinating multiple coworkers when an incident spans compute, storage, database and network.

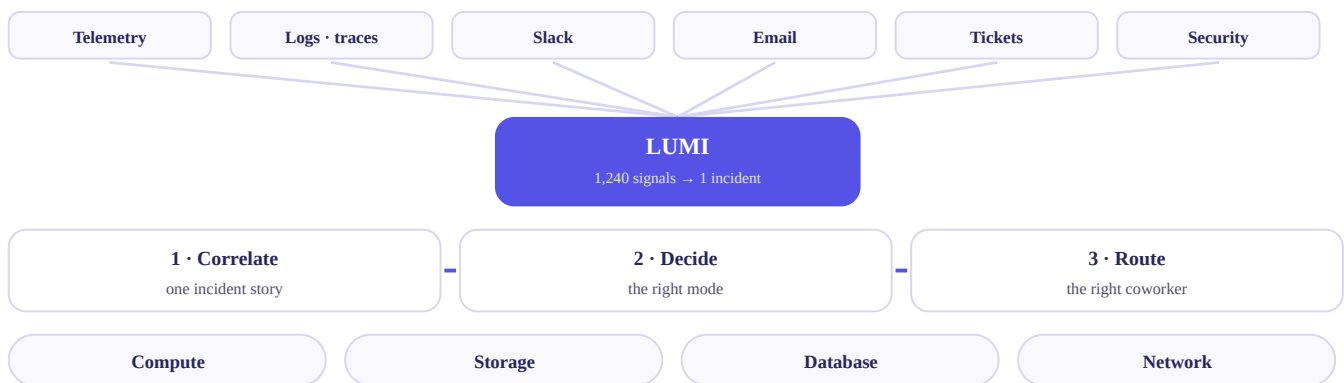


FIGURE — CORRELATE, DECIDE, ROUTE

1 · Correlate → one incident

Fans in device telemetry, logs, traces, tickets, Slack and email, and collapses thousands of signals into a single incident story.

2 · Decide → the right mode

Chooses autonomous, human-in-the-loop, or advisory for each pattern — always inside your guardrails.

3 · Orchestrate → the coworkers

Routes the fix to the right ITOps Coworker, and sequences Compute, Storage, Database and Network when an incident crosses layers.

— A CROSS-LAYER INCIDENT, COORDINATED

```

LUMI — ORCHESTRATE ● live

signal checkout-api p99 alert · storage IOPS warning · 2 Slack threads

# correlate: same window, same dependency graph
correlate → 1 incident: "checkout-api degraded, storage-fleet saturated"

decide --guardrails
  → Storage Coworker: rebalance tier → autonomous
  → Compute Coworker: scale checkout pool (+2) → autonomous
  → Database Coworker: pool near limit → human-in-the-loop

✓ rebalanced · scaled · DBA approved · resolved 4m50s
  
```

— THE PAYOFF

You get your **night back**

Same team, same stack — a very different on-call.

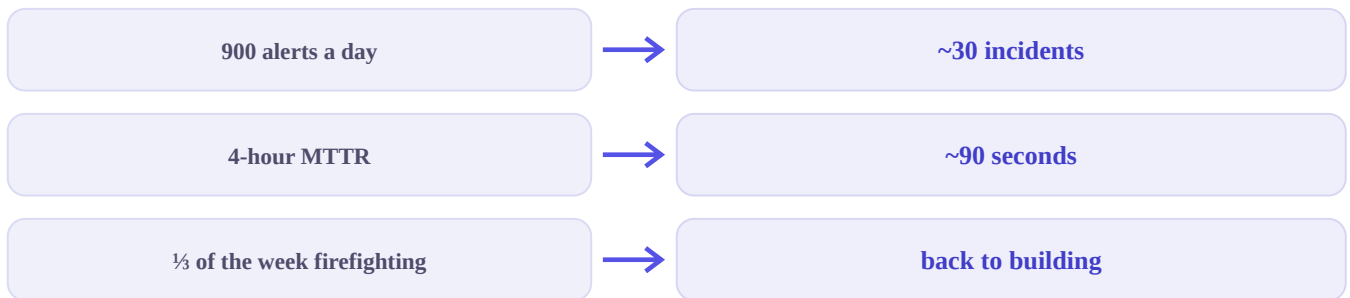
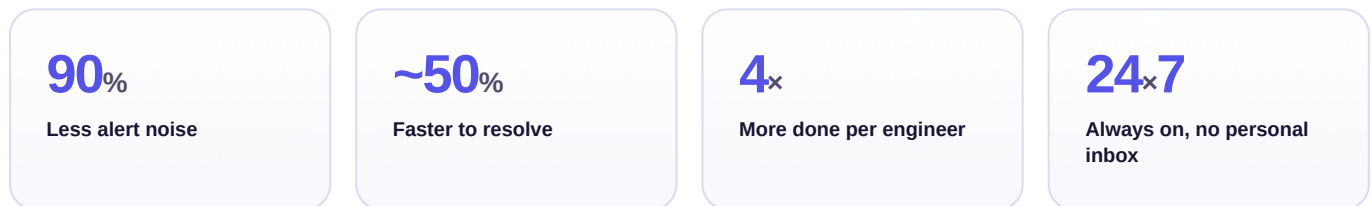


FIGURE — SAME TEAM, SAME STACK, A VERY DIFFERENT ON-CALL



Public AIOps benchmarks: up to 90%+ less alert noise, 40–60% lower MTTR, sub-second detection, and ~1/3 of engineering time freed from firefighting (ITIC, Forrester, New Relic, 2024–2026). Your numbers depend on your stack.

— WHY THE NUMBERS MOVE

Correlation removes duplicate paging

1,240 raw signals collapsing into one incident story means one page instead of dozens — the interruption a person actually experiences drops before any fix is applied.

Known patterns close themselves

Autonomous resolution on well-understood patterns means a share of incidents never reach a human at all — they open and close inside the guardrails you set.

Specialists skip the handoff

An incident that spans compute and storage no longer waits on two teams comparing notes — both coworkers work it in parallel, coordinated by the orchestrator.

SAME TEAM, SAME STACK

Nobody hired a bigger team. Nobody worked more nights. The work that used to fill a rota now runs in the background, on the estate you already have.

— WHO IT'S FOR

One coworker, every ops team's job

SRE

Thousands of alerts become a few real incidents — so you can focus on reliability.

ITOps & datacenter

Servers, network, storage and facilities in one view, watched 24×7.

ITSM & service desk

Tickets arrive pre-solved: root cause, impact and fix already filled in.

DevOps & platform

Every cloud in one console, tuned before problems reach production.

— WHY IT'S DIFFERENT

Better than a traditional "agent"

	TRADITIONAL AGENT	ITOPS COWORKER
Coverage	One generic bot	A crew of specialists for compute, storage, database and network
Awareness	Alert-driven	Context-aware — reads telemetry, tickets and email to find the real story
Control	All-or-nothing automation	Autonomous, human-in-the-loop, or advisory — per pattern
Governance	Bolted on afterward	Unified on CERNE — governed, compliant and cost-aware by design

● ● ● LUMI · INVESTIGATION SUMMARY

Why It Was Dismissed

Lumi's overnight orchestrator run correctly determined this alert was a **false positive** because:

1. **Current state is healthy:** Device pings successfully now
2. **No structural failure:** All 40+ monitored items are operational
3. **Resources are fine:** No CPU spike, no memory exhaust, no thermal throttling
4. **No correlation with changes:** No deployments, config edits, or recent incidents on this device
5. **No blast radius:** No downstream services reported impact

No action required. This is typical noise from edge router monitoring — intermittent ICMP loss over the Internet is normal; ICMP is not reliable enough for SLA-critical alerting.

— IN THE PRODUCT

An overnight alert, closed by Lumi in 36 ms as a false positive — with the five checks behind that call written out for whoever reads it next.

— A DAY WITH THE COWORKER

SRE

Overnight, 900 alerts resolve to 30 incidents. By standup, the ones that mattered are already annotated with root cause.

ITOps & datacenter

A rack's thermal drift is caught and correlated to a failing CRAC unit before the ticket queue even sees it.

ITSM & service desk

A user's slow-VPN ticket arrives with root cause, blast radius and a proposed fix — not a blank form.

DevOps & platform

A noisy-neighbour pod gets right-sized in the background; the on-call engineer sees the summary, not the page.

— TRUST & GOVERNANCE

Automation you can **actually** approve

Every action runs inside guardrails you set. Speed, without losing oversight.



Policy-governed
Define what's automated, what needs approval, and what stays advisory.



Full audit trail
Every decision, recommendation and change is logged and traceable.



Safe by default
Changes are policy-checked, and Lumi rolls back when something drifts.



Cost-aware
FinOps + GreenOps context weighs spend and sustainability, not just uptime.

— WHERE IT RUNS

AWS

Azure

GCP

Oracle Cloud

Private cloud

On-prem datacenters

Containers & Kubernetes

Facilities via DCIM & BMS

— RESOLUTION MODES, IN PRACTICE

MODE	WHAT HAPPENS	WHAT'S LOGGED
Autonomous	Lumi resolves the pattern end to end, no approval step	Full decision trail, evidence and outcome — reviewable after the fact
Human-in-the-loop	Lumi proposes the fix and waits for a named approver	The proposal, the evidence behind it, and the approval decision
Advisory	Lumi recommends only; your team decides and acts	The recommendation and whether it was followed

The mode is set per pattern, per coworker — and all three run on the same CERNE control plane that also governs LumiOps AI's SRE, Security and FinOps orchestrators.

THE PRINCIPLE

Guardrails are not a brake on autonomy. They are what makes autonomy something you can actually turn on.

— QUESTIONS, ANSWERED

Before you start building

Does Lumi replace my existing ITSM or monitoring tools?

No. Lumi sits on top of your stack and works with what you already run. Your ITSM stays the system of record while Lumi handles detection, diagnosis and resolution in the background.

Can I control how much Lumi automates?

Yes. You set the rules per pattern — fully autonomous for known low-risk issues, human-in-the-loop where you want an approval step, or advisory where Lumi only recommends and your team acts.

Which environments does Lumi support?

Public cloud (AWS, Azure, GCP, Oracle Cloud), private cloud, on-prem datacenters, containers and Kubernetes, plus facilities telemetry through DCIM and BMS.

How does Lumi handle security and compliance?

Every action is policy-governed and fully audited, and Lumi runs on the CERNE control plane so governance, compliance and cost-awareness are built in rather than added later.

1 · Connect

Point Lumi at your telemetry, tickets, Slack and email. No deep integration required to start.

2 · Set modes

Choose advisory or human-in-the-loop for every pattern to begin — nothing acts until you say so.

3 · Widen

Move proven patterns to autonomous as the record of clean resolutions builds.

BOTTOM LINE

See it take a real incident from alert to resolved — on your stack.

Meet the coworker who works the night shift.

Get a live demo, or talk to our team about ITOps Coworker for your estate.



GET IN TOUCH
lumiops.ai/contact-us



POC
~2 weeks to value



LINKEDIN
linkedin.com/company/lumiops