BIZCOMMUNITY

The major trends to impact the data landscape in 2023

By Kate Mollett

9 Jan 2023

The major trend impacting the data landscape is the advancing nature of cyberthreats, which continue to evolve and become ever more sophisticated, damaging, and costly to address. While having backup and recovery in place is essential, the reality is that this is no longer enough. Once a breach occurs, the damage has been done and businesses face the financial and reputational implications.

Kate Mollett, senior director at Commvault Africa | image supplied

In addition, there is a growing trend toward double and triple extortion, where even when affected organisations pay the ransom or manage to recover through a clean copy of data, their stolen information is leaked and/or used to attack specific individuals.

Data management needs to become more than just backup and recovery, however, finding a solution to address multiple different workloads is a major challenge.

The mega: cybercrime

Cybercrime is no new phenomenon, but since Covid-19, it seems to have accelerated at a rapid pace. For businesses, it is no longer a question of if they will be attacked, but when. Furthermore, the repercussions of a data breach can be broad, from the immediate impact of lost data and lost productivity, to the cost of recovery, fines associated with compliance breaches, and the hard to quantify damage to reputation that can have long-lasting consequences.

The African online community is one of the biggest in the world, with over 500 million active internet users. However, 90% of online businesses and services in the region do not have the necessary robust security protocols in place. With the number of online users, the wealth of valuable data being transmitted, and the lack of security, countries in Africa are an

attractive and lucrative target for cybercriminals.

The macro: ransomware

Within the cybercrime space, ransomware remains the top threat. In Africa, more than 61% of companies were affected by ransomware in 2020, with attacks targeting critical infrastructure like healthcare and the maritime sector. Phishing is still the leading method that cybercriminals use to gain access to networks to launch ransomware attacks, and social engineering makes these attacks increasingly difficult to detect.

Once a breach has occurred and data has been compromised, there is no guarantee that businesses will not be exploited again, even if they pay the ransom or manage to recover in another way. Increasingly, cybercriminals continue to extort businesses by leaking sensitive information as well as by using the information they have stolen to target individuals.

While it remains critical to ensure that a clean copy of the backup is always available, by the time a ransomware attack occurs, it is already too late and it can be fatal. We need to move toward prevention, rather than attempting to cure the problem after the fact.

The micro: SaaS and AI

Businesses today operate with a variety of workloads and storage platforms across their premises and the cloud. This adds complexity to data management, which is driving the increased adoption of Software as a Service (SaaS) within the data management space. Data Management as a Service (DMaaS) enables businesses of all sizes to afford a robust solution. Inherent in this platform is also automation, resourcing, and skills, which add to increased security posture without adding to expenses.

Given the changing data security landscape, it has become imperative to be able to detect a ransomware attack early. Ransomware typically infiltrates networks days or even months before an attack is launched, and this dwell time can result in backups becoming infected and gives cybercriminals the time to find the most valuable information they can.

Detecting ransomware before it can do damage is increasingly critical, and artificial intelligence provides the key. An AI-based evolution of honeypot traps can be used to lure bad actors or bot attacks to false data points in the network, enabling alerts to be sent within minutes of infiltration, which in turn enables businesses to respond faster, isolate and shut down the attack before damage can be done.

Consolidated solutions are needed

Having a mix of point solutions is no longer effective or manageable. Customers are demanding simplification and consolidation of this complex environment, and companies offering data management and data protection can no longer offer vanilla, off-the-shelf security solutions. Digitalisation needs to incorporate data protection, data management, security, and data insights to drive additional value.

The emerging trend moves away from data management toward data transformation, enabling businesses to leverage the inherent value of their data in a secure and compliant way, with automation and powerful AI delivering system intelligence and improved security posture to allow rapid response to attack.

ABOUT KATE MOLLETT

Kate Mollett is senior regional director at Commvault, Africa South and East.
- Modern data challenges demand advanced management platforms - 4 May 2023
- #BizTrends2023: The major trends to impact the data landscape in 2023 - 9 Jan 2023
- Ransomware is a business resilience issue, not an IT problem - 16 Sep 2022
- Big spike in ransomware attacks calls for adoption of backup-as-a-service - 14 Apr 2021
- Successfully managing risk in a digital world - 3 Jul 2019

View my profile and articles...