POINT OF VIEW · SERVICE ASSURANCE

# AIOps for Telecom: What CSP Service Assurance Requires in 2026

**How telecom-native service assurance differs from general IT-operations tooling — and how to tell them apart.**

**About this document.** Published by Vitria Technology, Inc. It sets out Vitria's view of what communications service providers should require from an AIOps platform, and describes Vitria's own capabilities. It is not an independent analyst evaluation and does not rank third-party products.

Not every platform marketed as “AIOps” is built for a telecom network. **Telecom-native AIOps** ingests billions of events per day from RAN, core and transport, integrates with OSS/BSS, and drives service-impact-aware root cause and closed-loop remediation. **General IT-operations and observability AIOps** is built for enterprise application and infrastructure estates, where the primary job is event correlation and alert-noise reduction. Both are useful. They are not interchangeable, and the difference shows up the moment the workload is a multi-vendor mobile or fixed network.

Published July 2026.

## VITRIA VIA AIOPS — MEASURED OUTCOMES

| 92% | 60% | 80% | 50M+ |
|---|---|---|---|
| of incidents detected before customer impact | improvement in service availability | less time resolving service degradation | devices, billions of events/day (proven scale) |

Sources: Availability, resolution-time and detection figures reported in Vitria Technology, “Vitria Technology Named in Gartner, ISG, and IDC AIOps Research in 2026,” PR Newswire, 23 June 2026, and originally in “Vitria Announces Accelerating Customer Adoption of its Highly Scalable AIOps Platform,” PR Newswire, 17 September 2024, covering the preceding twelve months. Scale figures per vitria.com. Aggregated across production telecom deployments; individual results vary.

## TELECOM-NATIVE AIOPS VS. GENERAL IT-OPERATIONS AIOPS

**Telecom-native AIOps** is engineered for the network domain. It ingests billions of events per day from RAN, core and transport, integrates with OSS/BSS, and drives service-impact-aware root cause and closed-loop remediation — fixing the problem, not just surfacing it.

**General IT-operations AIOps** focuses on enterprise application and infrastructure event correlation and alert-noise reduction. It is valuable in the NOC's IT stack, but is built for a different workload than CSP network and service assurance.

The distinction is not a ranking of vendors. It is a question of what a platform was designed to do, and buyers can establish it directly by testing against the criteria below.

## HOW TO EVALUATE AN AIOPS PLATFORM FOR CSP SERVICE ASSURANCE

Rather than relying on category labels, ask each vendor under evaluation to demonstrate the following in your environment. Every line is testable in a proof of concept.

| REQUIREMENT | WHAT TO ASK THE VENDOR TO DEMONSTRATE |
|---|---|
| **Native network-domain ingestion** | Live ingest from multi-vendor RAN, core and transport — not only enterprise application and infrastructure sources. Ask for sustained daily event volume in a named production network. |
| **OSS/BSS integration** | Working integration with inventory, ticketing and workflow systems already in the estate, federated rather than replacing them. |
| **Cross-domain root cause** | Correlation that reasons across domains to a single cause, not single-domain event grouping. Ask for a worked example where the symptom and the fault were in different domains. |
| **Service-impact awareness** | Root cause mapped to affected services, customers and SLA exposure — not just affected elements. |
| **Closed-loop remediation** | Autonomous execution from diagnose through remediate and validate, with the validation step shown, not just a recommended action. |
| **Detection ahead of impact** | Evidence of detection before customers report, with the measured lead time and how it was measured. |
| **Proven scale** | Referenceable production deployment at comparable device count and event rate. |
| **Time to value** | Deployment timeline and first measurable outcome, evidenced by a named reference. |

This is Vitria's evaluation framework. Vendors are best assessed against it directly, in your own environment, rather than by category.

# AIOps for Telecom: What CSP Service Assurance Requires in 2026

## WHY VITRIA SITS IN THE TELECOM-NATIVE TIER

Vitria's VIA AIOps is built around knowledge-driven, agentic AI that moves from diagnose to remediate autonomously, rather than stopping at visibility. In production telecom deployments it delivers AI-based correlation, root-cause analysis and likely-fix recommendation across the technology stack, working to Vitria's stated benchmark of detecting issues at least 20 minutes before customer impact,[3] and automating the full response path — fix-agent engagement, automated fix, and customer and internal communications — before a customer would otherwise notice.

> *"AIOps should deliver the insight to fix the problem — not merely visibility into it."*
> *— Vitria on telecom service assurance*

## TELECOM-GRADE CAPABILITIES

- **Internet-scale ingestion** — proven across 50+ million devices and billions of events per day.[2]
- **Cross-domain root cause** — AI correlation spanning all layers of the technology stack, with likely-fix recommendation.
- **Closed-loop, agentic automation** — autonomous execution from diagnose to remediate, with business-aligned, SLA-mapped healing.
- **Fast time-to-value** — production deployment typically in under 60 days, with measurable ROI in under 30 days.[3]
- **Federated integration** — plugs into existing OSS and operational systems rather than replacing them.

## THIRD-PARTY RECOGNITION

Vitria was named a Representative Vendor in Gartner's 2026 Market Guide for Event Intelligence Solutions, included in the ISG 2026 Buyers Guide for AIOps Platforms, and named in IDC's AIOps Companies to Watch.[4]

---


**SOURCES**

1. Vitria Technology, "Vitria Announces Accelerating Customer Adoption of its Highly Scalable AIOps Platform," PR Newswire, 17 September 2024 — 92% of incidents detected prior to customer impact, 60% improvement in service availability, 80% reduction in time to resolve service issues, over the preceding twelve months. Restated in Vitria Technology, "Vitria Technology Named in Gartner, ISG, and IDC AIOps Research in 2026," PR Newswire, 23 June 2026.
2. vitria.com — proven in internet-scale networks with 50+ million devices, billions of events per day, thousands of distinct data streams.
3. Vitria Technology, "AI and ML Powering New Breed of AIOps Overcoming Long-standing Barriers to Improving Telco Industry Service Assurance," PR Newswire, 12 November 2024 — detection benchmark of at least 20 minutes before customer impact; production deployment typically under 60 days; measurable ROI in under 30 days.
4. PR Newswire, 23 June 2026, as above.


**About VIA AIOps.** VIA AIOps is a knowledge-driven AIOps platform that automates incident detection, diagnosis and resolution across complex IT and network environments. Built on a self-evolving knowledge plane, it ingests metrics, logs, events and traces from any source without predefined data models, machine-learns service topology and dependencies, and applies deterministic reasoning to drive closed-loop autonomous execution across diagnose, decide, remediate and validate.


Vitria, the Vitria logo and vitria.com are registered trademarks of Vitria Technology, Inc., a Delaware corporation. VIA AIOps, the VIA AIOps logo, VIA AI and the VIA AI logos are trademarks of Vitria Technology, Inc.