anodot

Case Study

Leading Telcos Monitor BSS 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

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

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

Growth and profitability require robust monitoring

Telcos are facing a radical challenge of managing and monitoring the growing number of products, campaigns, retail channels, prepaid and roaming services, billing, customer experience and support, and order and fraud management operations. But staying on top of 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 data centers and telecom networks are being built with redundancies, they nonetheless suffer a variety of outages and 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 2016 survey from Ponemon Institute and Emerson Network Power, studying the cost behavior of unplanned data center outages for data centers:

- The average cost of a data center outage rose from $690,204 in 2013 to $740,357 in 2016, a 7% increase. The cost of downtime has increased 38% since measurements began in 2010.

- Downtime costs for the most data-center-dependent businesses are rising faster than average.
- Maximum downtime costs increased 32% since 2013 and 81% since 2010. Maximum downtime costs for 2016 are $2,409,991.

For a telco operator with 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.

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

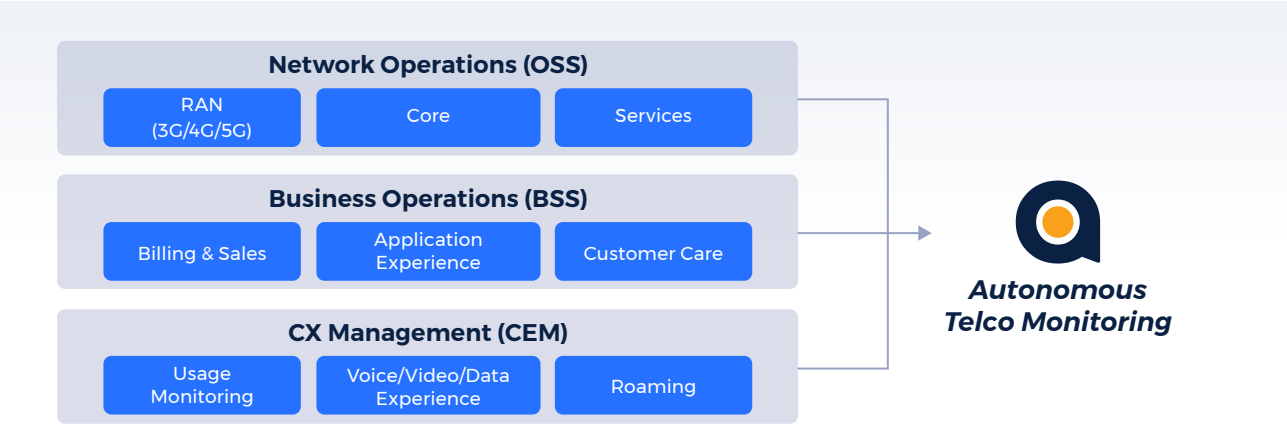
Improving overall time to detect invariably leads to quicker resolution of incidents. This reduces costs associated with outages and helps prevent lost revenue and brand impact. According to a recent Cisco report, the automation of incident management can reduce opex costs by 3-7%. Cisco's figure lines 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.

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**

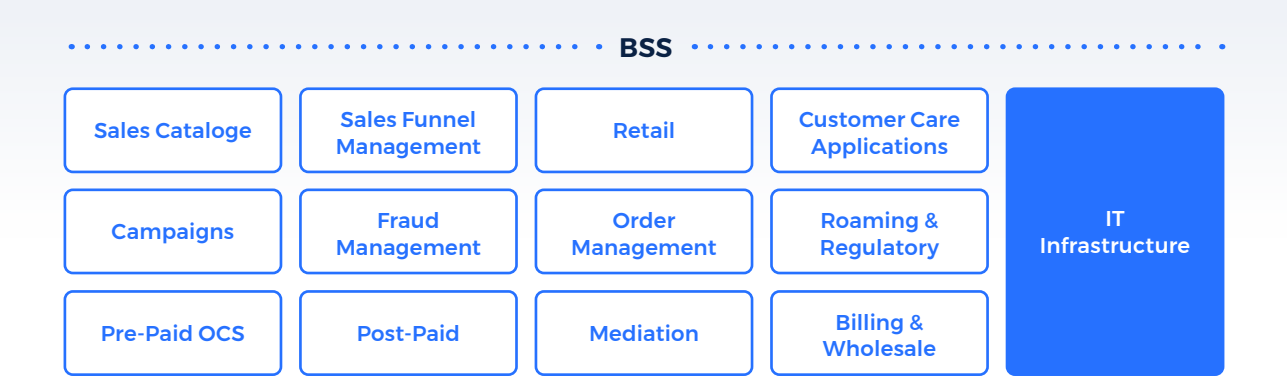
Autonomous Telco Monitoring

Anodot ingests data from siloed business operations systems, and using patented algorithms autonomously analyzes millions of KPIs 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. Large telco operations use Anodot's autonomous monitoring technology for the fastest detection and resolution of incidents across their operations.



BSS Monitoring

Anodot is used by leading telcos 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.



A Year of Spot-on Alerts

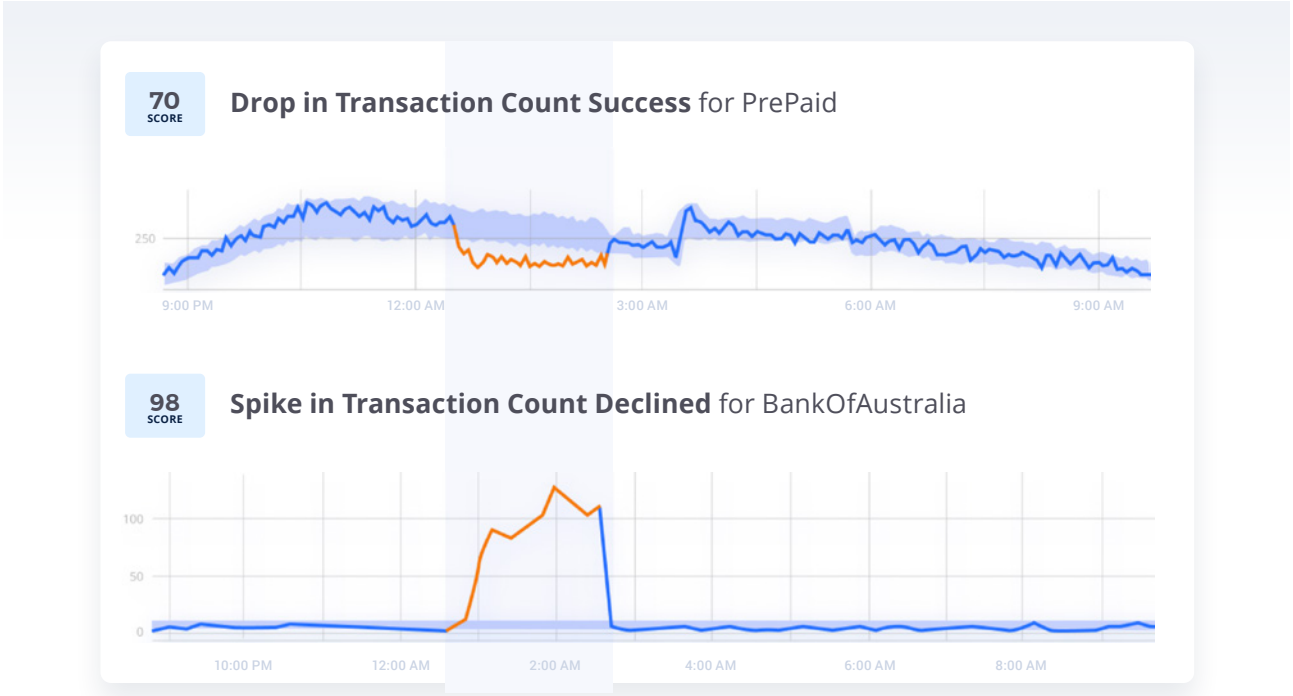
Below is a selection of incidents exposed by Anodot, helping its telco clients to save costs and cut losses while maintaining their business in prime operational mode and increasing customer satisfaction.

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.

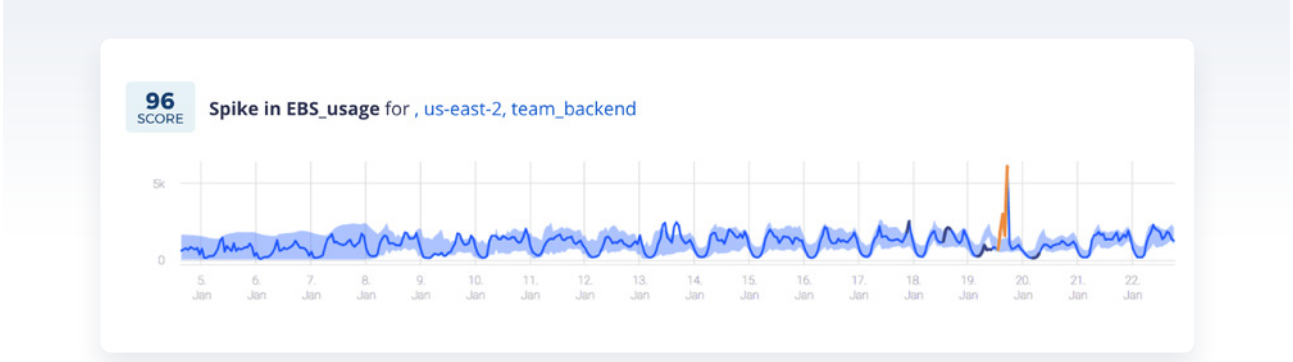
Revenue Protection

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.



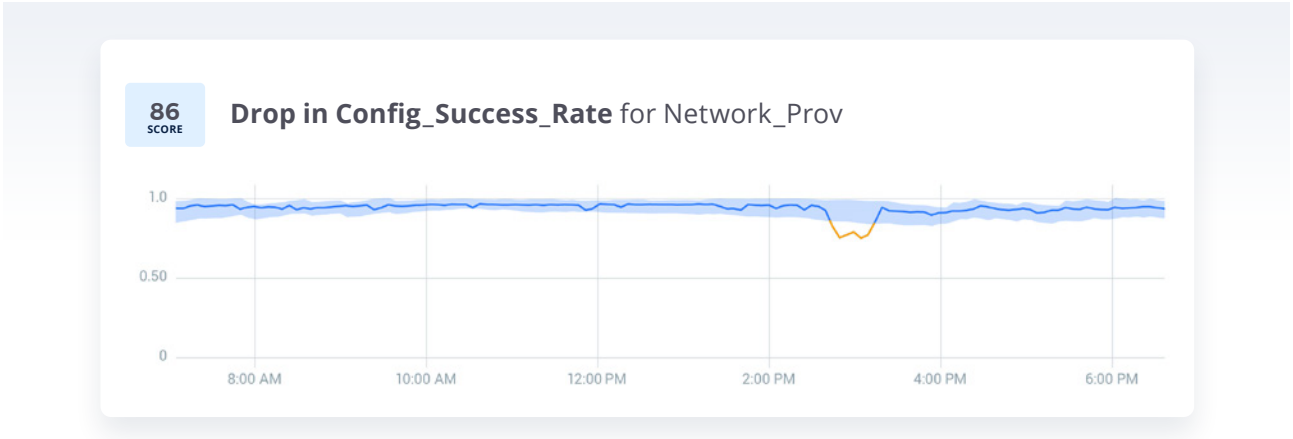
Cloud Costs

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.



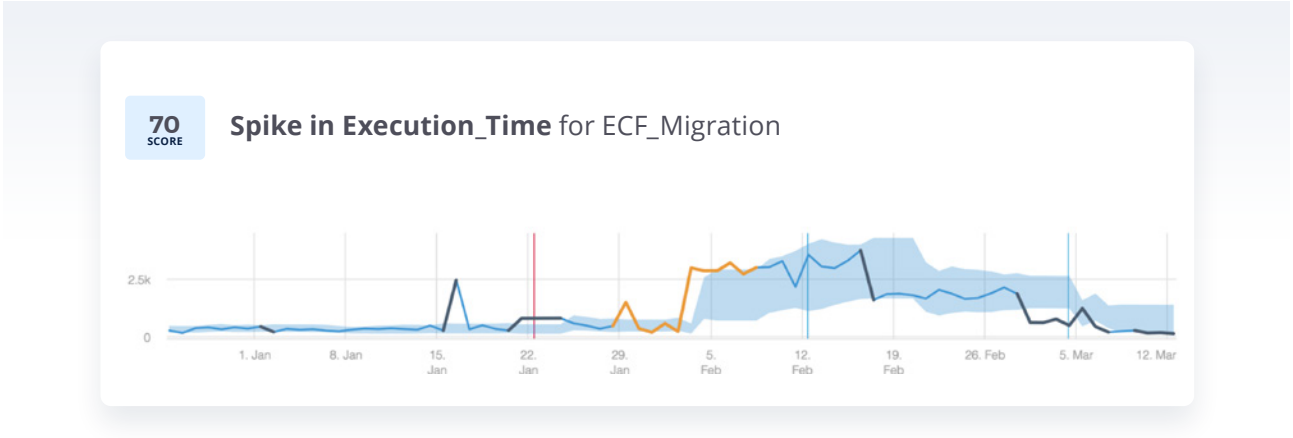
Provisioning

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.



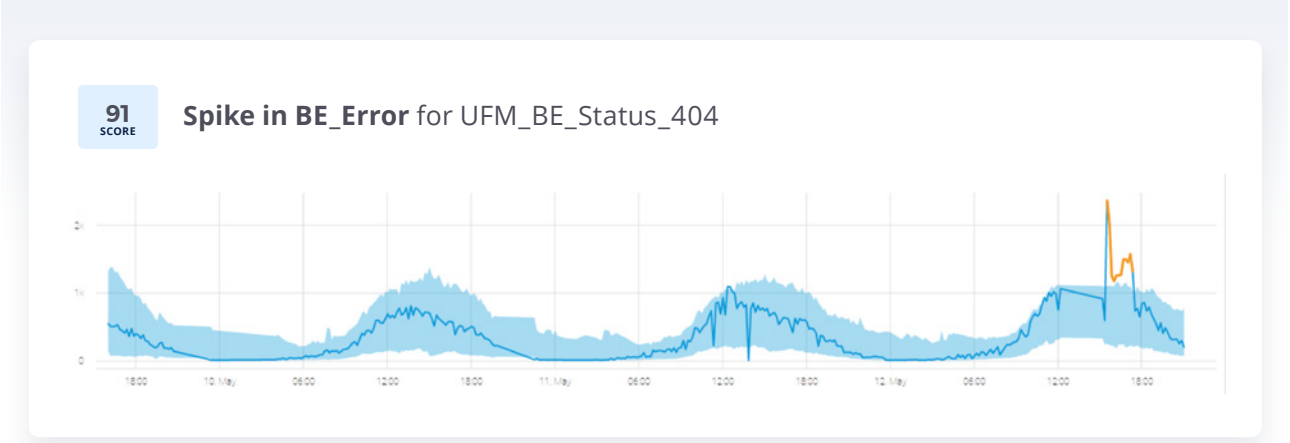
ETL Monitoring

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.



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.



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.

Optimize Telco operations with lightning-fast incident detection

ML-based anomaly detection is key for ensuring that 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 operational excellence, early detection of service degradation and process 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 business and service operations towards AI-driven automation and intelligent operations.

AI-based use cases address the following business needs:

- **Better customer experience management** – such as predicting churn, proactively retaining valuable customers, preventing customer complaints, automating customer service inquiries, routing customers to the right agent, 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.

In the business operations context, every product and service generates millions of time series data, measuring all aspects of the 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 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 that monitors 100% of your data, learns every metric's behavior, tracks data throughout the enterprise and provides spot on alerts to critical failures.

anodot