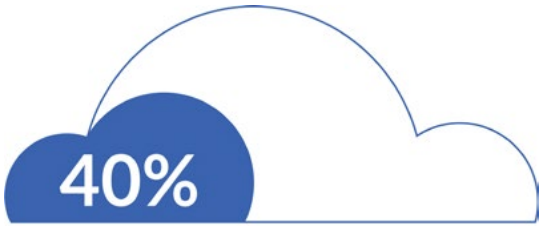
How to Assemble a Data Protection Strategy Checklist

According to IDC, 92% of organizations have adopted a cloud environment, with 64% adopting a multi-cloud approach. With a mix of different clouds and on-premises systems, agencies are struggling to protect data across workloads while meeting compliance and security requirements. To make matters worse, they 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).

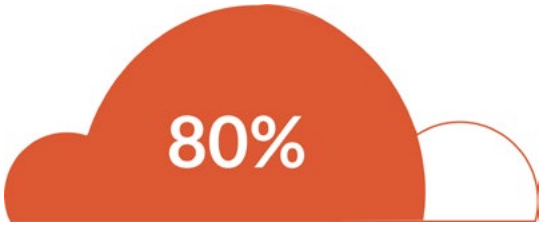
How can agencies simplify their data protection strategies in this complex environment? GovLoop teamed with Dell Technologies and Affigent to offer this checklist to guide your decision-making process.

DATA PROTECTION DATA POINTS

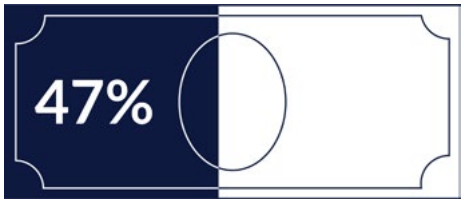


40% of core IT spending will be cloud-related by 2022.

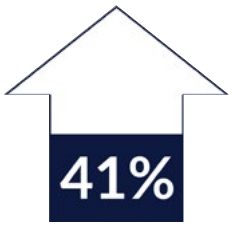
49% of data will be stored in public cloud environments by 2025.



Cloud will account for 80% or more of IT spending by 2028.



Agencies can potentially save 47% by moving a data protection solution to the cloud.



41% increase in ransomware in 2019 from the year before.

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

Ransomware damage costs will reach $20 billion by 2021 .

KEEPING DATA PROTECTION SIMPLE

Because of the various platforms where data resides — the public cloud, the private cloud and on-premises systems — data protection is increasingly complex. The solution? Deploying data backup and recovery solutions in the cloud itself. **Be sure your cloud-based solution covers all three environments:**

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

When choosing a solution be sure you address three priority areas:

1. **EFFICIENCY:** A solution that downloads backup data quickly sends fewer data across the wire and reduces the use and amount of the infrastructure needed to get the backups down.
2. **SIMPLICITY:** Legacy backup environments are typically complex and costly. Look to tools to make backing up data easier and quicker, and therefore cheaper.
3. **TRANSPARENCY:** Data protection should be user-friendly and easy for the mission areas to use through self-service and automated tools.

It's easy to get overwhelmed by the various capabilities and options vendors offer. But don't let that distract you from getting a solution that meets your requirements. **Here are five attributes you should look for in a solution:**

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

When evaluating a vendor solution for cyber recovery and data protection, **you should ask several key questions:**

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

ENTERPRISE-GRADE DATA PROTECTION CHECKLIST

Government agencies can't afford to cut corners on data protection. Whatever solution you select, be sure it can meet the demands of your operations and your mission. **Here's a checklist of enterprise-grade capabilities:**

Start with the essentials:

- O Backup and restore
- O Protect virtual and physical servers
- O Data protection from edge to core to cloud
- O Disaster recovery
- O Any Point-in-Time recovery
- O Flexible deployment options

Make it comprehensive:

- O Multi-cloud optimized with backup/recovery, long-term retention and disaster recovery
- O Comprehensive protection designed to meet your business objectives
- O Protection for multiple hypervisors from a single solution

Leverage automation:

- O Automated policy management
- O Automated discovery of databases and storage

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

Affigent, a Dell Technologies Titanium Partner, 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. As a wholly owned subsidiary of Akima, an Alaska Native Corporation, Affigent offers customers the flexibility and agility of working with a small business, while also receiving support from a global enterprise with decades of experience working with the federal government.

To learn more about how Affigent and Dell Technologies can assist with your data protection needs, please visit affigent.com

Affigent
AN AKIMA COMPANY

DELL Technologies
FEDERAL TITANIUM PARTNER