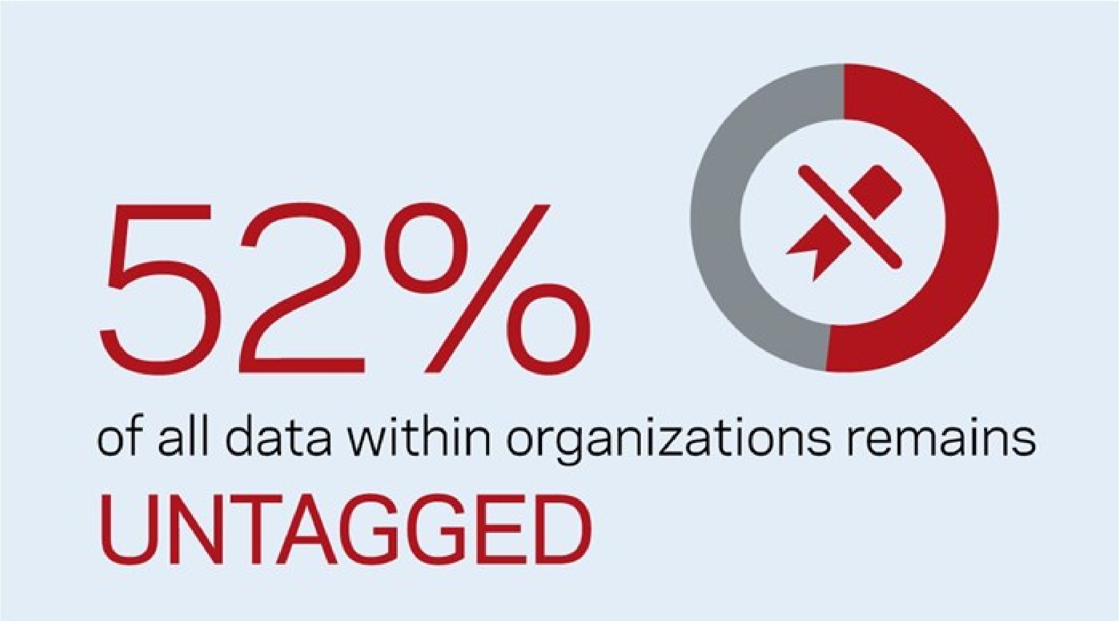
BIZCOMMUNITY

Report reveals 'dark data' exceeds 50%

Global businesses continue to house 'dark data' within their organisations, creating a honeypot for cybercriminals, finds research from Veritas Technologies, a global enterprise in data protection and software-defined storage.

The Value of Data study, conducted by Vanson Bourne for Veritas, surveyed 1,500 IT decision makers and data managers across 15 countries. It reveals that on average, over half (52%) of all data within organisations remains unclassified or untagged, indicating that businesses have limited or no visibility over vast volumes of potentially business-critical data, creating a ripe target for hackers.



Classifying data enables organisations to quickly scan and tag data to ensure that sensitive or risky information is properly managed and protected, regardless of where that data lives. This broad visibility into data helps companies comply with ever-increasing and stringent data protection regulations that require discrete retention policies be implemented and enforced across an organization’s entire data estate.

The weakest links

Public cloud and mobile environments represent the weakest links in data security, with the majority of data across these environments most likely to be left unclassified and potentially unprotected. Just 5% of companies claim to have classified all of their data in the public cloud, while only 6% have classified all of the data that sits on mobile devices. Three in five

(61%) companies admit they have classified less than half of their public cloud data, while over two-thirds (67%) have classified less than half of the data that sits on mobile devices.

3 in 5
companies classified
LESS THAN HALF
of their public cloud data

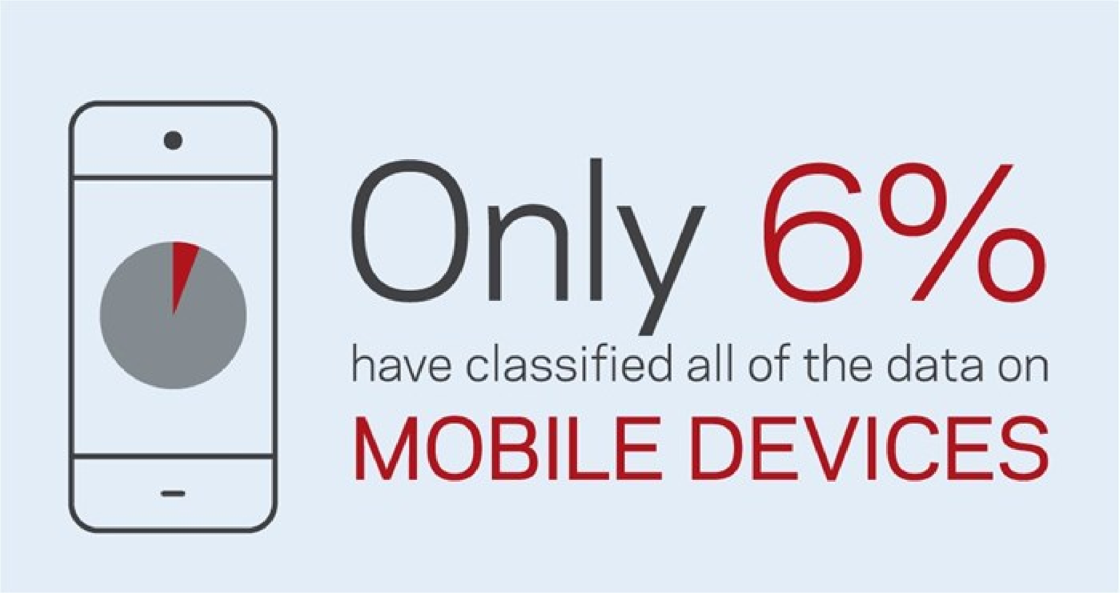
Veritas' previous *Truth in Cloud* research revealed that an alarming majority (69%) of organisations wrongfully believe data protection, data privacy and compliance are the responsibility of their cloud service providers, although cloud provider contracts usually place data management responsibility on businesses.

"As workforces become more mobile and the barriers between work and personal life break down, company data has become dispersed across numerous environments," said David McMurdo, regional director: South Africa.

"When data is fragmented across an organisation and has not been properly tagged, it is more likely to go 'dark', threatening the company's reputation and market share if it falls foul of data protection regulations such as GDPR. So, it's vital that organizations take full responsibility for ensuring their data is effectively managed and protected."

The dark age of data

Organisations consider strengthening data security (64%), improving data visibility and control (39%) and guaranteeing regulatory compliance (32%) among their top key drivers for day-to-day data management. Yet the majority of respondents admit that their organisation still needs to make improvements in all of these areas.



“A company’s dark data reservoir may be out of sight and out of mind for many organisations, but it’s an enticing target for cybercriminals and ransomware attacks. The more organisations know about the data they hold, the better they will be at judging its value or risk,” added McMurdo.

“But with the average company holding billions of data files, manually classifying and tagging data is beyond human capability. Businesses must implement data management tools with algorithms, machine learning, policies and processes that can help manage, protect and gain valuable insights from their data, regardless of where it sits in their organisation.”

Download the full report here