THIS IS NOT SCIENCE FICTION: ANOMALY DETECTION SYSTEMS MANAGE MASSES OF DATA TO BOOST PROFITS, CUT FRAUD AND WIPE OUT WASTE

Interview with David Wright
Executive Chairman by
David Myton

When endeavouring to explain the function and value of an anomaly detection system, David Wright turns to science fiction, specifically Star Trek's Tricorder – a (fictional) multifunction device aboard the USS Enterprise that performs sensor environment scans, data recording, and analysis.

"Almost every company receives inputs of masses of data, but much of that data does not get tracked and analysed because they do not have the capability," says Wright, Executive Director and Chairman of Sydney-based RoZetta Technology.

"They are losing or overlooking huge amounts of data that they have access to today that, if properly used, could be vital to the increased profitability and efficiency of their organisation," he says.

"If you can't harness and analyse that data, you're not even close to tapping into those opportunities."

Well, the Tricorder is fictional; the RoZetta's Anomaly Detection application, supported by its DataHex Data Management platform, is very real with a proven capacity to analyse and derive insights from huge amounts of time series data – which, for all its intrinsic value, cannot analyse and interpret itself or make its own decisions.

Like Star Trek's Tricorder, RoZetta's solutions can detect unusual and unexpected patterns in large amounts of data.

Put simply, it takes multiple streams of data over the same time period, combines them, and compares the actual data to the expected data. This turns the data into more useful information than any person could ever see. Microscopic variations in trends can matter.

Similar systems operate today in health and business. For example, in health, they are used to detect disorders such as Atrial Fibrillation – a heart condition in which a small number of data sets are streamed with thousands of samples taken each second, are compared against a health state and then combined with other streams to predict health outcomes in a manner impossible for humans alone.

Anomaly detection is crucial in business and industry. Anomalies may include patterns leading to an event such as product loss in logistic transfers, customer churn, equipment breakdown, and suspicious or non-compliant activity detection. Variations from efficient states indicate wastage or errors. Anomaly detection enables dynamic risk mitigation. Parties utilise data-based information to identify events causing loss of assets, machine or infrastructure damage and reduce the likelihood of future non-compliant behaviour.

“Anomaly detection exposes trends and patterns in large amounts of data that otherwise would have gone undetected,” Wright explains.

“You can have all these pieces of randomised information floating around inside your system, and on their own, they may appear to be of little value. But developing an anomaly detection system with RoZetta establishes the ability to reveal previously undetected patterns that may be symptomatic of anything from poor maintenance to behaviours indicative of error or waste to outright fraud."

“Like the Tricoder, when relatively simple and seemingly unrelated data is combined, new information is created that can have tremendous value both in detecting issues and events and predicting problems."

“And, of course, these can be investigated and remedial action taken with results that may eventually save large amounts of revenue and optimise operational costs.”

In healthcare, says Wright, estimates of fraud alone are generally accepted to rest between 3-10% of the total cost.

“For a relatively small population country like Australia, spending around $98 billion a year on health, that means a significant problem - even in a field where much is known already about how and when fraud is committed and in which data systems have grown in maturity.”

Wright cites an example of a supplier of prostheses who, over time, charged a health care provider between $800 and $18,000 for purchases of the identical prosthetic limb.

“A more common example is an insurer being charged for a consultation where the same provider is also charging them for another consultation at the same time. Such anomalies can get overlooked in a system with huge amounts of data inputs.

But when an anomaly detection system is utilised, it can detect the anomaly, scan for other instances of similar occurrences, and alert managers who can decide what action to take,” he says.

"Often anomaly detection is like trying to find large piles of needles in multiple haystacks that you know are there but are struggling to find one efficiently. Each individual needle is painful but may not warrant an action other than ‘beware’ - but piles of them can cause serious problems.”

Detecting and investigating major issues following a complaint or concern is the traditional purview of analytics teams, he says, but this is impractical for looking across most transactions in large-scale systems.

“A good anomaly detection system flips the process from seeing a problem externally and then going into a system and finding and diagnosing it, to finding problems - initially anomalies - and then diagnosing whether they are truly worth examining. If they are, analytic teams and response systems can take action, often having been provided with the recommended response.”

Wright says an anomaly detection system such as the solutions RoZetta builds within the DataHex platform serves to bolster the integrity and reputation of the user.

“You can’t guess that someone’s being fraudulent,” he says. “You need evidence – and the system supplies that evidence and so reduces the risk of brand damage for the provider by preventing unfounded allegations.”

“It makes sure the business or enterprise runs efficiently, ethically and with the highest integrity.”

Wright stresses that an anomaly detection system can be used to manage the risk of losses incurred in the transfer of products between parties in complex logistic chains while also enabling rapid response to business infrastructure failures, their location and type of fault.

Among other capabilities, it can also:

- Identify and prevent malicious activity in a computer network, e.g. malware detection
- Prevent the loss of sensitive data
- Detect anomalies in social networks, including fake accounts, spammers, and predators
- Determine why systems fail by reconstructing faults from patterns and past experience

However, the types of anomalies are seemingly endless and can be extremely complex. The best anomaly detection systems will not find all issues, he says, but they should do at least three things:

1. Create a history of common data types and enhance that with trends and combinations (rules or algorithms) so the owner of the data can learn, create information, and build reliable systems – this is a fundamental aspect from which all others derive their value but is the most commonly underdeveloped (the Data or Data Asset stage).

2. Should address crucial weaknesses in the current system that enable fraud, waste and errors to occur by identifying and detecting them in the system, making them transparent (internally and increasingly externally) and constantly measuring them (such as volume and trends – i.e., this issue occurs X times, causing Y impact, and is growing by Z (the 'Business Information or Intelligence' stage). This stage needs collaboration from experts inside the target sector but from outside the data field – doctors, practitioners, engineers etc. – to determine what matters and diagnose why and how to prevent it.

3. Use the information to perform immediate short term activities, increase the efficiency of medium-term activities such as investigations (the 'Knowledge' stage), and improve the ability to create a better future state by operating a new system that has removed the weaknesses and now directs resources to enhanced outcomes (the 'Wisdom' stage)

A fundamental part of data system design should be a clear understanding of how it will be used, but this is regularly left until later. The result is often unusable or impractical.

> *"Part of what we do at RoZetta is to help organisations and individuals to see big data as their ally and a valuable internal asset that can produce measurable returns,"*
> Wright says.

To that end, RoZetta's experts work with clients to extract full value from their data banks.

RoZetta, says Wright, has a trusted track record of expert big data management – "from analytics that add value to the data, to data management technology that enables business, industry and organisations to make meaningful decisions".

RoZetta's DataHex continues to add value to operators in the energy, utilities, health sectors and digital messaging. In a water supply network, the pressure, directional flow and volumes of water were measured by sensors placed throughout the system. The first benefit was the immediate detection of supply interruptions by location and severity.

In the energy sector, sensors measured the volume and purity of a liquified product as it moved through the logistics chain. The system was able to identify changes in volume and detect pollutants as the liquid was transferred from one container to another. An anomaly system was developed to identify possible fraud in mobile and social media messages in digital messaging.

RoZetta experts work with clients, helping to determine why systems fail by reconstructing faults from patterns and evaluating previous experience.

"Detection and diagnosis is a valuable new capability," says Wright.

> *"We help at every stage of the learning process to ensure that the business runs efficiently, ethically, and with the highest integrity – we take a system-wide view, technically and ethically."*

To find out more about RoZetta's solutions to address anomaly detection, contact us via email at **enquiries@rozettatechnology.com**