Intellyx White Paper

Real-Time Anomaly Detection and Analytics for Today's Digital Business

Jason Bloomberg

The mad pace of digital innovation today raises the bar for all technologies that underlie customer-facing solutions. Case in point: Eyeview, a video advertising technology company whose platform ingests a wide range of consumer, brand, and retail data into a real-time decisioning engine that delivers personalized video across a wide diversity of touchpoints.

"Eyeview is a very high volume, low latency, high throughput system," explains Gal Barnea, CTO of Eyeview. "Our system evaluates 20 billion requests and drives hundreds of thousands of dollars every day."

The business performance of a company like Eyeview ties directly to the performance of its technology – a fundamental reality in today's digital age. As a result, identifying issues promptly and resolving them immediately present more than a technology challenge – the business itself depends upon success.

"Maintaining the system's stability and preemptively identifying potential issues correlates directly with the company's revenue," Barnea says. "Using Anodot's central monitoring, anomaly detection and alerting system we are able to achieve this."

Founded in 2014, Anodot is among a rarefied category of next-generation real-time anomaly detection and analytics vendors, whose patented technology rises to the exceptional challenges of digitally forward companies like Eyeview.

The 'Next Generation' of Anomaly Detection

Historically, anomaly detection had little to do with the business. Traditional anomaly detection tools monitored infrastructure-centric data sources (log files, CPU and memory metrics, etc.), looking for spikes that might indicate a problem.

When such a spike occurred, the tool would send an alert, typically to a hapless admin who had to decide the appropriate course of action – but the sheer quantity of such alerts made discerning the important information from the noise virtually impossible.

Such 'alert storms' are only one type of problem that Anodot's patented technology is especially well-suited to handle. Anomaly detection is such a difficult challenge because of the presence of noise as well as the large number of anomalies. To address these issues, Anodot analyzes anomalies in the patterns of anomalies themselves.

ANODOT ANALYZES ANOMALIES IN THE PATTERNS OF ANOMALIES THEMSELVES.

These algorithms for second-level learning about anomalies can distinguish among more and less significant anomalies. For example, instead of simply looking at anomalies in patterns of CPU usage, Anodot uncovers anomalies in the average CPU usage across a server cluster.

Another example: detecting anomalies in the number of web site errors, vs. anomalies in number of hits or unique visitors. From this information, users can calculate the ratio of errors to visitors, and then track that metric in real-time.

Anodot doesn't stop at simple calculations like ratios, however. Users can create more complex formulas as well, for example, statistical functions that provide a mathematical measure of data clustering, thus identifying outliers to arbitrarily complex groupings of data.

Some Anodot customers even create sophisticated nested, composite functions. Such composite functions can track advanced business logic that ties directly to business key performance indicators.

The result is *business* intelligence – in real-time, leveraging all available data feeds relevant to business performance.

Anodot's Secret Sauce

Anodot's patented innovation is how it performs *real-time machine learning at scale*. This combination of real-time anomaly detection across large data sets differentiates itself from other similar products on the market.

Anodot has a five-step process for anomaly detection: metrics collection, normal behavior learning, abnormal behavior learning, behavioral topology learning, and real-time insights and dashboards.

Furthermore, Anodot is agnostic with respect to the data themselves. Anodot can ingest any type of time-series data in real-time, and then immediately detect anomalies at the time of ingestion. Anodot then analyzes input time series data to determine its normal range.

Once it understands normal behavior, Anodot flags all anomalies, assigning them a significance score based on how unusual the data are and for how long. Anodot is also able to handle complex patterns such as seasonality, trends, and changing data behaviors.

Next, the platform automatically selects the most appropriate algorithm for describing the exhibited data pattern from several options and adjusts it over time based on real-time data. The platform is also able to recognize several different common anomaly patterns, even when the data are noisy, as shown in the diagram below.
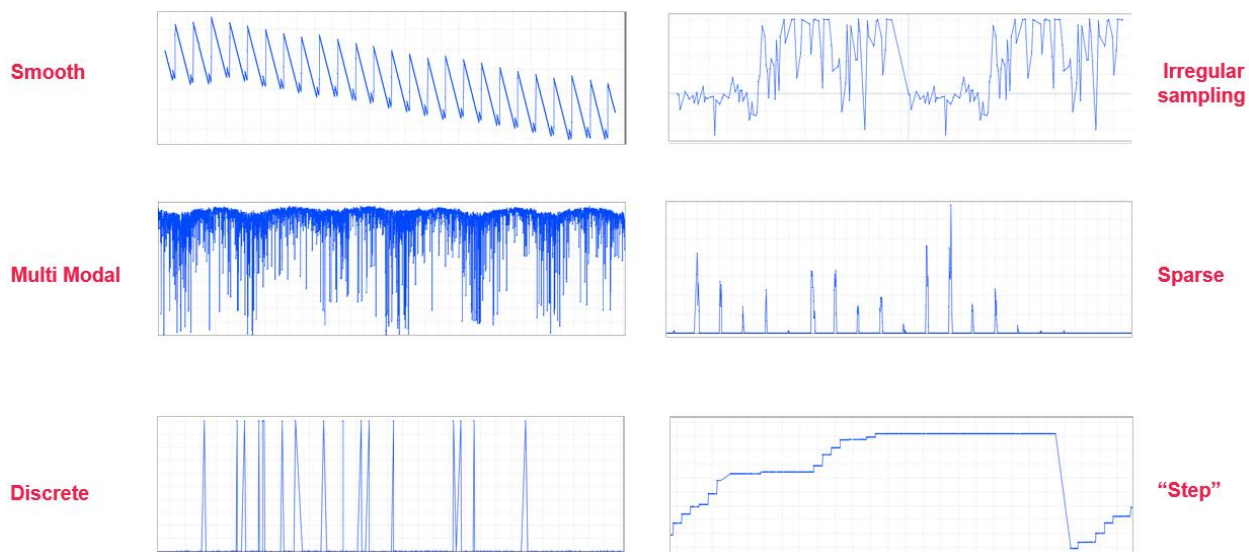
Detectable Anomaly Patterns (Source: Anodot)

Based on the anomaly patterns above, Anodot scores the anomalies it finds, thus differentiating between more and less interesting spikes in noisy data. Furthermore, Anodot's learning behavior is automatic – there are no preset thresholds or other human input that can lead to biased results.

The Intellyx Take: Anomaly Detection for the Digital Age

It's easy to get lost in the technical minutiae of Anodot's patented machine learning algorithms for anomaly detection, but don't let the company's technical accomplishments interfere with its business value proposition to its customers.

The real win for Anodot's approach isn't simply to eliminate the alert storm problem. Instead, its real value is providing valuable insights to today's digital business – in real-time, at scale.

Modern digital businesses are both software-driven and customer-focused – and thus any such organization must connect the dots between the customer experience and the performance of the underlying technology. Efficient, real-time anomaly detection is an important enabler of this connection.

As the Internet of Things (IoT) grows, furthermore, real-time anomaly detection at scale will become increasingly important. IoT data feeds originate at vast numbers of sensors and controls – increasing the noise even more so than the data themselves do.

Anodot's next-generation technology is particularly well-suited for such challenges. In fact, all of today's digital businesses deal with increasingly massive, diverse data streams. Anodot is able to correlate anomalies from disparate data sources in order to uncover unexpected patterns in the data – patterns that can be critical for business decision making.

ANODOT OPERATES IN REAL-TIME – AN INCREASINGLY IMPORTANT REQUIREMENT FOR ANY DIGITAL BUSINESS, AS CUSTOMERS DEMAND REAL-TIME BEHAVIOR FROM THE COMPANIES THEY WORK WITH.

Furthermore, Anodot operates in real-time – an increasingly important requirement for any digital business, as customers demand real-time behavior from the companies they work with.

This capability helps to differentiate Anodot, as other anomaly detection tools either leverage machine learning or provide real-time analytics. Anodot, in contrast, is able to combine the two into a digital-ready offering that stands out among its competition.

Anodot is an Intellyx client. At the time of writing, No other organizations mentioned in this article are Intellyx clients. Intellyx retains full editorial control over the content of this article.