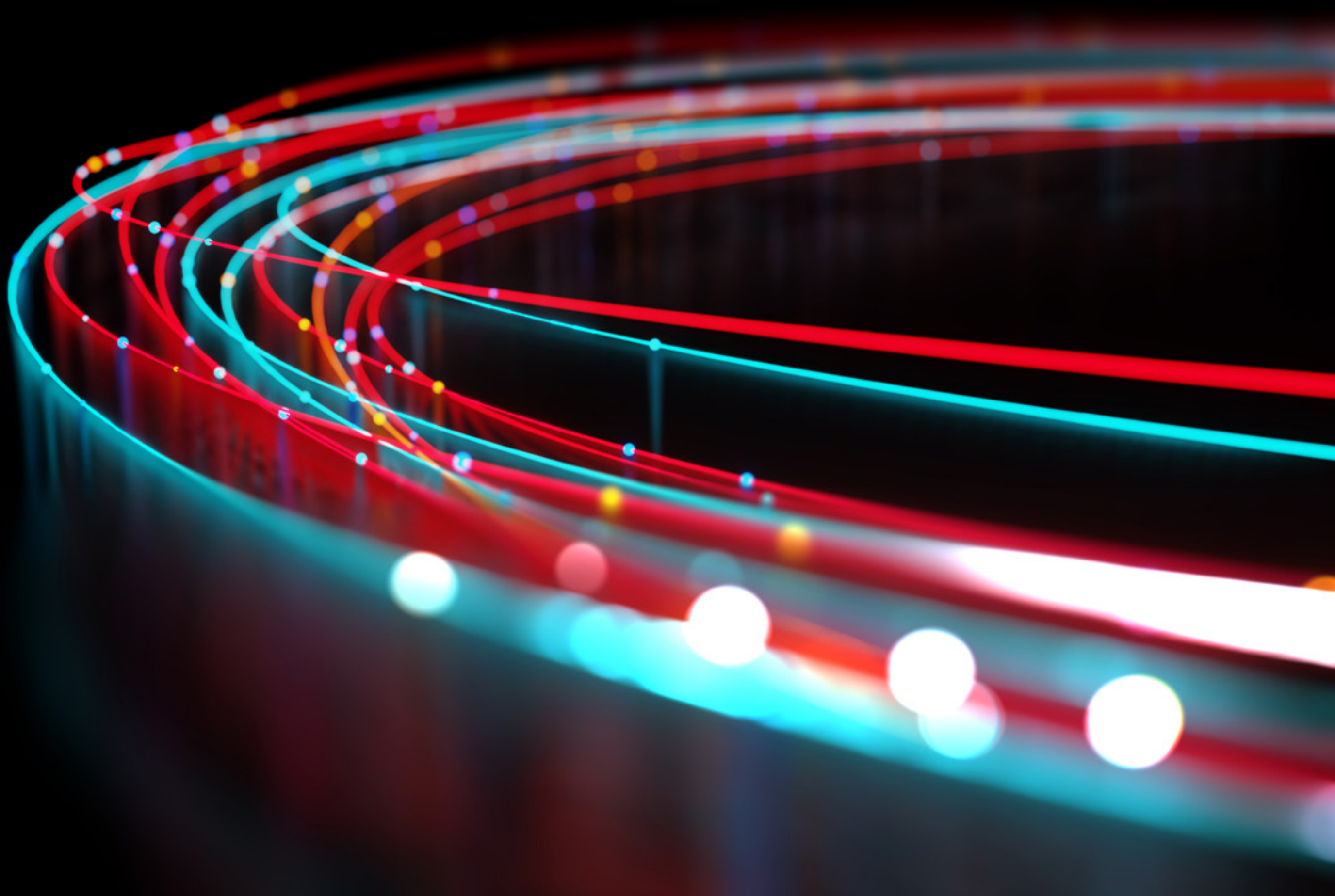
Hybrid Fiber Coaxial (HFC) networks monitoring

The inherent agility of HFC networks makes it a prime candidate for scale, but a lack of proactive monitoring of its complex infrastructure makes it prone to late detection of service degradation. Now, machine learning-based anomaly detection solutions enable CSPs to take their HFC networks to the next level.



The Power & Agility of HFC

Hybrid Fiber Coaxial (HFC) networks serve globally over 200+ million subscribers, delivering high-speed internet, communication, and entertainment services Although the demise of HFC has been predicted a number of times due to the emergence of new access technologies such as FTTx, 4G, community WiFi, and now 5G — HFC continues to rise to the challenge, making rapid strides towards delivering Gigabit internet speeds through the evolution of standards and technology.

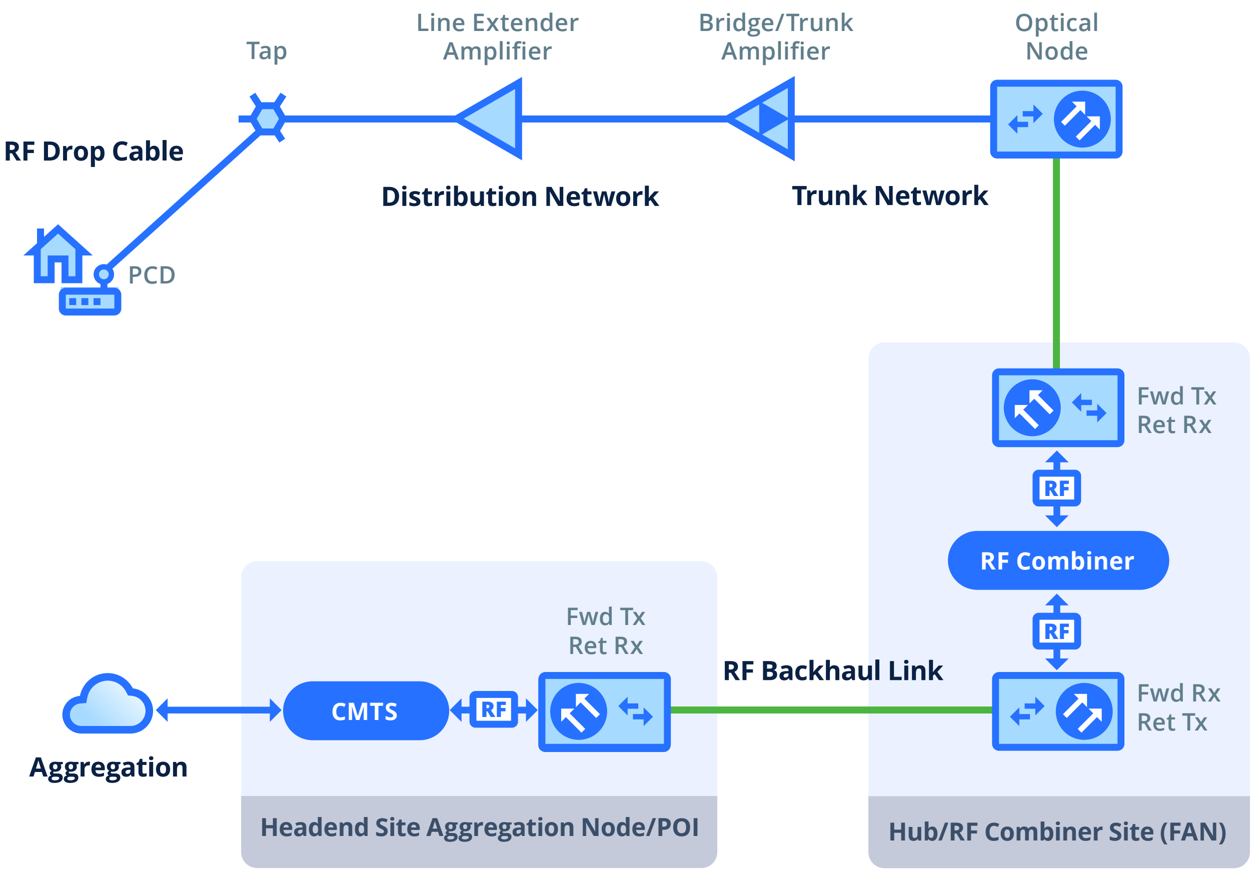
HFC networks are inherently agile and able to adapt to demand spikes. This significant characteristic was most recently demonstrated by their success in handling pandemic-induced traffic surges. However, according to a recent article by Light Reading, changes in end-user behaviour due to the pandemic, including increased uplink usage, are nevertheless imposing additional customer experience and network planning challenges for HFC network operators. Cable operators now prioritize HFC over FTTH projects, adding capacity to their HFC networks, pushing ahead with node splits, and accelerating the use of AI-assisted technologies that enable networks to use the existing spectrum more efficiently.

HFC and FTTH networks differ in that HFC extends fiber to a node within a mile of the home or business, while FTTH extends fiber all the way to the home or business—typically terminating the fiber at a customer premises device, which then provides service to devices in the home over copper lines, coaxial cable, or wireless connections. As a result, FTTH networks have greater capacity and significant functional benefits over HFC networks.

However, HFC can scale in capacity both through expansion of fiber and upgrading of electronics, thereby providing a logical evolution path for the hundreds of millions of homes and businesses connected by the technology to gradually reach gigabit speeds.

HFC Monitoring Challenges

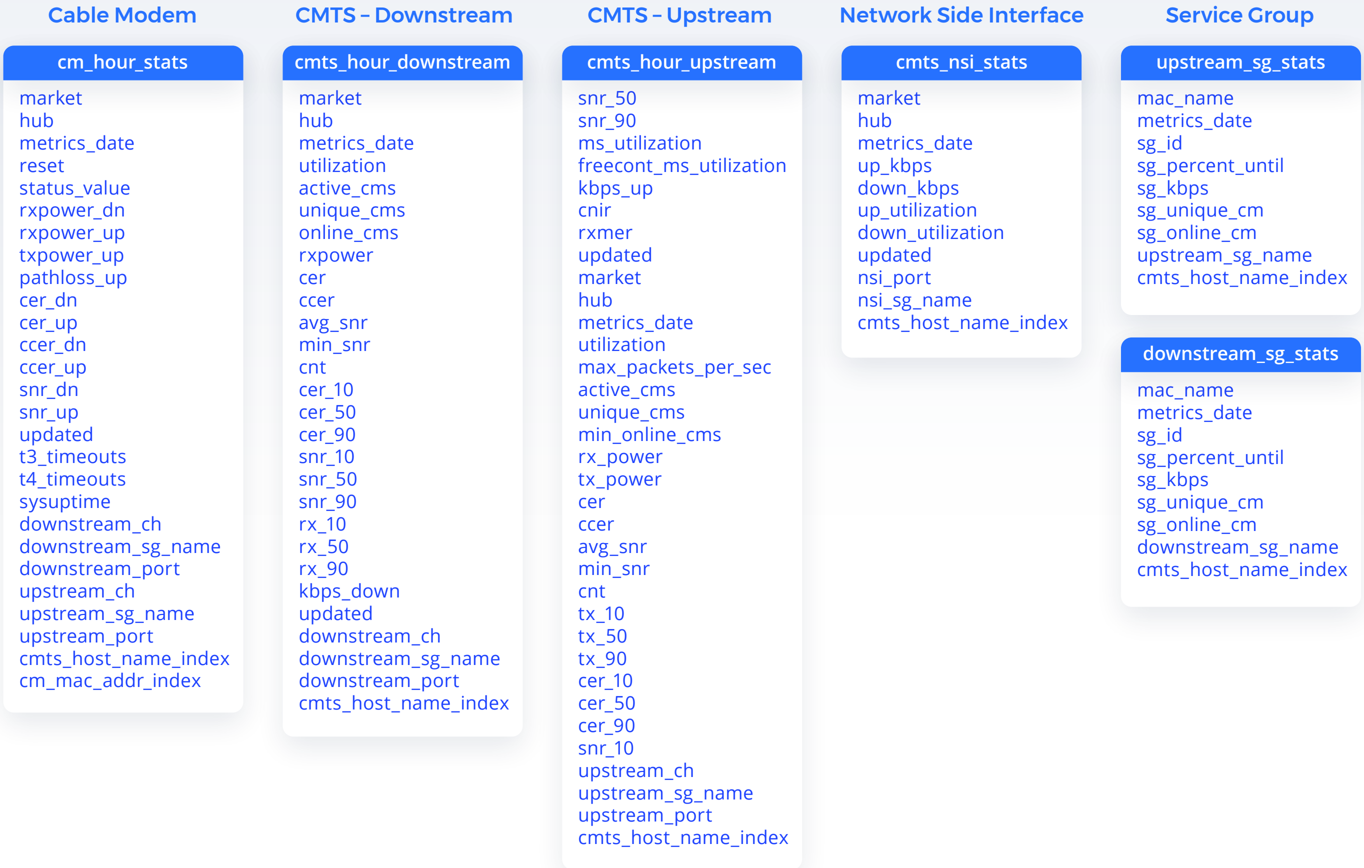
As the name suggests, HFC is by nature a hybrid technology composed of Optical and Radio Frequency (RF) technology delivered through a complex interaction of active and passive network elements. The diagram below provides a high-level overview of a typical HFC network:



The true scale of this network depends on the geography and subscriber density of the network. In general, however, a typical deployment has thousands of street cabinets with the optical nodes, hundreds of hub sites, and hundreds of CMTS nodes. To add further complexity, the end-user Cable Modems, the passive end elements, are typically from multiple vendors, each with their own network management and performance management platforms, each with its own representation of performance.

A typical HFC network generates millions of metrics at various parts of the network. For example, a single cable modem can generate around 300 KPIs (there are millions of cable modems in the network), and thousands of additional metrics generated by the access, edge, core, backbone and interconnected layers.

The typical metrics that can be monitored are summed in the diagram below:



It's easy to see that monitoring such multiple disparate metrics represents significant challenges. The most pressing of these are:

1. Metrics are generated by multi-vendor technologies and infrastructures in silos.
2. Existing tools and techniques such as dashboards, static thresholds, and periodic reporting are often inadequate to detect issues quickly, identify the root cause, or offer any assistance in cutting the mean-time-to-repair (MTTR).
3. For HFC networks, this is especially important in the context of slow leaks. Since very often failure indication takes time due to service or network element degradation, slow declines that don't represent big drops take long to reach the static threshold level.
4. When subscribers experience uplink and downlink incidents such as throughput drops or packet loss there is no way to generate a coherent view of the root cause. This often leads to an increase in customer complaints, loss of brand reputation, and increased Opex costs.

The complexity of the network and infrastructure make it extremely difficult to understand performance degradations proactively. The NOC is often flooded with alarms to the extent of millions per day, and customer complaints trigger truck rolls that are often misdirected due to the lack of visibility and the lack of a common view between the NOC and the customer service teams. These dynamics often cause service disruptions that can take 48-72 hour spans to resolve. As a result, the operational costs of HFC are 10x compared to FTTx technologies.

Monitoring your HFC Network

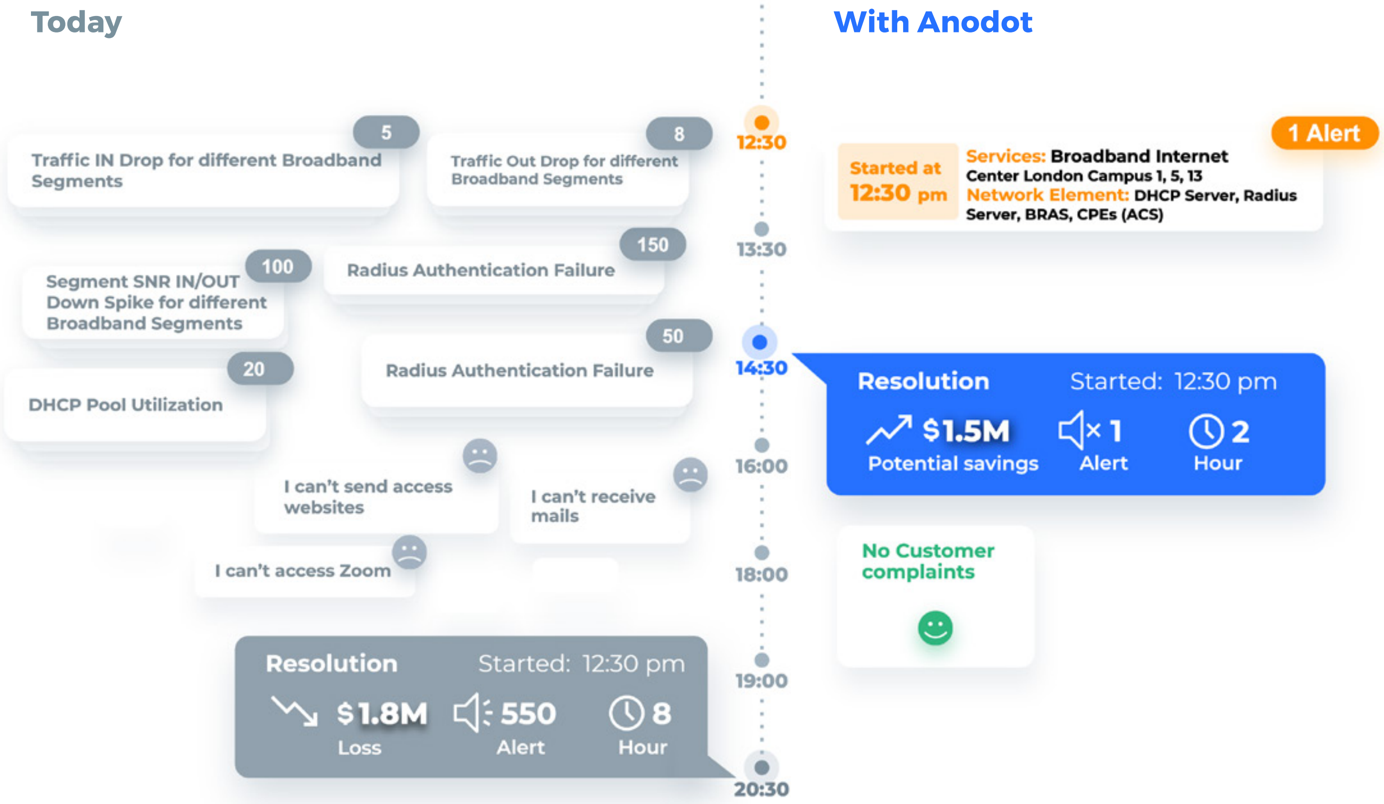
In order to build confidence and scale the upstream/downstream capacity of hybrid fiber/coax (HFC) networks, CSPs need to create the monitoring environment that provides the transparency needed to seamlessly identify and mitigate any issues as quickly as possible.

Monitoring complex multi-vendor environments has never been easy. As broadband usage increases at a rate of 20-25% CAGR, identifying failures is becoming increasingly difficult. It's not surprising that engineers list monitoring as a major obstacle for HFC networks.

Manual alerts and thresholds are a non-starter when it comes to HFC networks. CSPs run multiple hybrid networks, each with a large number of nodes, making static alerts completely impractical. Manual, or even semi-autonomous monitoring platforms, will inevitably produce alert storms (too many false-positives)—or you could miss key events (false negatives). CSPs face daily issues in the HFC segment of their network where late and reactive issue detection creates a negative impact on OPEX efficiency and customer experience, with a potentially adverse effect on revenues and churn.

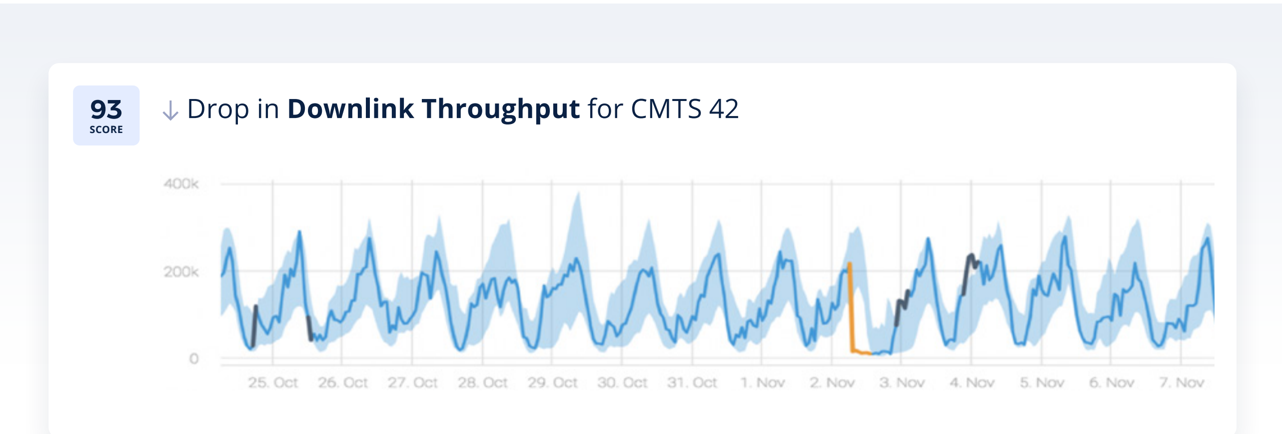
By adopting a zero touch monitoring solution like Anodot, CSPs can use machine learning to constantly track millions of HFC events in real time and be alerted to anomalies and issues when needed. Machine learning based anomaly detection for HFC networks directly improves customer experience and increases OPEX efficiency in HFC.

Broadband Internet – ISP Scenario

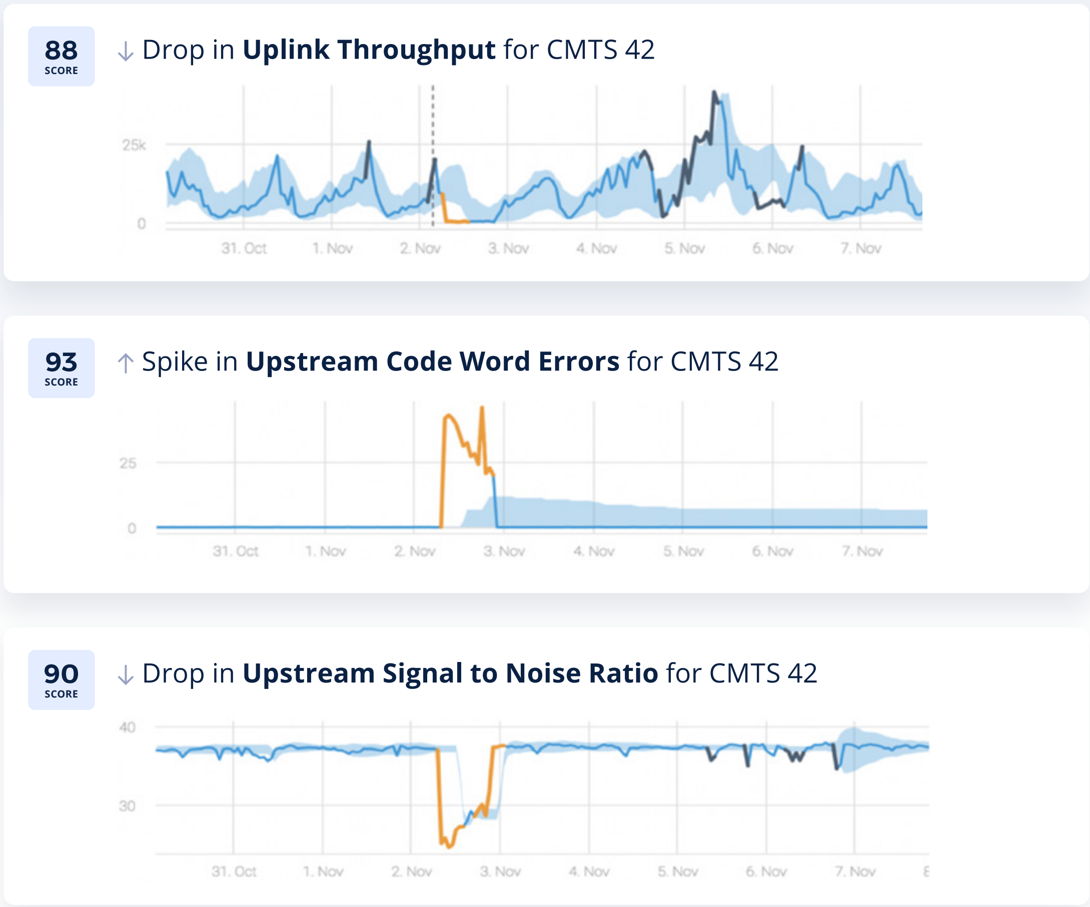


The following use cases demonstrate how tier 1 CSPs use Anodot to proactively monitor and correlate anomalies across the HFC network.

In the example below, an anomaly was detected in downstream throughput drops in a specific CMTS:

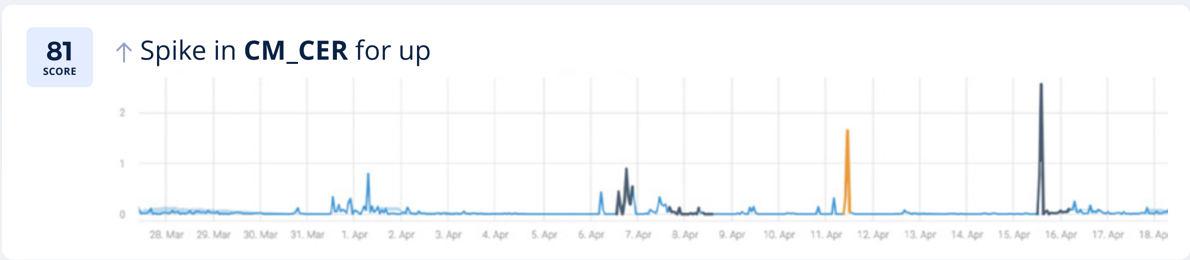


By correlating between anomalies across the network, the AI-based monitoring solution was able to link the incident above to the following incidents:

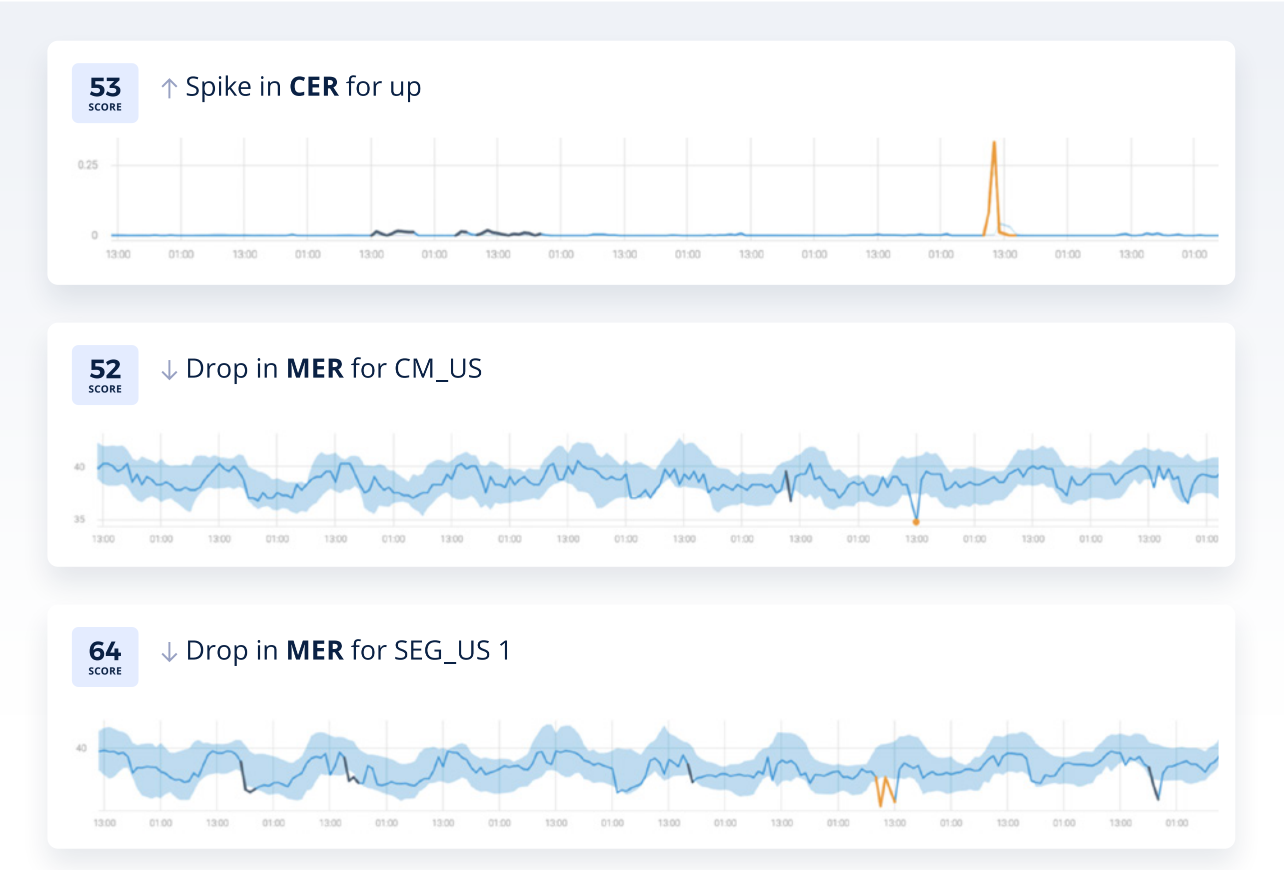


Based on these incidents, the telco was able to proactively notify customers in the region about the service degradation, creating a better customer experience and taking a load off customer service complaints. In addition, by relying on the correlated anomalies that caused the incident the technical team was able to resolve the issue much faster than in previous cases.

Another instance of proactive monitoring is related to the monitoring of the Cable Modem metrics. Below is an example of a spike in Cable Modem Code Word Errors in the upstream.



This anomaly is correlated with other anomalies, including Code Word Errors in the uplink for the segment, Modulation Errors in the Cable modem and the Segment.

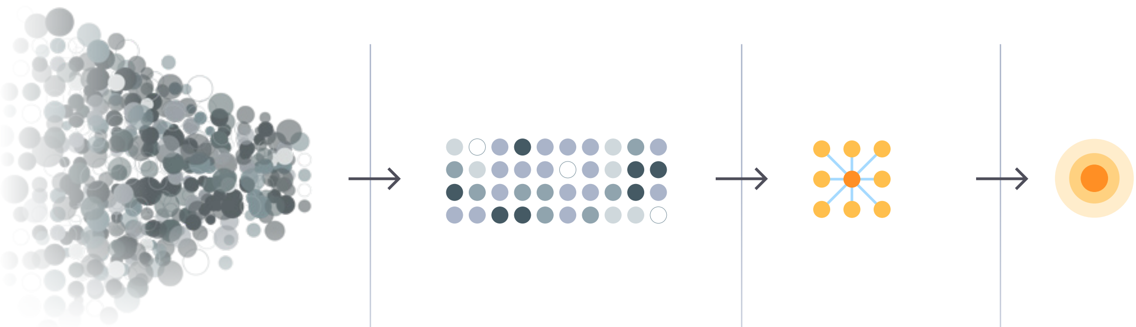


By proactively monitoring the vast number of metrics in a HFC network, CSPs can detect incidents earlier, shorten time to investigate, correlate across domains, find the root cause quickly, thus vastly reducing alert storms, customer complaints and unnecessary truck rolls.

Anodot Zero Touch Network Monitoring

Anodot's zero touch network monitoring platform is the brain on top of the OSS, giving CSPs a holistic view across multi-vendor HFC environments for real time detection of service-impacting incidents. By monitoring network performance and service experience in real-time, Anodot provides lightning-fast detection of the incidents that impact your customers and bottom line so that you can ensure customer satisfaction, minimize revenue loss, automate problem resolution and reduce time to repair.

Proactive monitoring allows for a much greater level of granularity in the network monitoring process. This enables CSPs to identify issues as they happen, and proactively take actions or make changes before they dramatically impact the customer's experience — and the business.



Autonomous learning of data at scale

- Fault Mgmt. KPIs
- xDRs
- OSS/BSS
- Performance Mgmt. KPIs

Reduce False Positive & Alarm Storm

- Accurate Learning Models
- Multi Layers Data Sources

Correlations

- Anomaly Correlation
- Event Correlation

Root Cause Analysis

One Alert – Shortest Time to Detect

Anodot collects and analyzes data across the entire telco stack, including all data types from all network types, layers and domains at scale. All metrics are actively monitored, enabling CSPs to achieve full visibility of service degradation incidents. Anodot's patented correlation engine correlates anomalies across the network for holistic root cause analysis and the fastest time to resolution, leading to improved network availability and customer experience.

Anodot is completely autonomous. There's no need to define what data to look for or when, no manual thresholds to set up or update. New use cases can be added on the fly, and no monitoring maintenance is needed even as the network configuration changes.

Anodot delivers the shortest time to value for AI, and maintains that value over time. A short integration process enables you to seamlessly send your data to Anodot, deriving immediate value and new efficiencies. Anodot is built for business users — the platform is ready to use with no data science required. It is easily integrated with any type of data sources, and just as easily applied to new services.

CSPs use Anodot to build resilience into their HFC networks. Anodot enables CSPs to reduce alert noise by 90% and shorten Time to Resolve by 30%. This helps operations and NOC teams become proactive in their ability to identify service degradations and outages, improving network availability, customer experience and operational efficiencies.