anodot

Top barriers to successful AI implementation

To guarantee their competitiveness, CSPs are opting for advanced AI-based network monitoring solutions. But alongside its promise, AI poses major technological, operational and management-related challenges and costs. Hitting the ground running with AI requires a well-defined adoption strategy and methodology. We present the major adoption barriers and best practices for avoiding them to achieve fast time to value and increase ROI from your AI investment.

Smart CSPs are investing in AI

The telecom industry is in the midst of a massive shift to new service offerings enabled by 5G and edge computing technologies. With this digital transformation, networks and network services are becoming increasingly complex: RAN, Core and Transport are only a few of the network's many layers and integrated components. Today's telecom engineers are expected to handle, manage, optimize, monitor and troubleshoot multi-technology and multi-vendor networks. The biggest challenge is balancing the innovation that pushes for new technologies, layers and nodes with the need to provide robust, high quality products and services 24/7, 365 days a year.

That's why smart communications service providers (CSPs) are investing in AI. By cutting time to detection, reducing false alarms and alert storms, and providing the context for the shortest time to resolution, AI solutions enable CSPs to ensure availability and reliability, deliver more business value, and stay ahead of the competition.

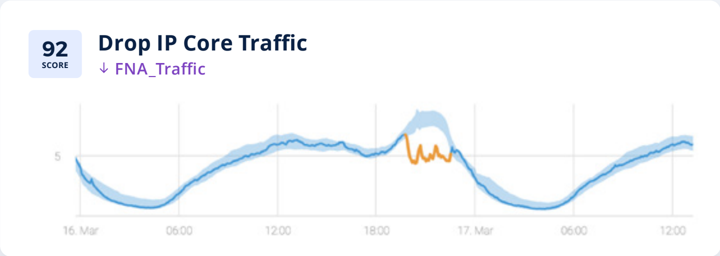
CSPs need to stay on top of hundreds of metrics, but with the ongoing growth in operational complexities, effectively managing and monitoring connections, devices, radio networks, current and legacy core networks, services, and transport and IT operations is becoming a radical challenge. Static network monitoring gives rise to billions of alarms with a very high rate of false positives, since it's based on manual thresholding for a system that is too complex and volatile to adhere to predetermined states. What is worse — static monitoring leads to late detection of service degraragation and incidents. Even after detection, which often occurs after the incidents have already impacted customers and appear in downdetector, there is no context to go on for expedited resolution.

Compared to manual, dashboard-based monitoring systems, ML enables unprecedented scale, accuracy and speed. It enables today's telecom engineers to handle, manage, optimize, monitor and troubleshoot multi-technology and multi-vendor networks. Machine learning enables CSPs to move from reactive problem solving to proactive monitoring and learn more about what is happening across their networks before any minor issues escalate into bigger problems.

In the network operations context, every network generates millions of time series data, measuring all aspects of the network. Anomalies can cause service degradations and system-wide outages/incidents. Therefore, discovering these anomalies and identifying the technical root cause to fix incidents is a key objective of network operations. Autonomous anomaly detection minimizes time spent looking for issues, leaving more time to focus on resolution.

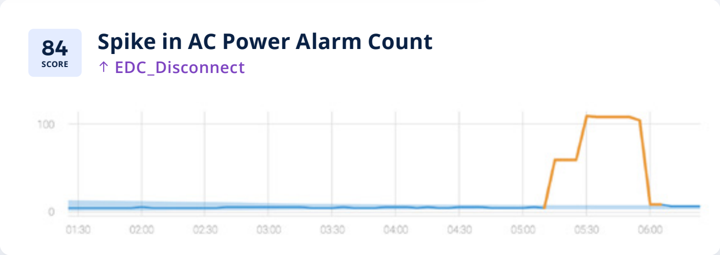
AI enables the transformation of traditional network and service operations towards automation and intelligent operations through three crucial steps that can only be achieved by applying cutting edge machine learning: anomaly detection, correlations and root cause analysis, and, finally — remediation.

Autonomous alerts generated by Anodot



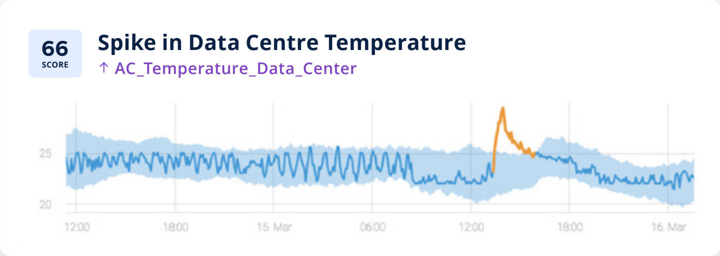
Drop IP Core Traffic

↓ FNA_Traffic



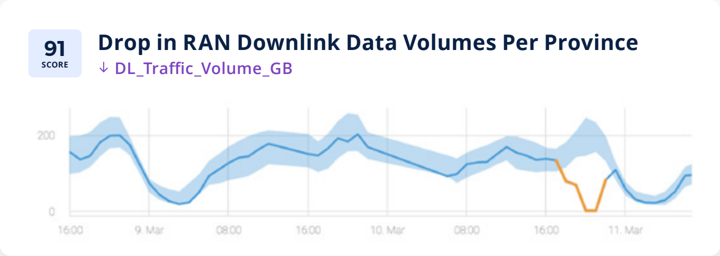
Spike in AC Power Alarm Count

↑ EDC_Disconnect



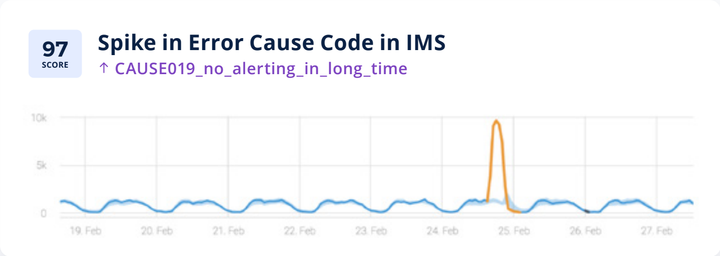
Spike in Data Centre Temperature

↑ AC_Temperature_Data_Center



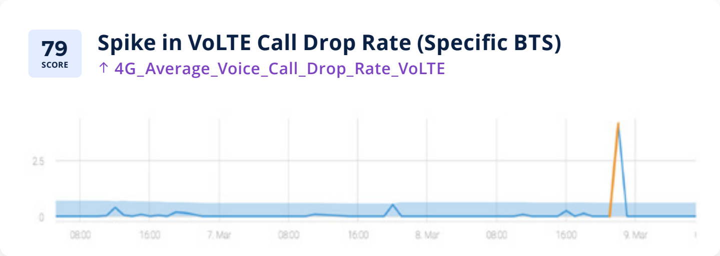
Drop in RAN Downlink Data Volumes Per Province

↓ DL_Traffic_Volume_GB



Spike in Error Cause Code in IMS

↑ CAUSE019_no_alerting_in_long_time



Spike in VoLTE Call Drop Rate (Specific BTS)

↑ 4G_Average_Voice_Call_Drop_Rate_VoLTE

The high stakes of AI adoption

According to a recent research by McKinsey, telecom companies are amongst the leading adopters of AI, demonstrating the most aggressive AI investment intentions across verticals. CSP leaders' adoption is both broad and deep, building on multiple technologies across multiple functions, with deployment at the core of their business. Compared to partial- or non-adopters, CSPs with a proactive AI adoption strategy have significantly higher profit margins.

Not only do serious AI adopters with proactive strategies report current profit margins that are 5-7 percentage points higher than the industry average (partial adopters -2.5%, non adopters -5%), but they also expect this advantage to grow as the AI investment matures and starts paying substantial dividends. Over the next three years, these AI leaders expect their margins to increase by up to five percentage points compared to the industry average.

While the promise of AI is great, so are the challenges associated with implementing AI at scale, and, especially, of successfully moving AI applications beyond prototypes - an endeavor which only a fraction of companies trying to implement AI achieve. According to Gartner, 85% of AI projects ultimately fail to deliver on their intended promises to business. Multiple factors contribute to the high failure rates of bringing AI to production and positive ROI. Most prominent are the inherent complexity of AI solutions, multiple data challenges in training and production, and implementation challenges.

85%

of AI projects ultimately fail to deliver on their intended promises to business

20%

of companies currently use AI technologies in a core business process

According to Gartner, few organizations successfully move their AI model prototypes into production, with only about 20% of companies currently using one or more of its technologies in a core business process or at scale. Only 1 in 10 organizations are able to get 75% or more of their AI model prototypes into production, according to the Gartner AI in Organizations Survey.

Why the disconnect between the ROI promise of AI and high failure rates?

Top barriers to successful AI implementation

Attempt to build it

Many telecom companies attempt to build ML solutions internally from scratch, but the build option poses multiple conceptual, technical and resource challenges. Hiring consultants and system integrators, investing in internal IT, devops, dataops, and data science resources, and building off of packaged software present not only costs but also staffing challenges and potential pitfalls that hinder a comparable return on investment. Even after investing the above resources, the final solution's performance will usually fall behind that of dedicated solutions. Under par results will inevitably translate into less accurate detection, longer time to detection and resolution, and more noise. In addition, homegrown solutions usually struggle to scale with the business.

Long time-to-value

Depending on the robustness of the solution you chose to pursue, some build scenarios could take more than four years to develop, particularly for complex and changing monitoring needs. The complexity of autonomous monitoring also makes it extremely expensive to build. Estimates show that developing a data-driven enterprise ML application can cost upwards of $14 million USD. Given that real-time monitoring is at the cutting edge of computer science, your project might greatly exceed that figure. If you are building your own solution you should expect an exceedingly long time to value.

Data scope or quality

As data quality and compatibility overwhelmingly determine the solutions' results, mitigating the ongoing challenges it poses for ML systems is a science in its own right. This is doubly true for CSPs working with multi-technology and multi-vendors systems that create thousands of separate data streams that are often siloed. Maintaining data stability and coherence in production is an ongoing concern, even for the most solid of ML models.

Integration complexity

Multi-domain CSP environments rely on siloed systems that create major integration complexities. Disparate legacy systems developed to solve tactical problems further complicate data consolidation processes. That's why even tech-savvy companies using advanced analytics stacks manage to monitor only a small percent of the data created, collected and stored by the business. According to Forrester, on average, between 60% and 73% of all data within the enterprise go unused for analytics. But analyzing data from disparate systems dramatically decreased monitoring efficiency. When streams are siloed or cannot be ingested by the solution, holistic visibility is sacrificed as well as the systems' ability to correlate across relevant metrics and dimensions. Only by monitoring, analyzing and correlating between 100% of the CSP data can a solution create the transparency and confidence needed for robust incident detection and resolution.

Poor ML Performance

Poor ML performance in production is associated with high costs. ML solutions that are not accurate, granular or robust typically do not benchmark well on false positive rate, false negative rate, and detection and resolution delay. False positives (which often escalate to alert storms) weigh down NOC teams and create alert fatigue that often leads to missing critical incidents. False negatives — whether it's a major issue, a degradation of service, or a slow leak - will negatively impact your customers and revenue. Detection & resolution speed depend on a fine-tuned ML model that also provides the context and root cause analysis that enable teams to quickly identify the core problem and attend to it.

Overcoming the challenges

Hitting the ground running with AI requires a well-defined adoption strategy and methodology. In order to overcome implementation barriers and successfully deploy AI to production, CSPs need to adopt the following strategies.

Buy it. Don't build it. As mentioned above, building a cutting edge monitoring and detection system is extremely time and resource heavy, with a high failure rate. In addition, there is fierce competition between tech giants for the limited number of skilled AI professionals required for such an undertaking. AI vendors with dedicated teams of data scientists, algorithm engineers, and data ops engineers can handle the majority of the heavy lifting for you, providing better, faster, and cheaper systems.

Accelerate time to value. Opt for solutions that enable shorter time to value from your AI investment. Multiple factors may hinder ROI from AI: long development / implementation / integration processes; sub-par systems that are not robust or accurate enough to deliver on their promise; use-case dedicated solutions that fail to scale / adapt to new and evolving use cases. Choose to adopt a solution that allows you to get ever increasing value from the product, independently of vendors or internal IT or data resources.

Eliminate AI and data integration complexities. Opt for AI solutions that can solve the data and integration complexities inherent to multi-domain CSP environments. Only solutions that can handle disparate data sources and multiple types of data/signals so that 100% of your data is monitored and analyzed can provide true incident detection across the network in all its permutations.

Opt for proven ML performance. Monitoring solutions vary widely in their performance. KPIs you should consider are: Early detection — the average time required to detect an incident; Spot on alerts — accurate and relevant alerts that cut false positives and alert storms on the one hand but don't fall for the false negative trap on the other; context and correlations — the solution's ability to provide root cause analysis to expedite time to resolution; and finally, robustness and scale — monitoring 100% of data with no limit to data streams or metrics. Your monitoring solution needs to provide spot on alerts with the context that lets you know what is happening, where and why as soon as possible, for lightning-fast resolution.

EMEA Telco NOC went from 50,000 alerts per day to under 50 with Anodot

1,565,548,853	›	*3,979,802*	›	*82,806*	›	*2,776*	›	*37*
Total processed samples		*Total number of metrics*		*Single metric anomalies*		*Correlated anomalies*		*Alerts*

Key Success Criteria and Requirements for ML monitoring

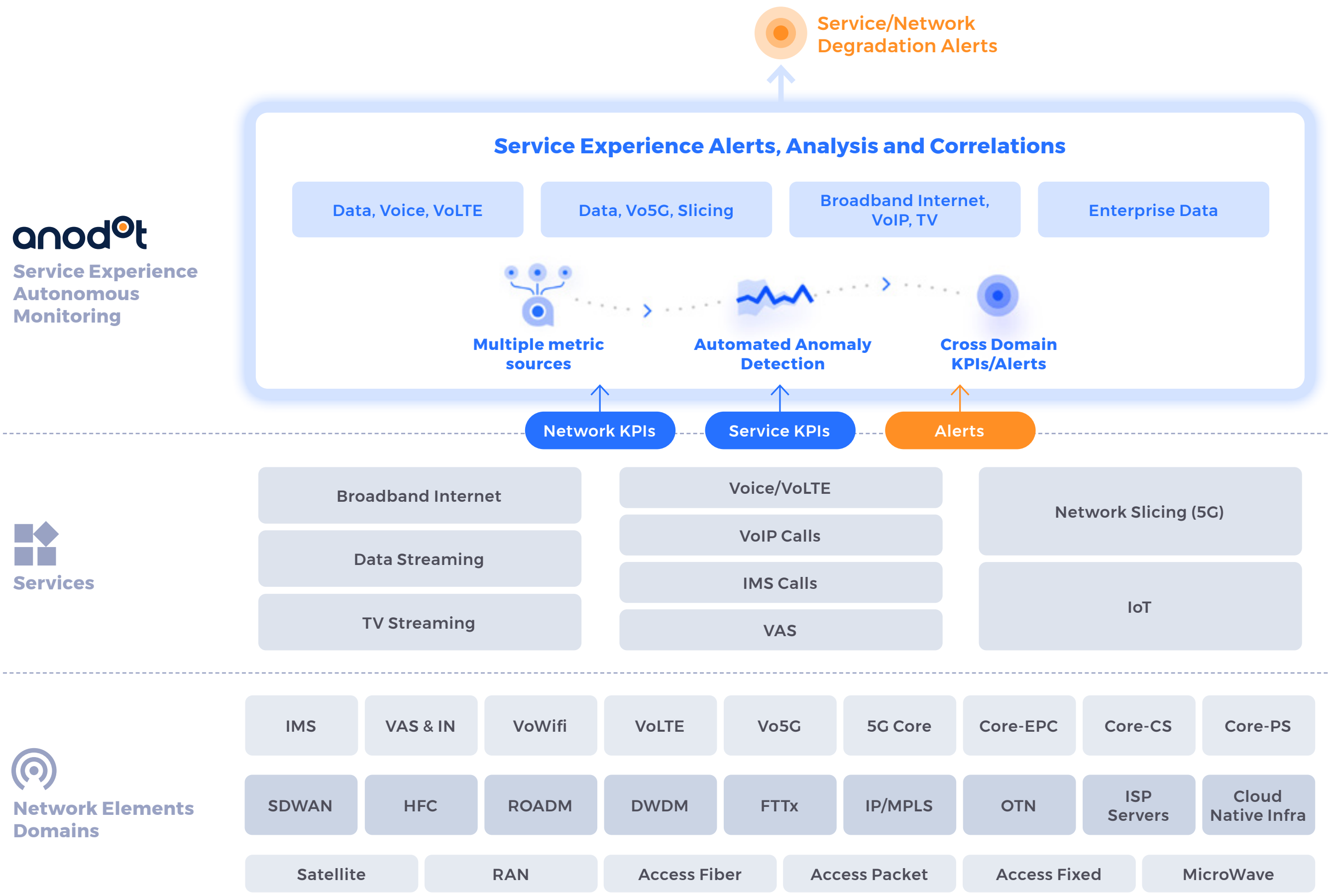
Success Criteria	Requirements
Reduction in mean time to detect network issues	• Anomaly detection applied on 100% of the network performance metrics. • Near real time detection.
Reduction in mean time to repair	• Autonomous correlation of all related anomalies and events. • Collect data from multiple network sources. • Autonomous learning of remediation actions.
Reduce false positives	• Robust and accurate ML based anomaly detection algorithms. • Context aware anomaly filtering. • Semi-supervised learning algorithms based on feedback
Reduce number of alerts on the NOC	• Autonomous alert correlation based on ML
Short time to value	• Minimal customization required. • Auto-ML: No data science knowledge required. • Great product usability. Easy integrations to multiple data sources.

Anodot Autonomous Network Monitoring

Anodot enables CSPs to monitor all network types (e.g., Mobile, Fixed, and Transport) and network layers to identify impacted services and customer experience in real time. This helps operation and NOC teams become proactive in their ability to identify service degradations and outages, improving network availability and customer experience.

Anodot ingests data from 100% of the network's data sources in real-time, including siloed network operations and customer experience systems. It uses patented algorithms to continuously monitor and analyze millions of KPIs, translating monitoring measures to service experience and KPIs to service impact. Anodot's unique algorithms correlate between network layers and types across billions of data points to provide early detection of service degradation across the entire telco stack. Stakeholders receive Anodot's alerts in real-time with the relevant anomaly and event correlation for the fastest root case detection and resolution.

Anodot gives CSPs the power to see across domains and understand real service experience by transforming measure-based monitoring to service experience. CSPs use Anodot to build resilience and service experience into their networks, prevent and mitigate outages and service degradation, save costs and drive operational efficiencies, providing better customer experience, and learning more about what is happening across their networks. With Anodot, CSPs grow more revenue, ensure customer satisfaction, and forecast the future — which is now looking better than ever.


Service/Network Degradation Alerts
Service Experience Alerts, Analysis and Correlations
Data, Voice, VoLTE
Data, Vo5G, Slicing
Broadband Internet, VoIP, TV
Enterprise Data
anodot
Service Experience Autonomous Monitoring
Multiple metric sources
Automated Anomaly Detection
Cross Domain KPIs/Alerts
Network KPIs
Service KPIs
Alerts
Services
Broadband Internet
Data Streaming
TV Streaming
Voice/VoLTE
VoIP Calls
IMS Calls
VAS
Network Slicing (5G)
IoT
Network Elements Domains
IMS
VAS & IN
VoWifi
VoLTE
Vo5G
5G Core
Core-EPC
Core-CS
Core-PS
SDWAN
HFC
ROADM
DWDM
FTTx
IP/MPLS
OTN
ISP Servers
Cloud Native Infra
Satellite
RAN
Access Fiber
Access Packet
Access Fixed
MicroWave