# Data-driven government

## How a software-defined framework makes data more secure & accessible

Government is awash in data. It comes from sensors, from online applications, from a wide range of citizen encounters. But the inherent limitations of legacy systems can make it difficult to access this valuable information and may imperil data security.

Agencies need a new way to interact with their data. They need a modernized approach that isn't tied to hardware, one that transcends siloes to make data readily available and usable across the enterprise, regardless of the source or where the data resides.

Here, Rubrik Public Sector CTO and Digital Transformation Strategist Jeffrey Phelan talks about a modernized vision of data accessibility and security, and points to a way forward for government IT leaders looking to make the most of their data resources.

### Let's talk about data security and data accessibility. Why is this a particular concern in the public sector?

It's a combination of factors. They've got to make sure that they're meeting certain data transparency and compliance standards. They also need to make sure citizen data is secure, whether from hackers or from adversaries or nation states.

At the same time, it's important to make the data available, both to citizens and to users within the public sector, to government employees as well as in the military and other areas. This idea of being able to make data available anywhere and everywhere -- while keeping it secure -- is non-trivial.

### Why is it hard for government to achieve the needed balance of data security and accessibility?

Part of it is the form in which it's kept. We're working with one organization right now that has over 25 million documents that are in paper. They have to digitize that and make that information searchable and available for FOIA requests, for legal requests, for discovery and investigations. And they need to be able to get to it very, very quickly.

And there's the sheer volume. Government is continuing to create more and more and more data every day. You've got sensors everywhere gathering and transmitting data. In the military and intel communities, it could be logistics information, supply chain data. On the civilian side it might be healthcare information or voting information. It just keeps growing.

The tools they have were really meant to manage data there, where it was gathered, or where it was centralized. Those tools made a lot of sense when the data was sitting at one data center or under somebody's desk. Now we've shifted to the cloud, we've moved out of the centralized data centers,

and those tools can't do what they're supposed to do.

That data is not readily available to people on a real-time basis. It is not digitally accessible, or searchable. You can't run analytics on it.

At the same time, the way that organizations are starting to think about data is changing. It's not just about storing it and keeping it there. Now they actually want to use it. They want to interact with it. They want to better understand it. So you have to do things a little bit differently.

## How should they be approaching issues of data storage and management?

The concept now is around having real-time access to that data, regardless of when the data was created or how long it's being stored for. If the need has changed, then the storage architectures need to be responsive to what the new need is.

The storage architectures have historically been tied to the physical location – where that data was generated or where it needed to be accessed. If you start to think about data being available everywhere, all the time, you have to start thinking in terms of software-defined data management.

## How does a software-defined approach hange the picture?

In a software-defined framework, you're freed up from the network limitations, the hardware limitations. You shouldn't really care where the data originates and where you want it to go. Data becomes available in real time, regardless of where you are, with maximum flexibility.

A software-defined framework also allows you to really focus on APIs and automation. The APIs give you maximum flexibility to be able to interact with systems, to apply the analytic tools. This, in turn, allows AI and machine learning techniques to begin to do a lot of the work that historically has been very manual.

## Would different government entities implement his in different ways?

Absolutely. If you think about priorities of an organization, they may be focused on protecting the data, or they may be focused on data governance. One agency might be more concerned about privacy issues, while another is more concerned with data availability.

By definition, a software-defined management framework will be flexible enough to accommodate those different priorities. If one office wants to save emails for 30 days, for example, while another needs to keep it for 90 days, all of that is easily managed within the system. In a software-defined framework, those budgets, those architectures, those governance rules all match up.

All of this simplifies data-management tasks. We can take a workflow that used to include 25 rules, 25 different jobs, and we use modern algorithms and artificial intelligence to go from the beginning to the end of that process in a single step, eliminating the 23 steps in between. We've effectively simplified and collapsed a whole series of legacy jobs into one automated process.

## What's the impact on the IT team?

We worked with one government organization that had eight full-time employees, and all they did every day was run backup jobs, protecting data. The first two hours of every single person's day, 25 percent of their time, was spent restarting jobs that failed overnight.

With automation, they can run their entire infrastructure with just two people, instead of eight. That 25 percent of the time that they spent restarting things that failed overnight, that's now less than 10 minutes per person.

## How can government IT organizations start to shift toward this approach?

Strong leadership is key. That's what helps the organization understand what the objectives are and what the strategies are, when it comes to modernizing the infrastructure.

Government is already working to consolidate its data centers, and with COVID there's been an urgent push to get things into the cloud. That makes this an ideal time to look at modernization – to look at new ways to consolidate data, to harmonize policies.

Agencies don't have time to buy or build an entire new infrastructure, and yet they need to make their data available immediately. This is where Rubrik is being used: To help facilitate that data management so that it's consistent both on-premises and in the cloud.

Agencies don't want to be running separate data protection schemes, and access schemes, and security policy and retention schemes, based on where that cloud is located. An organization shouldn't have its core data strategy dictated by the location or accessibility of the cloud. We feel that that shouldn't matter. We want you to be able to have a standard, a single version of the truth across all of your data, regardless where it's sitting and how it's accessed.

## What's the net win for agencies that are able to go this route?

When you don't have to be tied to your infrastructure, when you have that software-defined fabric managing data across all of the environments, it is actually very freeing. You can start to do automated testing, automated vulnerability scanning. Then data becomes a strategic advantage, a strategic asset.

With modernized data management, defense agencies can focus on supporting the warfighter. Civilian agencies can focus on citizen service. In government, mission is what matters. With data available anywhere, anytime – in a way that is accessible, secure, and manageable – government is empowered to meet the mission more efficiently and cost-effectively.