The first layer of successful data management is anomaly detection

Cybercrime incidents have surged in the last year, as malicious actors take advantage of the current global situation, including the work from home (WFH) trend. As IT has evolved, so too has ransomware, and attacks have become increasingly targeted, pervasive, and damaging. A multi-layered, proactive approach to data management and protection is essential, and this begins with anomaly detection as the first line of defence.

Kate Mollett, regional director at Commvault Africa | image supplied

As IT has evolved, so too has ransomware, and attacks have become increasingly targeted, pervasive, and damaging. A multi-layered, proactive approach to data management and protection is essential, and this begins with anomaly detection as the first line of defence.

The evolving threat

In a WFH environment, people are connecting to critical applications and data from multiple distributed points, without the safety blanket of the enterprise network perimeter. People working from home are also more vulnerable to attack, as it is difficult to maintain standards of awareness when face to face contact is limited.

In addition, cybercrime has evolved into a fully-fledged business. Ransomware-as-a-service is available to purchase on the dark web, and South Africa is an attractive target for attack. In fact, a report from Accenture reveals that South Africa has

the third most cybercrime victims worldwide, losing R2.2bn a year.

Ransomware has become extremely sophisticated, with multifaceted and highly targeted attacks exploiting multiple points of vulnerability. Malware has even begun to attack the data protection solution itself, rather than just production data, making recovery from a successful exploit all but impossible.

The attack surface is so vast, that traditional solutions are simply no longer enough. A new approach to data management and protection is necessary, and this begins with the ability to discover unusual activity before it can cause damage – also known as anomaly detection.

Proactive alerting is the key

Malware exploits rely on slipping through network defences without detection. Much like burglars need to get into a building undetected so that they can steal valuables, ransomware needs time to infiltrate and steal data. Anomaly detection can be likened to a security camera for your network.

It helps enterprises to identify unusual or suspicious network activity as it happens, flagging it for investigation and blocking it before damage can be done. For example, dramatic and sudden increases in network traffic, moved files, or even logins from unusual locations, can all be red flags that a threat actor is attempting to penetrate the network.

With anomaly detection in place, the appropriate people are immediately made aware of potential issues so that they can take action. As the old adage goes, prevention is better than cure. While protecting data is essential, it is actually a secondary issue because an early warning of potential issues means that risk and damage is mitigated. This enables enterprises to take a proactive approach to potential threats rather than reacting after the fact.

Layered threat detection and prevention

Backup and recovery should not be the primary defence against ransomware or any other form of data loss – it is the final step in the process. It is critical today to identify threats, protect applications and data, monitor systems, respond to threats, create awareness, and then if all else fails, recover from an event.

Anomaly detection as part of a data management framework is essential to a holistic solution because data management is about more than just security. Tools like artificial intelligence and machine learning help systems immediately identifying potential threats and automate processes to stop attacks before they can penetrate a network. Building the right framework to manage your data, with multiple layers, covering all areas from the endpoint to the data centre and beyond, is essential to a modern data management strategy.