Case Study

Leading Telcos Monitor OSS, BSS and CEM Operations with Anodot; Saving Millions of Dollars Annually

Autonomous Telco Monitoring ROI

$10.3M-$39.7M
saved annually by early detection of incidents*

89%-97%
reduction in time to detection

90%
reduction in total number of alerts

75%
reduction in the number of non-actionable alerts

50%
reduction in workload on support operations

30%
improvement in customer satisfaction scores

* For a telco operator with annual revenues of $1B

What Telco customers say about Anodot

T · ·Mobile·

Identify bottlenecks and drive improvements

> *"Anodot dramatically streamlined our process. Collecting more granular data throughout the incident lifecycle helped us identify bottlenecks and drive improvements. We could pinpoint the root cause of issues with certainty, saving frustration and critical staff resources."*

Antal Kovácsovics
Head of IT Service Management Centre at Telekom HU

Decrease operational complexity and solve incidents sooner

> *"We have a great collaboration with Anodot. Their automatic detection gives us prior warning about possible incidents an hour or two before they create an impact on customer experience, and allows us to quickly capture and address these problems."*

Dr. Kim Kyllesbech Larsen
CTIO at T-Mobile Nederland

T · ·Mobile·

OPTUS

Optimize customer experience and business operations

> *"We find Anodot's technology invaluable in identifying issues and opportunities buried deep in the data streams of different business and IT sources to optimize our customer experience and our business."*

Jason Wong
Director of Network Analytics at Optus

Modern telco operations are too complicated for manual monitoring

Telco infrastructure is a complex heterogeneous network. Typically, a wireless network has tens of thousands of base stations, a few hundred thousand cells, thousands of sites operating multiple frequency bands, multiple flavors of transport networks (Microwave, Ethernet, optical), thousands of core network nodes, multiple service networks (SMS, MMS, voice), network policy engines, Internet peering links, Content Delivery Networks (CDNs) and many other network elements.

In order to optimize operations, ensure availability and reliability and deliver more business value, Telcos 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.

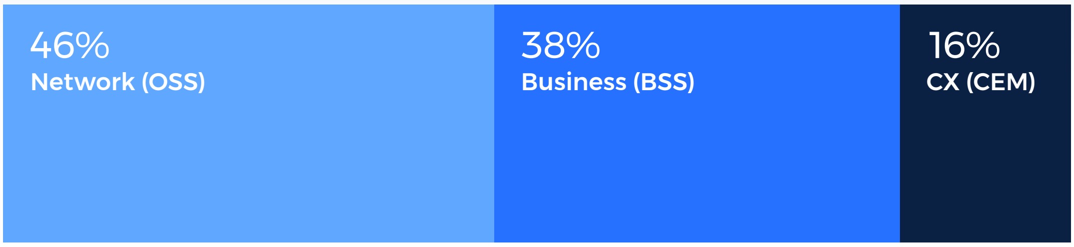
As networks become increasingly complex and service providers plan for more complicating factors — new devices on the network, 5G, increased cloud-based services and more — operators want to reduce manual monitoring and increase network automation. On the BSS side, telecoms need to manage a wide range of products, campaigns, retail channels, prepaid and roaming services, billing, customer experience and support, and order and fraud management operations. But monitoring these metrics is crucial for ensuring that underlying business support systems enable profitability and growth.

Revenue and cost data is too volatile for static monitoring. Since business data is so complex and dynamic, AI/ML-based autonomous solutions are critical for achieving business outcomes and avoiding blind spots. Static monitoring approaches based on dashboards and manual thresholds aren't sensitive, robust or agile enough to withstand this challenge. To keep business on track, AI-based early detection of revenue issues and business system failures is non-negotiable.

Reducing opex and incident costs with Autonomous Monitoring

Despite the fact that networks are being built with nodal and geographic redundancies, telecom networks nonetheless suffer a variety of outages and network incidents. These incidents impact network, business, and customer experience management operations.

Distribution of Telco Incidents as a percentage of Total Incident Costs



According to a 2013 report from telecom research firm Heavy Reading, these incidents cost the world's mobile operators around $15B a year, or an average of 1.5%-5% of their annual revenues. These figures are growing year over year.

For a telco operator with an annual revenues of $1B, annual incident costs can range between $11.6M-$41.1M, depending on the types of systems used for monitoring. The table below shows the impact of undetected and late detected incidents drawn from actual results of Anodot's telecom customers. Of particular note are the cost of medium-and low-severity anomalies. These far outweigh the cost of high severity anomalies. Lower severity anomalies are frequently harder to detect and last longer than their high severity counterparts, thus having a greater impact on true costs over time.

Improving overall time to detect invariably leads to quicker resolution of incidents and thus results in reduced costs associated with outages, and aids in the prevention of lost revenue and brand impact. According to a recent Cisco report, the automation of incident management can reduce opex costs by 3-7%. Cisco's figure lines up with our own ROI calculations based on our customer data. Anodot saves its telco customers anywhere between $10.3M-$39.7M annually by early detection of incidents and the prevention of revenue loss.

Annual Telco Incident Costs and Savings with Anodot's Autonomous Monitoring

For a telco operator with annual revenues of $1B

Incident Impact ››	High	Med	Low	Total
Avg. number of Incidents per Year	12	36	192	**240**
Revenue Loss per Minute	$32,610	$3,260	$870	
Static Thresholds				
Avg. TTD	48 min	76 min	80 min	
Incidents Cost	$18,783,360	$8,919,360	$13,363,200	**$41,065,920**
Competitor's Anomaly Detection				
Avg. TTD	14 min	21 min	22 min	
Incidents Cost	$5,478,480	$2,464,560	$3,674,880	**$11,617,920**
Anodot's Autonomous Monitoring				
Avg. TTD	2 min	2 min	2 min	
Incidents Cost	$782,640	$234,720	$334,080	**$1,351,440**
Anodot Savings over Static Thresholds	$18,000,720	$8,684,640	$13,029,120	**$39,714,480**
Anodot Savings over Competitor's Anomaly Detection	$4,695,840	$2,229,840	$3,340,800	**$10,266,480**

Based on actual results of Anodot's telecom customers

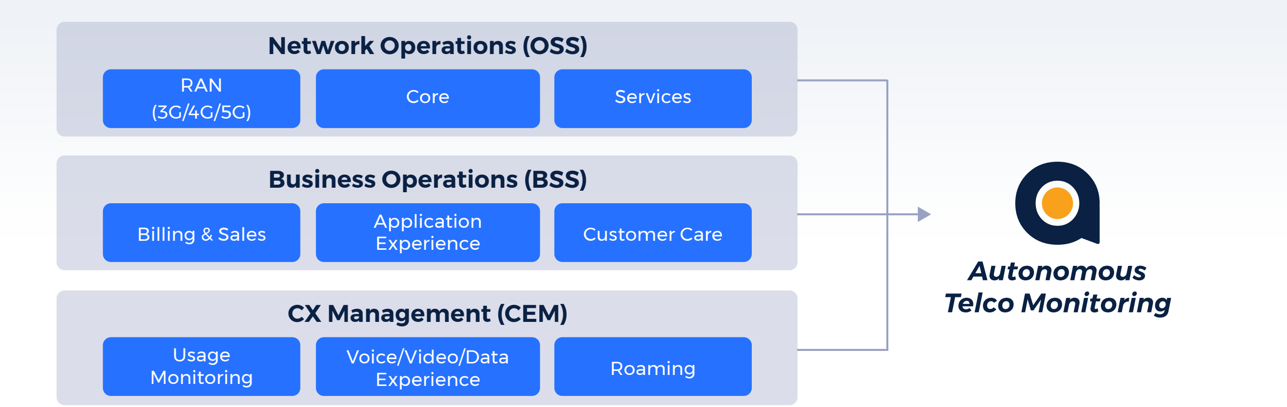
In addition to the significant cost savings outlined above, telecom operators using Anodot's autonomous monitoring solution typically experience:

- **89%-97% reduction in time to detection when compared to alternative approaches**
- **90% reduction in the total number of alerts**
- **75% reduction in the number of non-actionable or false positive alerts**
- **50% reduction in load on support attributable to the reduction of alerts, proactive detection of incidents and root cause analysis**
- **30% improvement in customer satisfaction scores**

Autonomous Telco Monitoring

Anodot is capable of ingesting data from siloed network operations and customer experience systems, and autonomously analyzing millions of KPIs using patented algorithms to provide early detection across the entire telco ecosystem. Anodot delivers the right alerts to the right stakeholders, saving valuable investigative time and accelerating root cause detection through anomaly and event correlation.

Over the course of the past 12 months, several large telco operations have been using Anodot's autonomous monitoring technology for the fastest detection and resolution of incidents across OSS, BSS and CEM operations.



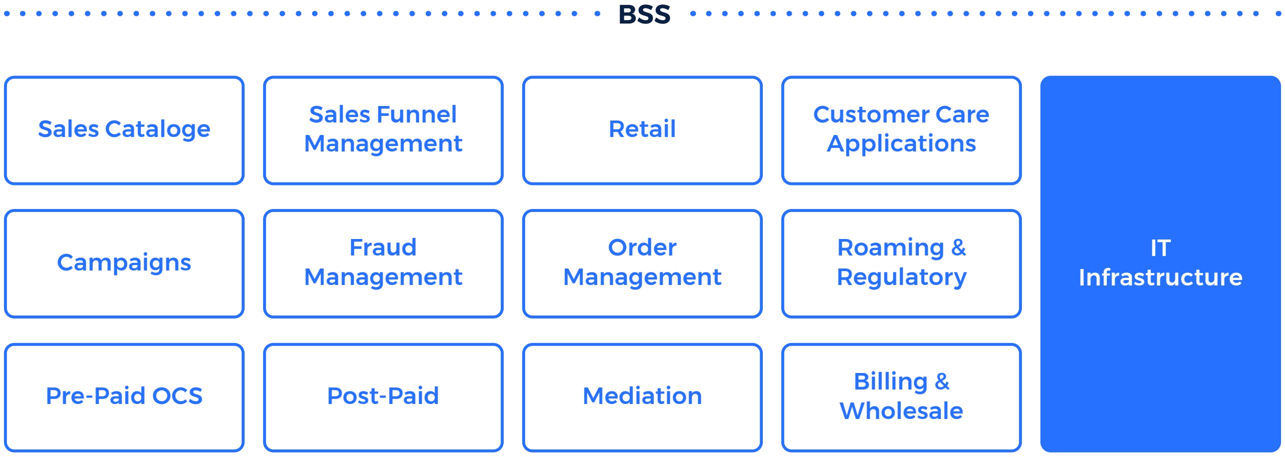
OSS Monitoring

Anodot is used by telecoms to monitor their network operations at scale, including:

- Radio Access Network (RAN), where failures in any part of the RAN networks must be quickly and accurately assessed so that field teams can be coordinated to deal with the root cause quickly.
- Transport Networks, where degradations such as increase in packet loss, increase in jitter, and latency often have direct impact on subscriber experience.
- Core Networks, complex multi-vendor networks with multiple scenarios, multiple interactions and interfaces—making them impossible to monitor using traditional dashboards, alarms and thresholds.
- Service Networks, where degradations are quickly noticed by end-users and impact brand image and subscriber experience.
- Fixed Broadband Access Networks, complicated mix of technologies such as fiber to the premise/node/curb, DSL, HFC, WiFi and even Satellite Broadband. In each of these cases, subscriber uplink and downlink throughput drops, packet loss, modem resets, and many other KPIs need to be monitored in real time to ensure the most significant anomalies are discovered rapidly to avoid unnecessary and expensive truck-rolls.

BSS Monitoring

Anodot is used by leading telecoms to monitor at scale their BSS operations — including billing, sales, provisioning, application experience and customer care — to provide a competitive edge by optimizing business processes, reducing customer care costs, improving brand and network quality, and consequently improving customer experience.



BSS

Sales Cataloge

Sales Funnel Management

Retail

Customer Care Applications

Campaigns

Fraud Management

Order Management

Roaming & Regulatory

Pre-Paid OCS

Post-Paid

Mediation

Billing & Wholesale

IT Infrastructure

CEM Monitoring

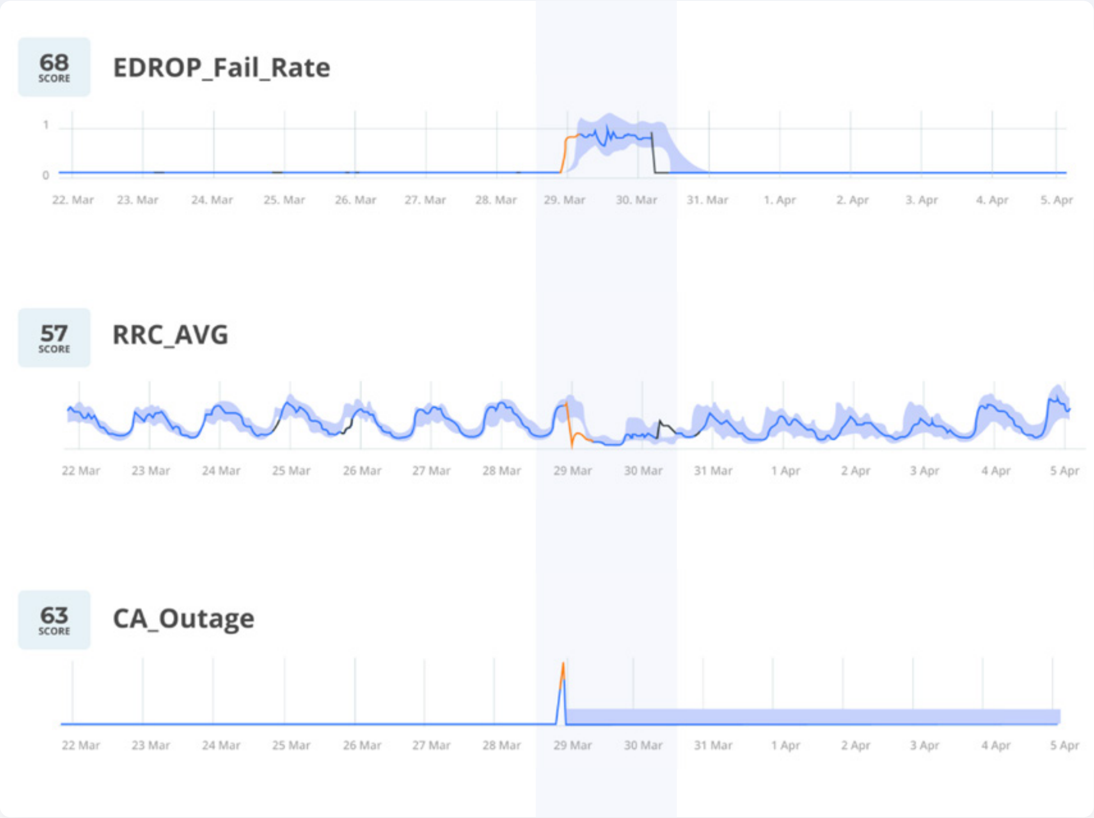
On the Customer Experience Management side, Anodot is used by leading telecoms to monitor customer engagement, usage patterns, inbound and outbound roaming, and voice, data and video experience to deliver better customer experience.

A Year of Spot-on Alerts

Below is a selection of incidents exposed by Anodot, helping its telco clients to save costs and cut losses while maintaining their networks in prime operational mode and increasing customer satisfaction.

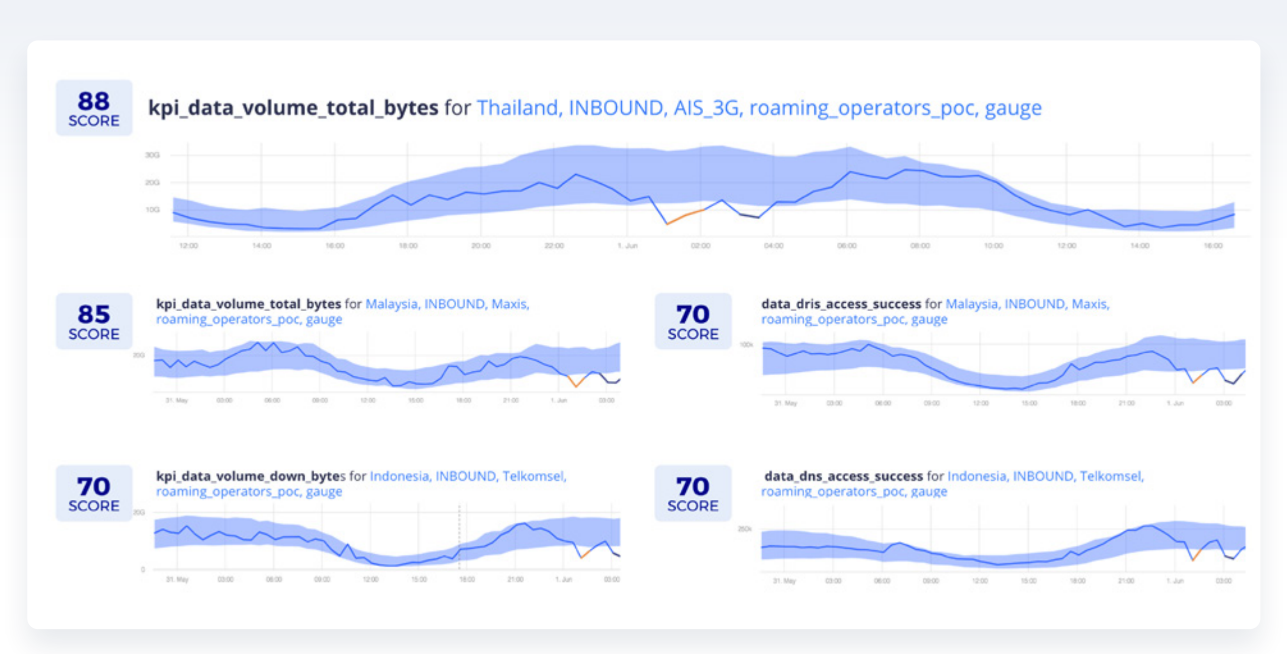
RAN Network Operations

Anodot alerted relevant stakeholders monitoring the company's RAN to a spike in EDROP fail rate across the network. Anodot correlated the spike with a parallel spike in Cell Availability outage and a drop in RRC. By creating the context needed for fast resolution, Anodot enabled the company to resolve the issue with minimal impact to the bottom line.



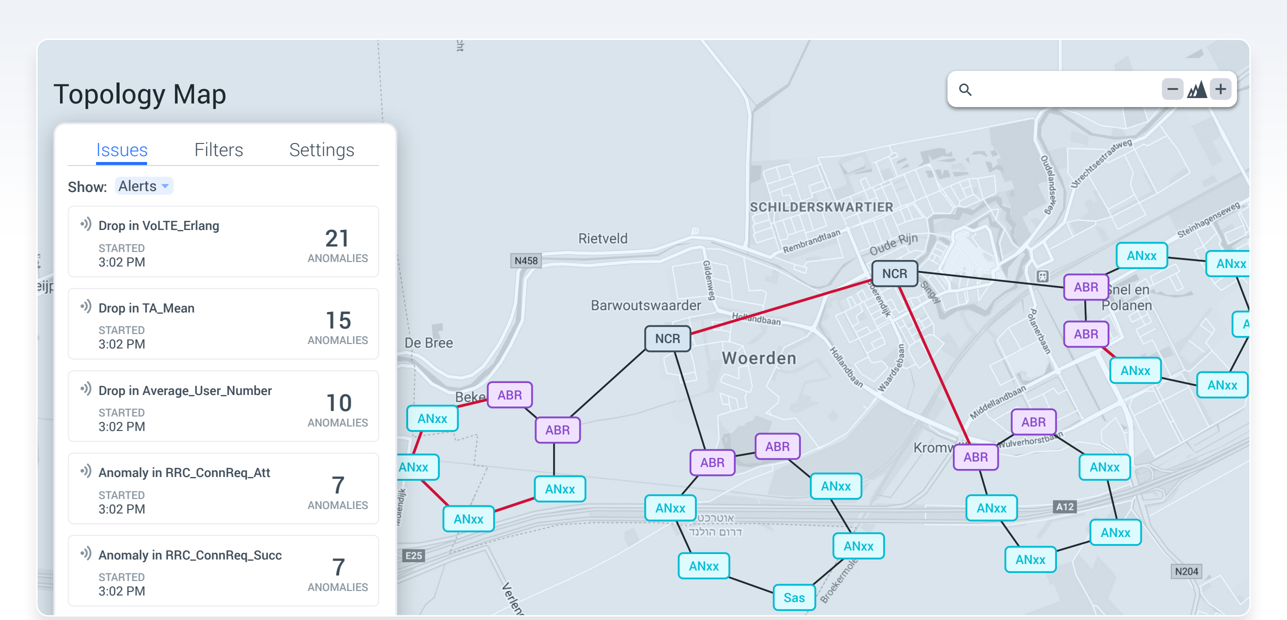
Roaming Analytics

Anodot alerted the teams monitoring the company's RAN to a drop in data volumes for inbound roamers from Thailand, Malaysia, and Indonesia. Anodot correlated the drop with parallel drops in DNS access success rates for the corresponding regions. Anodot identified the incident in less than an hour and enabled the company to resolve the issue quickly.



LTE Traffic Mapping

Anodot alerted relevant stakeholders to multiple drops in VoLTE Erlang across several sectors. Anodot showed the correlated drops using Anomap, an intuitive map-based interface that provides situational and spatial awareness and a quick summary of all the key dimensions related to the affected KPI. Anomap provided the network operations team with the context needed for fast resolution, enabling them to resolve a critical issue that was impacting multiple sites with minimal effect to the bottom line.



Drop in VoLTE_Erlang
STARTED 3:02 PM
21 ANOMALIES

Drop in TA_Mean
STARTED 3:02 PM
15 ANOMALIES

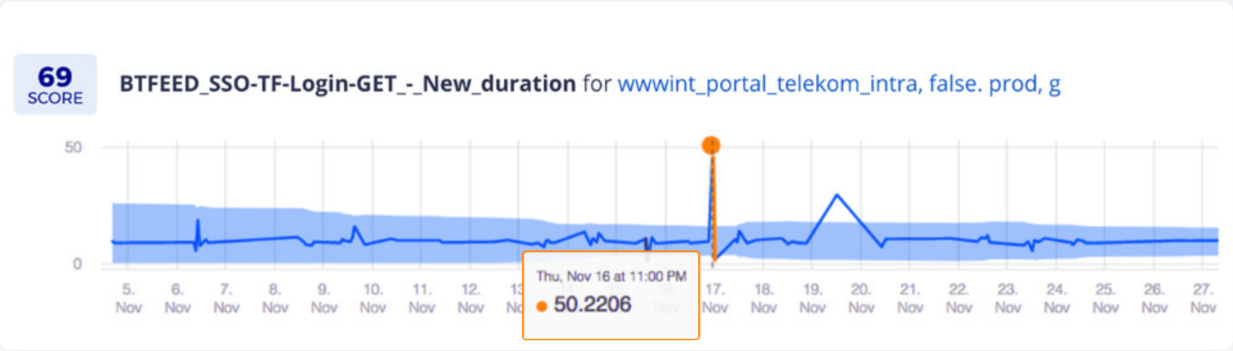
Drop in Average_User_Number
STARTED 3:02 PM
10 ANOMALIES

Anomaly in RRC_ConnReq_Att
STARTED 3:02 PM
7 ANOMALIES

Anomaly in RRC_ConnReq_Succ
STARTED 3:02 PM
7 ANOMALIES

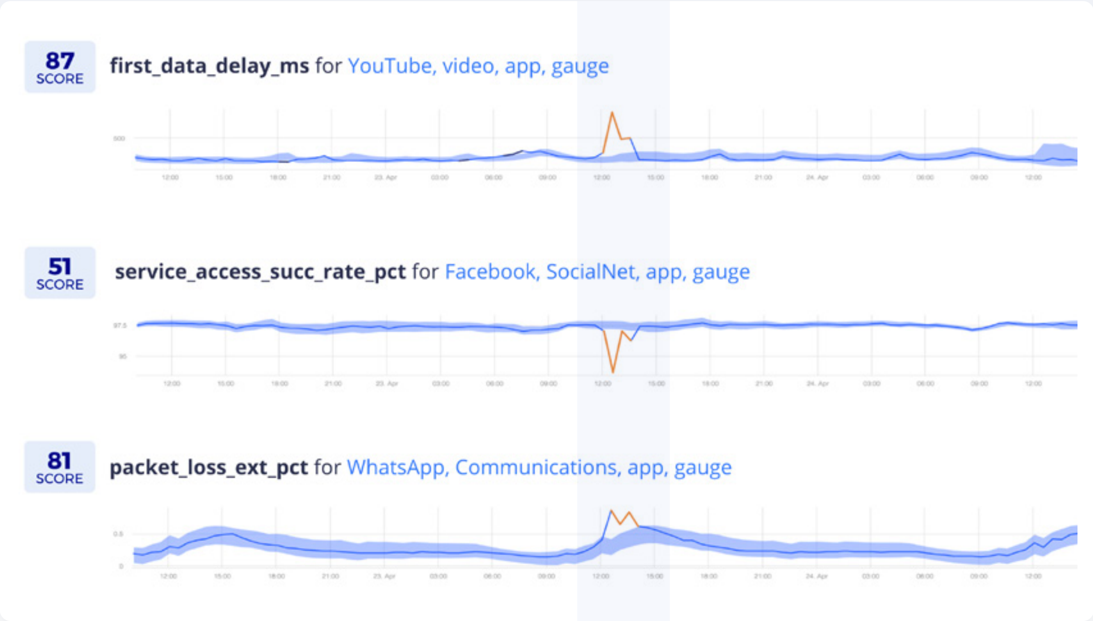
Customer Portal Login

Anodot alerted CEM stakeholders to a spike in login time for their customer portal. Anodot identified the anomaly and alerted the customer within 1 minute. The customer was able to redirect subscribers to another server, avoiding customer complaints, lost revenue, and saving 2 hours of outage for the customer portal.



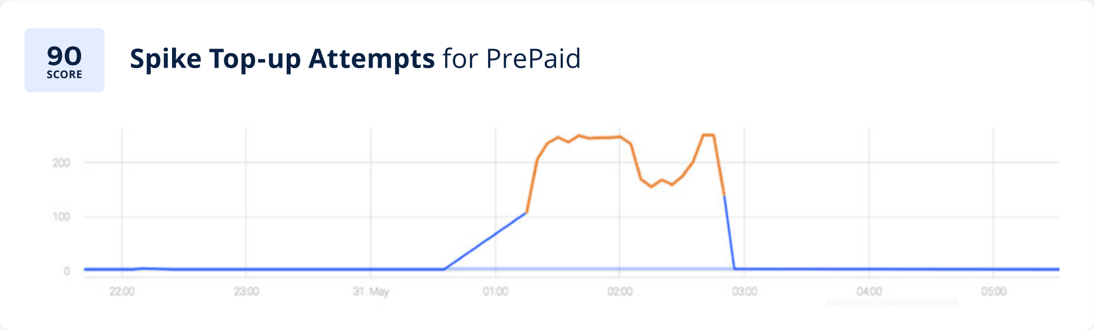
Packet Loss

Anodot alerted relevant stakeholders about a spike in first data delay for subscribers using Youtube, Facebook and Whatsapp. Anodot correlated the spike with a parallel spike in packet loss and a drop in service access success rate. By creating the context needed for fast resolution, Anodot quickly identified the issue and provided the necessary context to resolve the issue before customer complaints could roll in.


87
SCORE
first_data_delay_ms for YouTube, video, app, gauge
500
51
SCORE
service_access_succ_rate_pct for Facebook, SocialNet, app, gauge
97.5
95
81
SCORE
packet_loss_ext_pct for WhatsApp, Communications, app, gauge
0.5
0
12:00
15:00
18:00
21:00
23. Apr
03:00
06:00
09:00
12:00
15:00
18:00
21:00
24. Apr
03:00
06:00
09:00
12:00

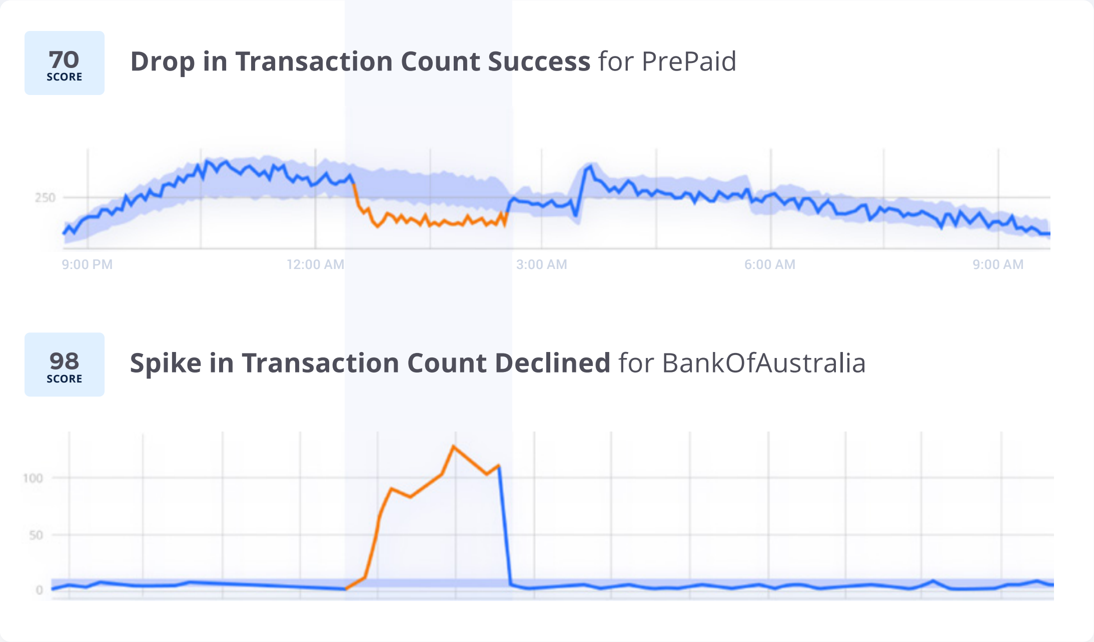
Fraud Prevention

Anodot alerted stakeholders of revenue data to an unusually high volume of top-up attempts. Anodot quickly identified the unexpected anomaly as ghost subscribers attempting to top-up and alerted the customer to the fraud, significantly decreasing time to detection and associated costs.



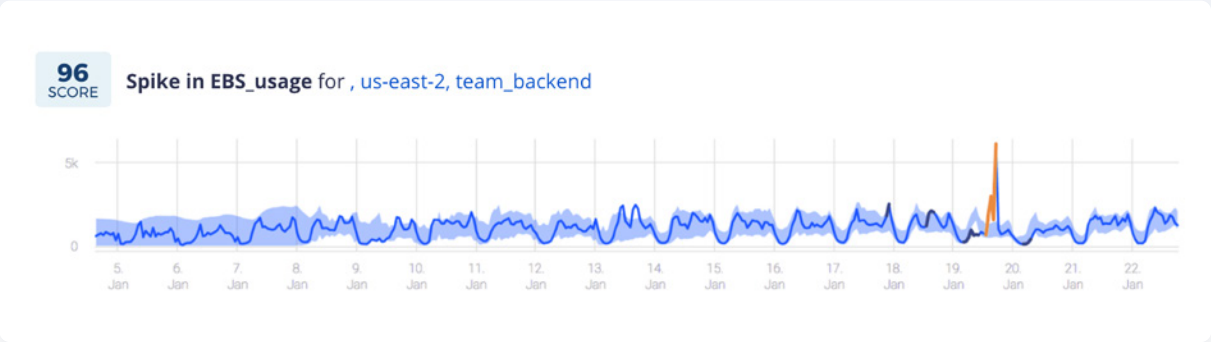
Revenue Protection

Anodot alerted relevant stakeholders to a drop in Prepaid Top-ups. Anodot correlated the drop to a spike in declined credit card transactions due to an external bank outage. Anodot enabled the company to detect the root cause as quickly as possible and resolve the issue with minimal losses.



Cloud Costs

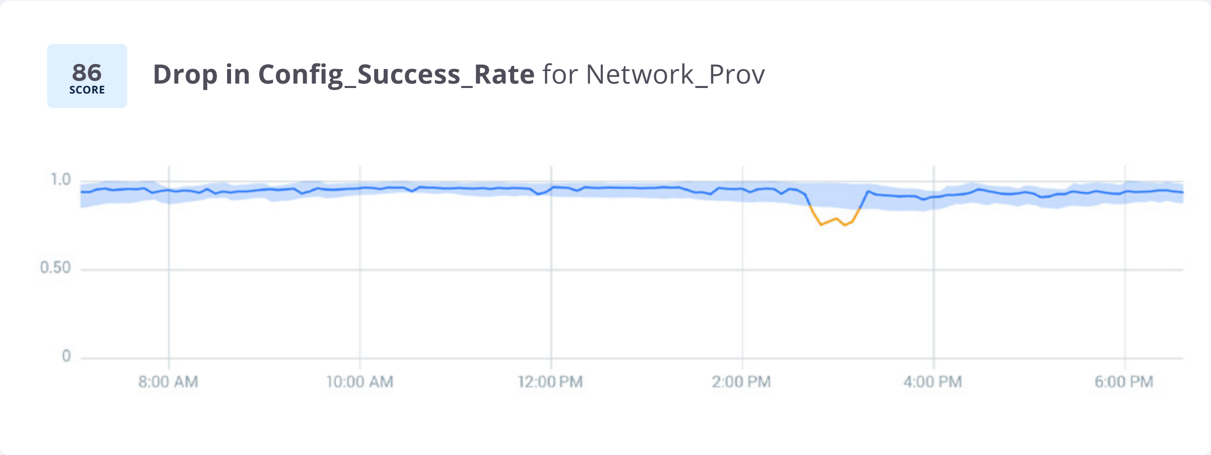
Anodot alerted cloud infrastructure stakeholders to a spike in cloud costs. Anodot identified the spike within 1 hour, serving the alert with a root cause analysis which enabled teams to resolve the incident quickly and with minimal monetary damage.



96 SCORE **Spike in EBS_usage** for , us-east-2, team_backend

Provisioning

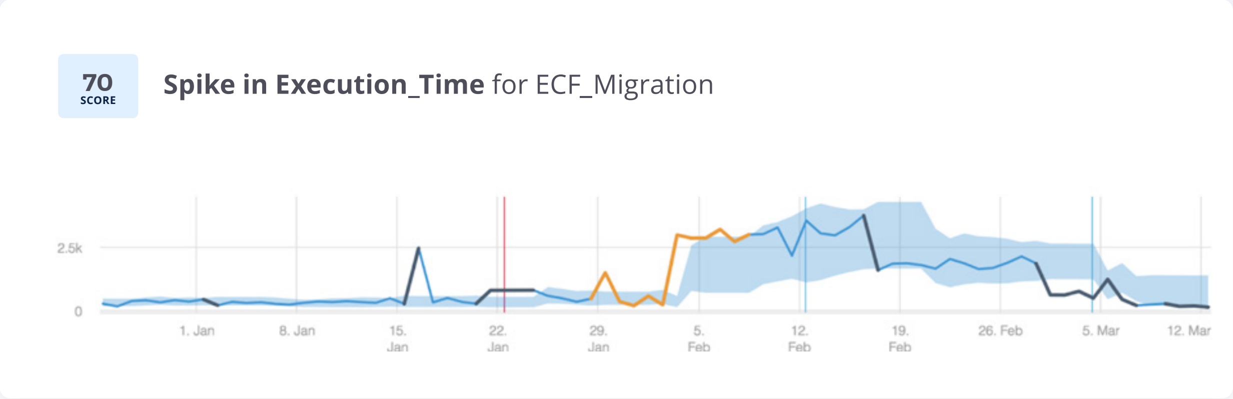
Anodot alerted BSS stakeholders to a drop in network provisioning configuration success rate, that was correlated with a parallel spike in service configuration creation error rate. Anodot identified the drop within minutes. Teams relied on Anodot's root cause analysis to resolve the incident within half an hour of initiation.



86 SCORE **Drop in Config_Success_Rate** for Network_Prov

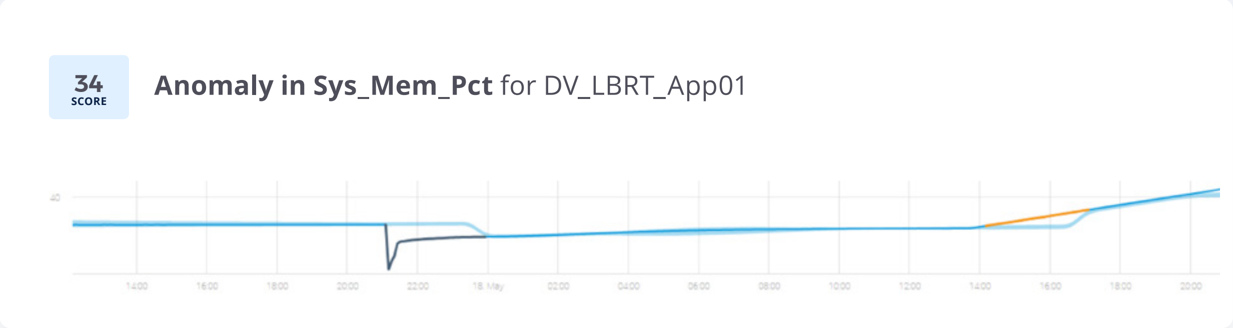
ETL Monitoring

Anodot alerted IT stakeholders to a spike in execution time for a critical ETL process. Anodot identified the spike within hours, serving the alert with a root cause analysis which enabled teams to restore the process quickly.



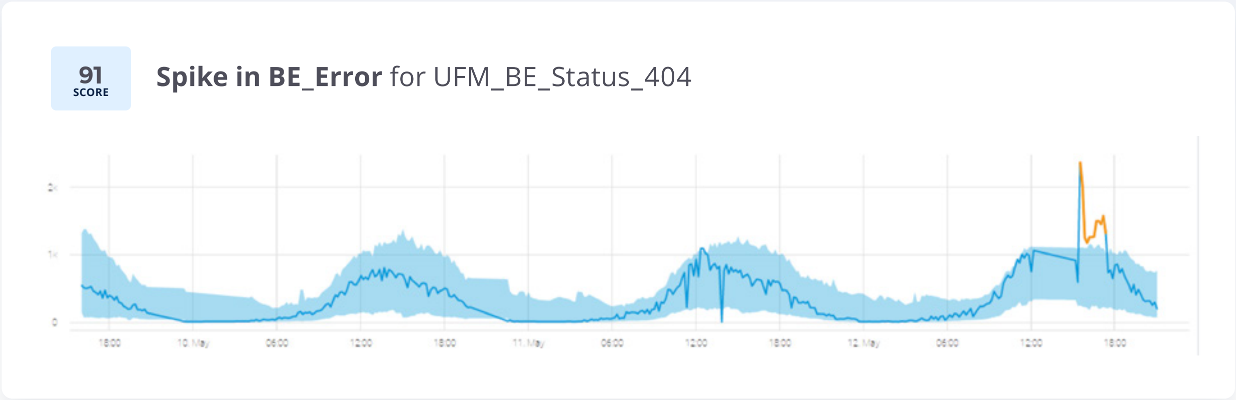
Slow Memory Leaks

Anodot is also able to track sluggish anomalies, such as an increase in RAM consumption on BRT. These kinds of alerts are especially conducive to avoiding memory-related application crashes or an A3 level accident.



Backend Errors

Anodot alerted IT stakeholders that an abnormal number of errors was recorded on UFM Backend. During the analysis it turned out that the errors were caused by an incorrect connection of subscribers from dealers. Anodot provided the necessary context to resolve the incident swiftly.



Optimize Telco operations with lightning-fast incident detection

ML-based anomaly detection is key for ensuring that network and business support systems can keep pace with the high level of service required for mission-critical applications. To deliver on customers' high expectations and maintain and improve quality of service, early detection of service degradation and network failures is critical. Human-centric approaches like dashboards and static thresholds are not scalable, efficient or cost-effective enough to meet this challenge.

AI enables the transformation of traditional network and service operations towards AI-driven automation and intelligent operations. AI effectively augments and automates early detection, predictions and decision-making in operations and in business processes where humans can't deal with the volume or velocity of data.

AI-based use cases address the following business needs:

- **Network optimization** – giving telecom companies the ability to identify the root causes of complications in network operations; identifying potential faults and their root causes in LTE, 3G, and 5G networks before they generate impacts or outages; establishing closed-loop service assurance to continuously improve the service quality and efficiency; accurately monitoring the service levels, optimizing customer interactions, network design, planning, operations and more to allow for optimized CAPEX and OPEX resource allocations.
- **Better customer experience management** – such as predicting churn, increasing engagement, optimizing network for usage patterns, inbound and outbound roaming analytics, and enhancing voice, data and video experience, etc.
- **Order Management & Provisioning** – such as order management and fulfillment, service configuration, multiple channel dependencies, and coordinated and dynamic product provisioning.
- **Billing & Revenue Management** – such as payment gateways, billing workflows, cloud costs, preventing revenue leaks, gaining early visibility into revenue events, and preventing customer refunds.
- **Fraud detection** – including theft or fake profiles, behavioral fraud and other activities. Applying ML algorithms to customer and operator data can help prevent fraud and provide real-time responses to any suspicious activity.

Telco operations are highly dynamic and complex, with every network component, product and service generating millions of time series data, measuring all aspects of the network and business. 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 and business operations. Autonomous anomaly detection minimizes time spent looking for issues, allowing more time to focus on resolution.

Anodot's Deep 360™ monitoring technology makes these use cases a reality and helps telecom operators monitor their existing infrastructure in a more automated fashion. Anodot uses a patented ML approach to monitor 100% of your data, learn every metric's behavior, even tracking cross-platform data throughout the telecom enterprise, and provide spot-on alerts for critical failures.