PROTECTING YOUR CLOUD DATA FROM RANSOMWARE AND MORE

BREAKING DOWN WHAT YOU NEED TO KNOW

GOVLOOP
POCKET GUIDE
2020

GOVERNMENT AGENCIES CONTINUE TO FACE A GROWING THREAT FROM MULTIPLE FORMS OF CYBERCRIME, INCLUDING RANSOMWARE.

CONTENTS

EXECUTIVE SUMMARY

According to IDC, 92% of organizations have adopted a cloud environment, with 64% adopting a multi-cloud approach. With a mix of different clouds, protecting data across workloads while meeting compliance and security requirements has become a critical challenge for many federal agencies today.

In addition to increased cloud adoption, agencies have also seen tremendous growth in recent years in the volume and type of data they maintain, and they need to ensure that they can back up those growing stores and recover that data quickly in the event of system failure.

Additionally, agencies continue to face a growing threat from multiple forms of cybercrime, including ransomware — cyberattacks in which malicious actors take control of an agency's systems and data and demand payment for their release (and often never restore access in any case).

In this environment, it's essential to have reliable data protection and recovery abilities.

In short, agencies need to double down on data protection.

But how? These days, the term "data protection" means so much more than simple data backup. And the above challenges — growing data, multiple clouds, a rising threat environment and difficulties to recovery — stand in the way.

There is a path forward, though. This pocket guide explains how federal agencies can find a backup and recovery solution that will stop data protection sprawl, so they can:

- **Consolidate their tools**
- **Simplify their environments**
- **Streamline compliance processes**
- **Improve the overall state and transparency of their backup and recovery capabilities**
- **Scale effortlessly**
- **Reduce cost**

We'll also discuss the current landscape of data protection and recovery in the federal government; share case studies from organizations that are protecting and backing up their data efficiently and effectively; and offer insights and best practices about how you can continue to keep your agency's data safe, accessible and reliable.

CLOUD DATA & RECOVERY: THEN AND NOW

Let's delve into the progression of federal agency cloud and data storage with an overview of how ransomware and cyberattacks pose serious threats to these efforts.

By the Numbers

40%
of core IT spending will be cloud-related by 2022, and by 2028, cloud will account for 80% or more of IT spending.

49%
of data will be stored in public cloud environments by 2025.

47%
The amount agencies can potentially save by moving a data protection solution to the cloud.

39%
of detected malware is ransomware.

4,000
the average number of ransomware attacks that have occurred daily since Jan. 1, 2016 — a 300% increase over 2015.

$20 BILLION
The amount that ransomware damage costs will reach by 2021.

Important Landmarks

1989: Harvard-trained evolutionary biologist Joseph Popp, creates the first ransomware virus. It's called AIDS Trojan and known as the PC Cyborg. Popp sends 20,000 infected diskettes labeled "AIDS Information – Introductory Diskettes" to attendees of the World Health Organization's international AIDS conference in Stockholm. The disks contain malicious code that hide file directories, lock file names and demand that victims send $189 to a PO box in Panama if they want their data back.

> ***"Federal government data is critically important to the U.S. economy. Moreover, maintaining trust in federal data is pivotal to our democracy."***
>
> ***– President's Management Agenda: One Year of Progress***

2007: The Office of Management and Budget (OMB) releases a directive to executive departments and agencies to optimize individual network services into a common solution, known as the Trusted Internet Connection. The tool is designed to improve the government's security posture by establishing a set of baseline security capabilities through enhanced monitoring and situational awareness of external network connections.

2010: The Obama Administration releases the "25-Point Implementation Plan to Reform Federal Information Technology Management," which spotlights cloud computing.

2011: The "Cloud First" strategy is released to accelerate the pace at which the federal government realizes the value of cloud computing. The policy requires agencies to evaluate safe and secure cloud computing options. To complement the effort, OMB also releases a plan for "Security Authorization of Information Systems in Cloud Computing Environments" known as the Federal Risk and Authorization Management Program.

April 2015: IT staffers at the Office of Personnel Management, which manages the government's civilian workforce, discover that some of its personnel files have been hacked. Among the sensitive data that were exfiltrated were millions of SF-86 forms, which contain extremely personal information gathered in background checks for people seeking government security clearances, along with millions of fingerprint records.

October 2018: The federal government marks its growing maturity in the cloud by replacing Cloud First with "Cloud Smart." When the government developed its Cloud First strategy, cloud adoption was still an emerging trend. Cloud Smart's goal is to increase cloud adoption by addressing concerns around security, workforce and procurement.

May 2019: A ransomware attack hits Baltimore city government computers, shutting down the majority of its servers. The attack costs the city an estimated $18 million, with about $10 million going toward recovery efforts and $8.2 million counted as lost or delayed revenue due to the loss of operations, according to the Baltimore Sun.

June 2019: The Federal Data Strategy is revealed. First teased by the data cross-agency priority goal in the President's Management Agenda in March 2018, the strategy includes principles and practices for federal agencies' data governance along the lines of mission, service and stewardship.

LANDSCAPE: MOVING FORWARD WITH DATA PROTECTION AT YOUR AGENCY

Protecting Data in the Cloud Era

Today, there is no doubt: Data fuels the federal government's mission. And federal agencies are working to harness the power of data. For example, the federal government's proposed 2021 budget funds the development of a U.S. Federal Data Service within the Commerce Department. The budget also puts a priority on bolstering the data science workforce to support initiatives in artificial intelligence and machine learning.

But with more data comes more challenges. They include:

Managing the massive growth of data. Growth is happening across both traditional and unstructured data, such as video and text, making the maintenance, storage and complexity of data real hurdles.

Extending protection to applications. That might be third-party software that employees use for productivity, enterprise resource planning or custom web software designed for public use. Many applications must be backed up while running, which requires application-aware backups that include pending transactions and data sitting in memory.

Application containers, which are growing in popularity, are an important consideration.

- A container is a small bundle of one or more applications that can run on pretty much any system.
- An orchestrator is software that manages containers, moving them from one server to another to ensure that resources are available.

Think of application containers as metal shipping containers and the orchestrator as the transportation folks who move those containers from trucks to trains or cargo ships, as needed. All of those assets — data, applications and containers — must be protected whether they exist in an on-premises data center or in the cloud.

The Case for the Cloud

The cloud has proven to be an effective repository for backups — easy, quick and able to scale on demand. As agencies continue to modernize their infrastructures and adopt digital transformation initiatives, the use of the cloud has become a key platform.

With the cloud in mind, agencies have a variety of strategies at their disposal to ensure their assets are properly protected. They include:

- Backup and recovery from on-premises to the cloud
- Backup and recovery in the cloud
- Disaster recovery to the cloud

Having choices is a good thing. But this all sounds like several standalone solutions, each with different tools and prices, which would mean more pressure on constrained IT staff and budgets. *What agency IT departments need is a single, flexible and easy-to-manage solution to protect sensitive data and all other assets.*

The Choice: Public Cloud or On-Premises?

Now that you understand the big picture of data protection and the cloud, let's look more closely at the public cloud vs. on-premises environments — and how data protection fits into both.

The *public cloud* is a collection of computing services, including software, platforms and entire infrastructures, that third-party providers create and host. Those services are available to anyone via the internet, typically on a subscription basis.

For even greater flexibility, you can spread workloads and storage across multiple clouds in what is known as a *multi-cloud environment*. This model helps ensure availability and keeps services close to end users for the best performance. The public cloud model is appealing to many agencies, mainly because of its simplicity, agility and low startup costs. Plus, you can choose to use whatever backup software you want.

Keeping in line with the Cloud First and Cloud Smart policies, agencies have already migrated many workloads to the cloud. Still, agency leaders continue to invest in their on-premises environments. Why? Security, control and proximity, to name a few reasons.

Right or wrong, the public cloud is often seen as less secure than an in-house environment, or at least more conducive to meeting complex regulatory requirements. And the notion of relying on a third party's services rather than controlling those services on-premises leaves some IT managers with concerns. Plus, your data center is in your backyard, so your data, applications, containers and all services are close by, enabling you to support critical workloads and keep latency issues to a minimum.

But protecting on-premises assets can be expensive, both in terms of capital costs for equipment and software, and operating expenses for maintenance and IT effort. In addition to backup and recovery solutions, they maintain *disaster recovery sites*, which often include a full replica of servers, backup and other systems that take over should a data center go down.

There is another option, which provides some of the best features of on-premises and public cloud environments.

The Hybrid Approach

In addition to a single, flexible and easily managed solution to protect sensitive data and all other assets, agencies must have another tool in their belt: a data protection strategy, which they should also connect to any IT modernization effort.

This strategy must address three priority areas:

- Efficiency: Agencies must be able to get the backups down faster, which means sending less data across the wire and reducing the use and amount of the infrastructure needed to get the backups down.
- Simplicity: Legacy backup environments are typically complex and costly. Agencies should look to tools to make backing up data easier and quicker, and therefore cheaper.
- Transparency: Data protection should be user-friendly and easy for the mission areas to use through self-service and automated tools.

To succeed in data protection efforts, agencies and their leaders should turn to a single, flexible data protection and recovery solution that operates across environments, reduces complexity and simplifies the data backup approach by moving to the cloud and adopting a robust data strategy.

How to Evaluate the Right Data Protection Solution for Your Agency

There are several must-have capabilities to look for in a cloud-based data protection solution:

- A public cloud-based software-as-a-service model for your data center and edge location, or a leased co-location space.
- Reliability and scalability, offering the same quality of data protection for cloud-hosted applications as for applications running in on-premises data centers. Automation and performance are achieved when an application can write directly to the protection target.
- Continuous backup capability with point-in-time recovery, which enables administrators to recover backed-up assets from a specific time in the past.
- Proactive monitoring and analysis, ensuring that backups are occurring as planned and error-free.
- Robust reporting and backup file search capabilities to simplify administration.

Protected from RANSOMWARE?

Together, Affigent and Dell Technologies can help your agency achieve enhanced cybercrime protection. The Dell EMC Data Protection Suite offers multiple options to simplify the protection of your workloads in the core data center, in the cloud, and at the edge. **Learn more at www.affigent.com.**

Affigent

AN AKIMA COMPANY

DELL Technologies

FEDERAL PREMIER PARTNER

INDUSTRY SPOTLIGHT

ACHIEVING CLOUD-BASED DATA PROTECTION ACROSS YOUR AGENCY

An interview with Kevin McDonough, Advisory Systems Engineer at Dell EMC

Today, hackers are attacking public- and private-sector organizations for their data more aggressively than ever. Some bad actors want to own it, some want to delete it and some want to use ransomware to hold the data hostage.

There's no denying it: Cyberattacks and ransomware are on the rise. And in the federal government, the risk of being unable to recover business processes and data affected by these breaches can be devastating because government data is a critical resource agencies can use to improve operations, drive innovation, deliver better services to citizens and improve civic democracy.

The task of data protection traditionally has been especially daunting, given the increasing complexity of the government IT environment. But a cloud-based data protection solution can reduce that complexity, making it easier to manage the environment and provide oversight of compliance and governance, said Kevin McDonough, Advisory Systems Engineer at Dell EMC.

Dell EMC Cyber Recovery is designed to protect an organization's most critical data, McDonough said.

"Cyber Recovery facilitates a robust and proactive workflow to help increase cyber resilience throughout your organization," he said. "We've interacted in this space for a long time, and we've put all our brainpower behind developing this product that is out there to protect people's critical data."

Dell EMC Cyber Recovery is a complete, isolated recovery solution that can help you minimize downtime, expenses and lost revenue by providing a resilient backup to critical data and a path to recovery from a cyberattack.

To start, Dell EMC offers professional services that help you assess, plan, implement and validate your cyber recovery solution. Dell EMC Cyber Recovery keeps your data in a vault, where it is physically and logically isolated from other systems and locations.

> *"Cyber Recovery facilitates a robust and proactive workflow to help increase cyber resilience throughout your organization"*
>
> *—Kevin McDonough, Dell EMC*

Physically, the Cyber Recovery Vault resides in a restricted room or area in your facility accessible only by individuals with authorized credentials. This limits the ability of in-house saboteurs who wish to hold your data for ransom to complete their objectives.

Logically, Dell EMC Cyber Recovery removes data from the attack surface by using the Representational State Transfer application program interface to provide authentication and authorization services in the Cyber Recovery Vault. Additionally, Dell EMC Cyber Recovery brings flexibility in automating robust analytics by integrating custom or well-known industry tools into your workflow. **For example, CyberSense analytics are fully integrated into the product, enabling faster, more assured recovery by identifying the last known good copy of data. Additionally, CyberSense enables forensic capabilities to help quickly identify the source and extent of an attack.**

McDonough said that when evaluating a vendor solution for cyber recovery and data protection, agencies should ask several key questions:

- How resilient is the solution?
- How does it protect you against insider attacks and zero-day exploits?
- How does it defend you if someone successfully penetrates your data?
- Beyond disaster recovery, does it support recovery from cyberattacks (i.e., business recovery)?
- Can the solution operate across environments?

Protecting your agency from the inevitability of cyberattacks — especially ransomware — requires a multilayered approach, he said. With Dell EMC Cyber Recovery, you'll be able to facilitate a robust and proactive workflow to help increase cyber resilience throughout your agency.

Takeaway: A cloud-based solution can reduce the complexity of data protection across the enterprise.

LEARNING FROM OTHERS: LESSONS LEARNED FROM THE FRONTLINE OF DATA PROTECTION + RECOVERY

Learn how organizations are using technology solutions to efficiently and effectively protect and back up their data.

Streamlining IT on the High Seas

Doctors perform 313 million surgeries every year all over the world, but only 6% of them serve the billion-plus people living in the developing world. That's where Mercy Ships and the Africa Mercy, a floating hospital aboard a former rail ferry, come into play.

Based in Sub-Saharan Africa and staffed entirely by a crew of 400-plus volunteers, the nonprofit relies on streamlined and simplified IT, so they can focus on serving those in need of life-saving surgeries and care. Like a federal agency, the Mercy Ships program is mission-driven, with a focus on using IT to improve the quality of care that it provides. Even its back-office systems affect what happens on the frontlines.

To serve more people, Mercy Ships decided to add a second ship to its fleet. They also needed to improve the efficiency of its onshore operations in Golden Valley, Texas, because the site's storage and servers couldn't keep up with applications' demand for resources.

"At least once a day, we had issues with applications slowing down and freezing," said Jonathan Dyson, Director of Enterprise Infrastructure at Mercy Ships. "And support was very difficult because, over the years, we've added many technologies from different vendors."

Even though the new vessel wouldn't launch for four years, builders needed the ship's data center design right away to meet their requirements. For consistency, Mercy Ships would use a similar model in its onshore data center. In addition to delivering excellent longevity, the new IT platform needed to be flexible enough to support hospital systems including medical records, diverse applications for managing safety and business functions such as logistics, and an onboard K-12 school for the staff's children.

Working with third-party Technologent, Mercy Ships evaluated offerings from several vendors — and chose a seamless, software-defined solution from Dell EMC.

"We wanted to consolidate vendors and have just a few partners who could help advance the vision of Mercy Ships," Dyson said. "We knew that Dell EMC would provide the solution and support that would meet our needs well into the future. It's not a flash-in-the-pan newcomer."

With the new platform, Mercy Ships boosted the efficiency of onshore operations and there's less risk of outages. "We have significantly improved our services now that we're using all-flash Dell EMC VxRail Appliances," he said. "Applications are fast and reliable, and data is there when people need it."

CHEAT SHEET

A rundown of what agencies need in a comprehensive solution to successfully protect and recover their data in the cloud from cybercrime and ransomware attacks.

Agencies need a solution that:

- Protects data using technologies including replication, snapshot, backup and archive.
- Delivers unified index and search of file and network-area storage backups.
- Uses long-term retention to public, private or hybrid cloud as a replacement for tape.
- Provides global copy data oversight and management without compromising self-service workflows.
- Provides replication and disaster recovery to any point in time.
- Provides centralized management, analysis and reporting.
- Empowers application owners to use their native tools.
- Delivers common user experience, whether on-premises or in the cloud.
- Covers all consumption models, from on-premise to virtualized environments to hybrid and public clouds.
- Delivers heterogeneous platform support while supporting a broad range of apps.
- Mixes and matches software to deploy across physical and virtual environments.
- Reduces total cost of ownership.
- Optimizes storage tiers with archiving to maximize performance and lower costs.
- Has the ability to modify the mix over time as data grows and the environment evolves.

CONCLUSION

The Case for Balancing Security and Usability in Protecting Federal Data

In the federal government and commercial enterprises, theft and inappropriate access to confidential information can compromise national security, damage a company's viability and reputation, and put individuals at risk.

The federal government and commercial enterprises make significant investments in data protection technologies and take steps to protect their data assets from theft and unauthorized access.

But today's data protection measures often restrict user productivity to achieve an acceptable level of security. And it tends to be difficult to achieve effective security while aiming to enable mobile employees to take advantage of all the features of high-end laptops and tablets.

Every organization must make tradeoffs between security and productivity. No matter what approach companies and government agencies take to provide mobile security, the risk of attack will persist. Nonetheless, they all must work to create and maintain an active defense against these threats and a robust plan for data recovery.

THANKS TO AFFIGENT AND DELL FOR THEIR SUPPORT IN PRODUCING THIS PUBLIC-SECTOR RESOURCE.

Affigent
AN AKIMA COMPANY

About Affigent

Affigent, an Akima Company is a turnkey IT solutions provider dedicated to helping agencies modernize their IT infrastructure while simultaneously improving security and delivering mission-serving solutions faster and at a lower cost. Our engineers, architects and technology partners have experience at all critical points across the enterprise. We can help you exactly when and where you need it most. It may be a cloud assessment, a physical or cyber security issue, or a need to upgrade your network... where we start is up to you. What's important is that together we finish with a stronger, more responsive enterprise and discernibly superior mission outcomes.

Learn more at **affigent.com**

DELL Technologies

About Dell

Progress lies at the intersection of technology and humanity – a reality government IT leaders live every day, but are challenged to support. Dell Technologies provides the end-to-end capabilities that enable federal digital transformation, offering solutions and services that reach from edge to core to cloud. Our story began with two technology companies and one shared vision: to provide greater access to technology for people around the world. Dell Technologies is instrumental in changing the digital landscape the world over, fueled by the desire to drive human progress through technology.

Learn more at **delltechnologies.com**

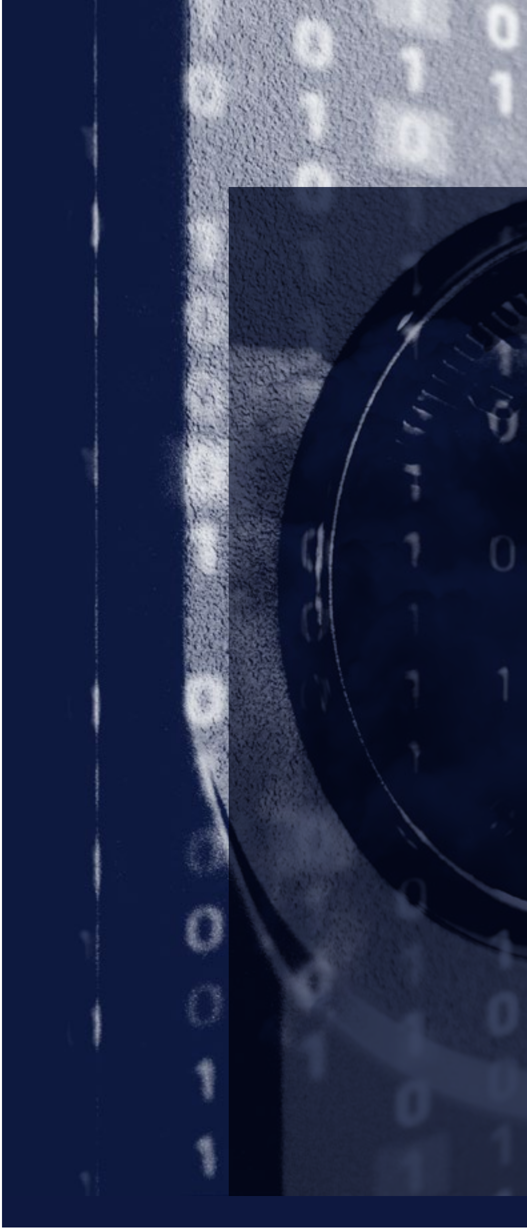
govloop

About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to **info@govloop.com**

Agencies should turn to a single, flexible data protection and recovery solution that operates across environments.



1152 15th St. NW Suite 800
Washington, DC 20005

P (202) 407-7421
F (202) 407-7501
www.govloop.com
@GovLoop