bizcommunity

Data management is at the heart of cloud security

More businesses are finally making the move to the cloud in the wake of accelerated digital transformation. While these businesses now benefit from enhanced agility and flexibility, cybercriminals have leapt into action to exploit any vulnerabilities that may exist.

By Johan Scheepers 1 Dec 2020

Photo by Alexander Sinn on Unsplash

Ransomware and malware have seen exponential increases in 2020 and this trend is unlikely to abate. Securing your cloud is critical, and the ability to effectively manage your data lies at the very heart of this.

Back to basics

When it comes to the cloud, data protection and availability are key concerns. Without access to data, remote work is impossible and productivity grinds to a halt. Data management is thus central to any cloud security strategy. Sound data management needs to include role-based security and encryption at 256-bit higher, which makes use of a 256-bit key to encrypt and decrypt data or files, making it extremely secure.

Securing and 'hardening' the data protection environment is essential, as is limiting access to the organisation's servers. The data management platform also needs multi-level authentication for approval a authorisation of any changes to data.

Remember the 3-2-1 backup rule, this still applies no matter where your data resides. Keep at least three copies of your data, and store two backup copies on different storage media, with one of them located offsite

An evolving threat landscape

Ransomware and malware are areas of increasing concern. There is a growing trend of cybercriminals beginning to target the data protection platforms themselves to prevent organisations from recovering thei data, even if their backup data becomes corrupted.

Kaspersky Lab's IT threat evolution report for Q3 2019 also highlighted the fact that ransomware attacks now target Network-Attached Storage (Nas) and backup storage devices. This change in malware strategy

necessitates a corresponding shift in data management and protection.

In light of this evolution as well as the recent rampant increase in ransomware attacks, it is crucial to keep a immutable copy of data. To counter the increasing sophistication of cyber threats, new data security techniques have had to be developed.

These include data isolation, which segments backup data to make it unreachable from public portions of t environment, and air gapping, which creates a network with no connectivity to public networks. A layered approach to security will greatly reduce risk.

Proactive prevention is better than cure

Security in South Africa is currently highly reactive. According to an IBM security study conducted by the Ponemon Institute, in 2019 in South Africa, the average time to identify a breach was 175 days and 56 day to contain it. With this time frame, when a threat is eventually detected, it has had enough time to do substantial damage.

The current modus operandi of cybercriminals is to split an attack into multiple payloads to maximise the chance of success. This makes a proactive threat and change detection an essential part of cloud security strategy. Artificial intelligence (AI) and machine learning (ML) are invaluable tools in this regard.

With AI in the data management platform, all files can be monitored and tracked for anomalies, such as suspicious changes to files. Alerts are then sent so that anomalies can be investigated, and potential attac stopped before they cause damage. ML helps the platform to continuously enhance itself for improved protection.

It all comes down to governance

Whether data is stored on-premise, in the cloud or in a hybrid of both, it is important to remember that accountability always lies with the data originator. Consuming services through the cloud does not absolve an organisation of responsibility; an organisation is always ultimately responsible for its own security, data environment and data management.

Ultimately the ability to safeguard data, including that stored in the cloud, relies on data governance. You need to know what your data is, where it is and who has access to it and have a strategy in place for when event occurs. It is obviously still critical to have multiple levels of security, from the endpoint to the data centre to the firewall. Creating multiple areas of fallback helps to reduce the attack surface, with data management acting as the final line of defence when all else fails.

ABOUT JOHAN SCHEEPERS

Johan Scheepers is Commvault systems engineering director for MESAT
View my profile and articles...