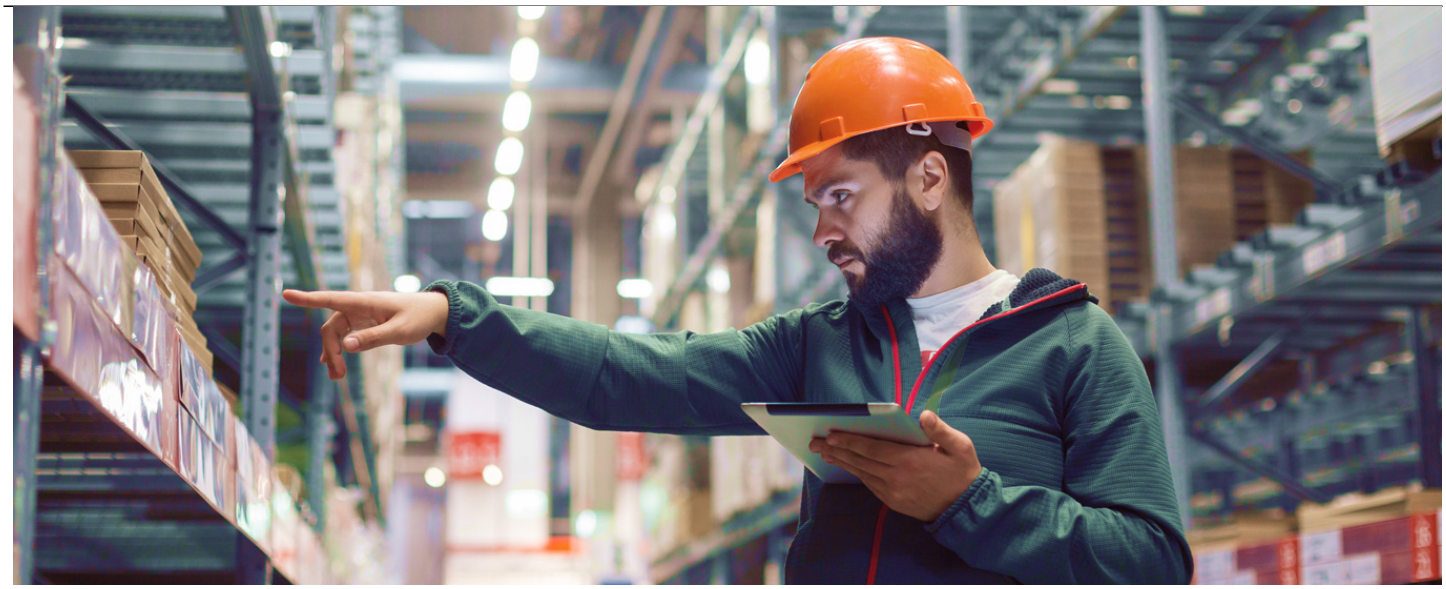
The Business Value of Data Anomaly Detection

The Business Value of Data Anomaly Detection

By Sandhya Prusty Data Center of Excellence Practice Lead | Digital Engineering Services



Data anomaly detection has quickly become a trending topic in the business world as companies look for better ways to predict performance outcomes based on raw data.

The global market for data anomaly detection services is expected to reach $8.6 billion by 2026, achieving a compound annual growth rate of 15.8 percent. But data anomaly detection is easily misunderstood. Let's look more closely at this topic, including how to achieve real value from data anomaly detection.

What Is Data Anomaly Detection?

Data anomaly detection means finding unusual patterns, deviations, and exceptions from the norm in any data set at scale with the help of artificial intelligence (AI). For instance:

Unusual sales spikes: sales of a product in a week for a single store or a website spiking 90 percent versus the week before.

- Unusual website activity: a surge in traffic to a website or a web page, which may suggest either something good (a company has published a massively popular blog post) or bad (a business is being threatened by a cyberattack).
- Yield issues: inconsistent product manufacturing yields, suggesting that upcoming maintenance might be required.

Data anomaly detection is commonly misunderstood, with many believing that its sole purpose is to

flag errors and problems. However, as the examples above show, brands can and should also leverage the technology to identify positive variances such as a surge in sales or an improvement in manufacturing output. When companies use data anomaly detection to spot positive variances (e.g., “Why are sales spiking on our website in October?” Or “Why did we get a surge in store visits in August at our Milwaukee location”) they uncover nuggets of gold that they might have otherwise missed: valuable data that they can capitalize on to improve performance by analyzing causes of positive variances.

That said, data anomaly detection has gained renown lately as businesses become more vigilant about fighting cybercrimes and fraud. The rise of cybercrimes such as ransomware attacks alone has made it more essential for businesses to protect themselves online. The ability to spot unusual patterns in network data traffic indicating a hacking attempt and fraudulent activities is crucial, which is where data anomaly detection plays a role.

How Data Anomaly Detection Makes a Business More Agile

Another misconception about data anomaly detection is that it’s used solely to report historical events. In fact, thanks to machine learning, data anomaly detection models can predict something that *will* happen – which is where data anomaly detection really proves its value. A data anomaly detection model helps a business:

- Spot unusual patterns, deviations, exceptions from norm in any dataset at scale with AI.
- Notify downstream consumers of the data (people, apps, process).
- Take appropriate action.

For instance, a data anomaly detection model could tell a manager of a retail store that sales of a particular product are beginning to spike, giving the manager enough time to restock. Or the manager might notice that the entire store is beginning to see a spike in customer traffic. Perhaps a promotion is going better than planned or an unexpected weather event is triggering a surge in store visits for weather gear. Armed with this data, a store manager might re-assign store associates in the area before sales spike to the point where the store cannot service customers.

In short, data anomaly detection makes it possible for a business to be more agile – sensing and responding to events (both negative and positive) before they happen, and making mid-course corrections.

The ability to predict anomalies as they develop also helps a business think more strategically. For instance, a consumer packaged goods company applying data anomaly detection at scale can more effectively tackle a number of business challenges such as:

Category	Business Challenges	Purpose
Sales/Insights	• How can I monitor pricing, volume, distribution, DOS, at scale for all customers, all SKUs? • Is the retailer respecting his engagement?	• Consumption impacts
Finance	• How can I validate charges on my cost centers? • How can I know when and where my COGs are getting impacted? • How could I validate my P&L at scale and at granular level of detail?	• P&L optimization
Revenue Management	• I want to understand which events are ROI negative? • How can I decrease my Post Audit and Write Offs?	• Trade optimization
Brand	• More and more negative reviews on product x and retailer y?	• Product Quality Issue
Demand	• Has the regional SKU allocation shifted? • Is my demand call matching consumption trends?	• Sustainability/Waste
Procurement	• Is my supplier's pricing increase in tune with the market variations? • Are there opportunity buys out there?	• P&L optimization
Manufacturing	• How can I anticipate unwarranted maintenance activities ? • I have a yield issue; How could I have predicted it?	• Production optimization
Logistics	• How can I make sure that my loads are consistently In Full and On Time?	• Decrease Fines, Increase ROI

In the above example, data anomaly detection happens along three dimensions:

- Business: consumption anomalies.
- Supply: procurement, logistics, allocations to SKU level etc.
- Finance (internal processes): alerts on where the problem could be specifically. validate financials faster.

The business can gain a competitive advantage by compressing time to market with products and shortening the development cycle.

How to Do It Right

Data anomaly detection AI models are only as effective as the data they rely on. And this is a huge challenge for most businesses. In fact, few organizations have the people and technology needed to prepare accurate data for an AI model to use in order to spot exceptions at scale – especially with large businesses that operate multiple locations and facilities. This is why Centific has launched Sherlock.

Sherlock leverages pattern recognition technology to detect unusual patterns, deviations, or omissions across your entire data ecosystem. Once detected, relevant stakeholders across your organization are alerted in real-time with an accompanying report that equips them with the visibility and context needed to resolve quickly – and before your stakeholders are affected.

Behind the scenes, Sherlock combines a process, platform, and people to train AI models with accurate and timely data required to provide agile reporting. Its components include:

- **Process**: Sherlock versatile configurable data onboarding
- **Platform**: Sherlock Ensemble Models
- **People**: Human in the loop collaborating with a client's own subject matter experts.

Examples of Data Anomaly Detection in Action

- Centific has been supporting a multinational technology corporation with data anomaly detection for digital fraud prevention on online payment
- A Centific client in the travel industry uses anomaly detection in search engine optimization for backlinks and keywords to increase leads by 75 percent with a 45 percent reduction in

lead costs.
- A global telephony company works with Centific to identify maintenance issues via the detection of anomalies in data streams. The business can address performance issues in real-time and reduce service disruptions.

Contact Centific

To become a more agile business with data anomaly detection, contact us.