GAINING TOTAL VISIBILITY OF YOUR DATA

BY FEDSCOOP STAFF

Tight, even decreasing, budgets. Manpower constraints. Escalating cyber threats. Expensive, obsolete legacy systems. Executive Order mandates. Federal agencies are struggling every day to find ways to deal with these and a host of other challenges that stress their IT systems.

At the same time, CIOs and agency data stewards must manage, protect and make smarter use of oceans of data that are growing constantly. Every day, the federal government produces or collects petabytes of information, from mission and operation data, to agency and employee records, to basic business documents and social media. All of it needs to be protected. But agencies often aren't making strategic decisions about what data needs to be saved. As a result, they tend to save everything, adding unnecessarily to storage and data management costs.

On top of the struggles faced by federal agencies to manage this explosive data growth, data needs to be put to work effectively. That involves knowing what data agencies have, where it's located, who's using it, and how it can drive better decision making. Ultimately, agencies need to have total visibility of their data in real time.

Compounding that challenge is the growing need to manage data in the cloud, and across hyper-converged infrastructure environments.

That's why a new generation of data management tools have become all but essential to help federal agencies automate the processes of classifying, archiving and discovering data, as well as ensuring that data is protected, regardless of where it resides or where it travels.

FEDERAL MANDATES ACCELERATE NEED FOR CHANGE

How agencies grapple with these challenges is driven in part by federal mandates. The current administration issued an Executive Order in May 2017 directing agencies to strengthen their cybersecurity measures and mandating agencies use the National Institute of Standards and Technology's Cybersecurity Framework to devise ways to protect their data and critical infrastructure.

Security is about more than guarding against intrusions, however. It is about protecting the integrity of the data, making sure it has not been altered, corrupted or deleted, as well as making sure it only gets into appropriate hands.

Meanwhile, the Managing Government Records Directive issued by the previous administration, in August 2012, requires all federal agencies to manage all permanent electronic records in electronic format by the end of 2019.

Agencies were also directed by the prior administration to consolidate data centers and begin migrating data and applications to cloud-based platforms. But agencies have struggled to keep up with the pace of technology changes, particularly as mobile computing and applications, the explosion of video imagery, social media and unstructured data has altered the data management landscape.

Behind that volume struggle lies an increased need for protecting data from hackers and insider threats. While 82 percent of enterprises have a hybrid cloud strategy, up from 74 percent in 2014, according to a report from RightScale, federal agencies have had to move more cautiously to house data in government-sanctioned data centers or government-only cloud environments, even as the data piles up.

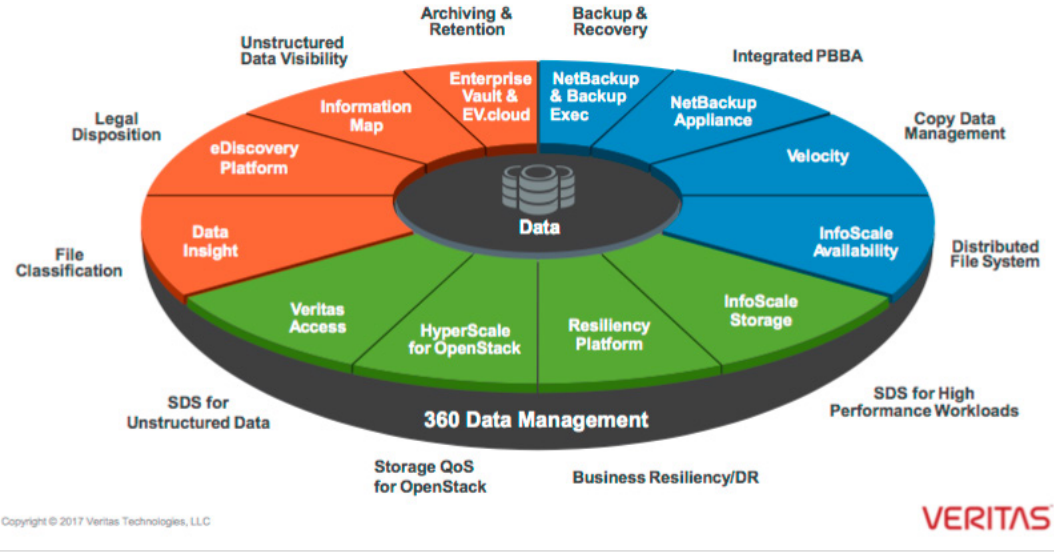
MANAGING DATA IN A CHANGING LANDSCAPE

As more and more information is generated, decisions must be made about where it goes, who gets access, whether it's formatted or unformatted, if it has been cleaned, whether it should be encrypted at rest, encrypted in transit, and how to make better decisions with it.

Those decisions are more difficult than many agency executives appreciate. For example, there's the challenge of "dark data" — information that organizations collect but don't contribute to business activities — where the "owner" of the data really can't be determined. Veritas estimates that organizations spend 52 percent of their storage budget on dark data. Another aspect of dark data is duplicated data – information that may be in multiple locations. Identifying which information is the original and most current, and which are duplicates, also dictates what should be stored, what should be moved to the cloud, and what should be cleaned.

THE NEW VIEW OF TOTAL DATA MANAGEMENT

As agencies grapple with the vast volume of data and documents they generate daily, it's become crucial to have a full suite of tools that can classify, archive and discover information data effectively.



One consequence of this complex environment is that agencies do not have an in-depth understanding of the nature of their data, how it is generated and where it lives.

To resolve this conflict, and make it possible to meet their missions within organizational and budget constraints, agencies need strong information governance (IG), the activities and technologies used to manage information with the goal of maximizing its value while minimizing risks and costs.

New data management tools are now available that can help provide a 360-degree view of the data residing across an agency's IT ecosystem that can drive efficiencies, lower costs and mitigate risk.

WHAT TO LOOK FOR IN DATA MANAGEMENT TOOLS

Data management platforms have evolved significantly beyond single business intelligence tools. The best of breed offerings today provides a combination of capabilities, delivered "as-a-service," allowing agency CIOs to move away from capital investments to more flexible, controllable operating expenditures.

Those platforms include a full suite of capabilities, helping agencies by:

- Establishing end-to-end visibility of data across hyper-converged infrastructure
- Automating data and application interdependencies
- Enabling controls for migrating data across multiple data centers and cloud platforms easily and efficiently
- Providing unified data protection, improving data portability and resiliency
- Generating more powerful insights and actionable intelligence through data mapping, archiving, e-discovery and other tools

Those capabilities, however, must also tie back to three core elements of information governance: Information availability, information protection, and information insight.

Information availability *tools* include data access regardless of where it resides – on-premises, off-premises or in the cloud – and wherever it travels-- to all devices, whether desktop or mobile. Those tools also must have the ability to manage and store data flexibly and on a massive scale, as well as ensure resiliency to maximize uptime and coordinate recovery across diverse platforms.

Information protection *tools* address such functions as automated data backup and recovery, data deduplication, and copy data management.

Information insight *tools* cover a gamut of capabilities, such as mapping data so agencies can better manage information retention policies, e-discovery capabilities, and take advantage of immersive reporting through visual maps and dashboards for unstructured data.

DATA MIGRATION TO THE CLOUD

An integrated suite of information governance tools is especially important in facilitating the transfer of data to a cloud provider, or from one provider to another, by setting in-common rules for data prioritization and classification, and by providing visibility into the process along the way.

Modern data management platforms can also address the challenge of pulling data from multiple agency systems. Look for tools that handle the heavy lifting of interoperability by integrating data drawn from multiple sources.

Additionally, in a multi-cloud environment, each cloud provider uses proprietary metadata, policies and protocols. Look for tools that undertake such tasks as data backup across platforms, so there can be one solution rather than several.

Finally, look for tools that meet federal compliance standards, from FIPS-140-2 to DISA STIGs, and that include modules that match up with government reporting requirements such as FISMA.

It may seem daunting for agencies to implement information governance, especially with all the technological and policy changes they already face. But having a 360-degree view on the scope, sprawl and condition of data can making moving data to the cloud significantly easier, and give agencies greater control.

For more information on what a 360-degree view of data management looks like, and how to improve data insights and security, read more at Veritas.

THIS ARTICLE WAS PRODUCED BY fedscoop FOR, AND SPONSORED BY, VERITAS.