QUESTIONS AND ANSWERS

# AIOps, the Gartner Market Guide, and VIA AIOps by Vitria

**Charlotte Patrick,** Independent Telco A3 Consultant interviews

**Chris Menier,** General Manager, VIA AIOps, VITRIA on the key characteristics of AIOps discussed in the Gartner Market Guide and how VIA measures up.

### Telcos are speaking and asking about AIOps. Could you define the term for us and talk about why you think there is this rising interest?

In the telco space, Vitria sees AIOps as analytics assisted operations. A mature AIOps deployment should unify operations across the networks, customer care, and IT. A robust AIOps deployment should be vendor and data stream agnostic with the goal of separating signal from noise and detecting and predicting service impacting issues before their customers do. That's really at the heart of AIOps or analytics assisted operations.

AIOps should uncover the probable root cause versus only identifying the symptoms and build the trust to enable analytic-driven automation and remediation.

Let me give a simple example. A link fails between two routers on a network and traffic is rerouted. But this causes congestion on the rerouted link, which then causes jitter, delay, and packet drops. Dropped packets cause API failures between virtual network functions. Those API failures cause service issues to device registrations. AIOps should correlate that link failure to the associated line card. Being topology aware, an AIOps solution should correlate the rerouted link to that same link failure and thus the jitter, delay, and packet loss. That same AIOps solution should correlate the VNFs as dependent on that link.

In today's operations, that doesn't happen. There would be multiple teams investigating these issues. With VIA AIOps, there would be a single incident created. All these signals would be correlated together, and the link failure determined to be the probable root cause, and perhaps automation implemented to reset the line card. The issue resolved before customers start calling.

### Vitria was cited in the latest Gartner Market Guide. What did Gartner see in your solution?

Foremost, we were able through our customers to demonstrate a quantifiable ROI. A tier one North American operator reduced their meantime to restore outages by 40% when our product had visibility to the data that described that service. More impressively, they were able to measure an 80% reduction in MTTR for impairments.

Impairments are harder to find. Outages are binary. They're off or they're on. But impairments, are nuanced issues. With our ability to correlate across the entire service delivery ecosystem, we're able to find those nagging issues, those impairments, those degraded service issues. I believe the delivery of quantifiable ROI is why we were chosen in the market guide.

### In the Market Guide, Gartner talked about anomaly detection and contrasted system centric and entity centric. Can you to give us a definition of terms here and an example of each?

It's an important distinction. System centric anomalies are degraded service such as buffering. This generally isn't caused by a single entity's failure. It's usually a combination of things. An entity centric anomaly is abnormal behavior or a fault that

can be tied to a specific device or host, like port utilization or CPU utilization on a router. It's very specific and can be pinpointed to the device that's generating it.

Entity anomalies only tell part of the story. There's an end-to-end relationship between systems and entities. For example, a fault or an anomaly on one entity may impact multiple services or symptoms. The same could be true where one symptom may be impacted by multiple, but separate entity faults. It's VIA's job to take an incident up approach versus a service down approach. We target those correlated incidents that might be resolved to restore the entity or services health. This gets to problem resolution prior to the customer experiencing issues, which is why the distinction is important.

### Gartner set out the characteristics of an AIOps platform. Could you please take us through these and just give us some examples from the VIA platform?

One of them is ***cross-domain data ingestion in analytics*** to provide a single pane of glass and unify operations. AIOps applications must be able to ingest, analyze, correlate across the full-service delivery stack. Without this, they'll just be relegated to another single purpose tool.

VIA clearly addresses this need by being, not just vendor agnostic, but data agnostic. Whether it's a trap or a log or a gNMI data directly from a device or model driven telemetry in a YANG, we're able to ingest that data across the entire service delivery ecosystem, then enrich and correlate it.

Another characteristic is ***topology***. Topology is assembled from both implicit and explicit sources. It's key in determining root cause and correlating different signals together. For Telcos, topology is very dynamic. As soon as you enter inventory into an inventory management system, it's out of date. We combine being taught topology from third sources and learning from the data itself.  VIA combines teaching and learning for topology to have the most accurate, the most up to date, enrichment.

***Correlation*** is key in an AIOps environment. AIOps must be a noise reducer and not a noise creator. So, this goes beyond simple de-duplication of faults. We nail this part. 99% noise reduction is generally what we see with VIA.  But VIA also detects anomalies in time series. And when we enrich that with inventory topology and service dependencies, that allows us to do true correlation, to get down to that single incident. Which leads into another Gartner definition, ***pattern recognition***. This is a way of getting smarter about anomaly detection and getting to root cause. It's child's play to find an anomaly in CPU utilization. Many vendors can do it. But understanding what caused that spike, that's what's important. VIA's use of AI and ML to generate baselines, an ontology approach to enrichment and the combination of human intelligence and artificial intelligence separates VIA from others.

Our goal is plainly stated. It's to detect, predict, action on service impacting incidents prior to widespread customer experience issues. And that leads to what Gartner refers to as ***probable remediation***.

VIA has the ability to recommend remediation in three ways. The first is through human feedback, quite simply, "Hey. We've seen this before. What action did Bob take?" And that's stored in, what we call, a digital fingerprint. The second is through integration with incident management systems. If the Telco's remediation is captured in a downstream incident management system, we ingest that and we learn from it. And then finally through industry experience. And this is something that's unique to VIA. Since we've seen so many use cases across different vendors, we deliver vendor best practices out of the box. For example, Cisco has technical support playbooks. If we've identified a Cisco entity as the probable root cause, we know what Cisco technicians would do. And that is informed right down through our incident creation.

### One of the top three AI topics is explainability. And Gartner claims that most AI tools today are mostly still in black box mode. So how are you ensuring that this is not the case with VIA?

The industry's evolved from data warehouses to very well-tuned black box algorithms to give some answers. But streaming data may not be like what was used to create the algorithm. It was likely created using static data in a clean environment. The realities of streaming data that's constantly changing are much different.

With VIA, we took a clear box approach. Although we have out of the box algorithms and settings, users can override these to match their operational best practices. We take an approach called progressive disclosure that allows the user to drill into why a detection occurred, why a baseline was generated the way that it was, why signals were correlated, why this root cause was identified. It's all there. And it's all adaptable to operational best practices. This approach builds trust and instills confidence in operations teams to use analytics to automate.

**Totally agree. Root cause identification on the network is just getting increasingly difficult because of the complexity. Gartner talks about topological analysis and contextualized topological analysis to improve the identification of cause. Could you just talk about how that is being tackled within VIA?**

Complexity has moved beyond mesh networks to virtual network functions that are containerized in Kubernetes environments, and those are deployed across physical infrastructure. To handle these dynamic environments, VIA takes, what we call, our ontology approach to enriching data streams.

This means you don't have to know the relationships that may exist between a stream of data and an entity or a network link. We learn this information from the data as we see new dependencies created, between a container and a VM, or between a VNF and its name space in a Kubernetes environment. Every data stream that's analyzed by VIA will be contextualized with this known topology and service dependencies. And that happens in real time. This context informs our correlation algorithms and helps understand which faults and performance anomalies should be correlated and then analyzed for root cause.

**In any market guide, there's many platform providers. What differentiates Vitria's VIA AIOps?**

We help operators and enterprises unify operations. And one of the first steps is combining fault and performance management into a single application. We can ingest and analyze across that service delivery ecosystem. From logs and traps and any format of time series. Second is our ontology approach. Our ability to dynamically enrich data streams with inventory data, makes, models, data centers, and things. The standard network topology, as well as the more complex topologies seen in virtualized environments. Finally, service dependencies, what services or systems are running across these elements that may be impacted when there's an entity impact.

Another differentiator is our analytics approach. We use unsupervised machine learning to generate more accurate baselines. We generally look at months of data to get accuracy, but we continue to learn as new data comes in all the time. And we go beyond the simple threshold crossing alerts. We go down to intra-day seasonality, down to that entity or sub-entity, to get accurate baselines and detect accurately. And then in the analytics side, our ability to use stochastic models makes us resilient to volatility that happens in this data.  All that gives us a more sophisticated approach as compared to other AIOps vendors. Finally, we're proven quantifiable results that come directly from our customers. Our customers' ability to quantify our impact speaks to our ability to deliver.

**We need quite a lot of AIOps support now and in the future to support increasing complex environments. Chris, it's been great to speak to you. Thank you very much.**

## About VIA AIOps

VIA AIOps easily integrates with monitoring systems located in silos across the service hierarchy. Enabled by explainable AI, VIA prescribes remedial actions to the designated system of action and predicts problems before they impact customers. VIA AIOps can be deployed from the cloud, on premises or in hybrid operating environments.