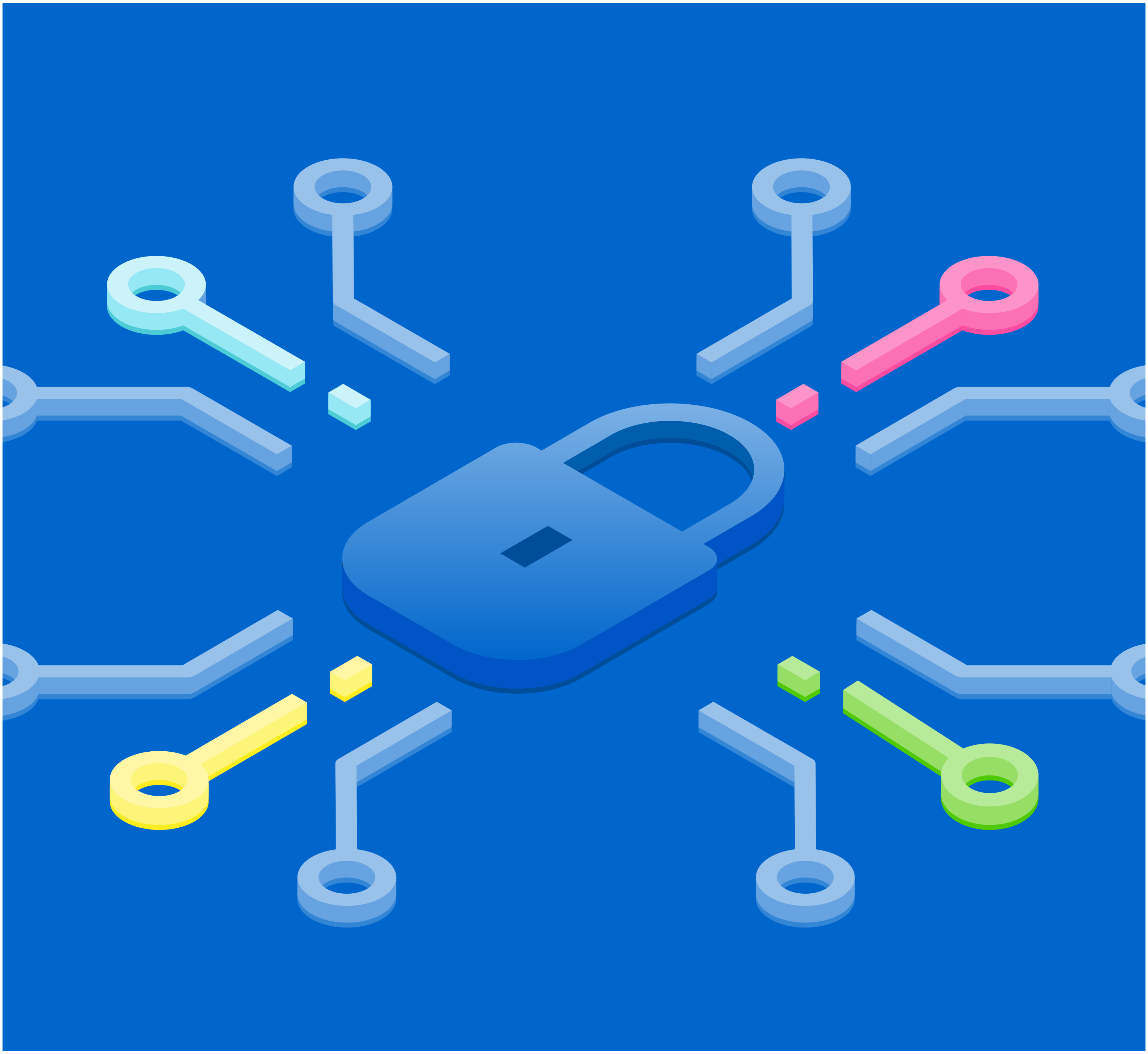

Four Best Practices for Protecting Data Wherever it Exists

MARKET TRENDS REPORT

govloop DELL Technologies carahsoft.

Introduction

The federal government relies on properly managed data to make crucial decisions and serve the public. It’s not surprising, then, that data management and analytics are the cornerstones of the Federal Data Strategy and are top priorities on the National Association of State CIOs’ list of Top Ten Policy and Technology Priorities for 2021.

Today, more of agencies’ valuable data is being created, stored and accessed in the cloud. There are many reasons why the cloud has become a go-to resource for government data: It’s more scalable, flexible and cost-effective than on-premises resources.

Data management challenges federal agencies to find ways to ensure their data is fully protected in the cloud. **While cloud platforms do have some security features, agency data is too important to leave anything to chance. The solution is cloud-native protection.**

To learn more about cloud-native security, GovLoop partnered with Dell Technologies, which provides end-to-end tech solutions to the federal government, and government IT solutions provider Carahsoft, to create this resource. We discuss the elements of a cloud-native solution and offer best practices for ensuring data is fully protected no matter where it resides or how it is accessed.

By The Numbers

85%

of public sector employees who began working remotely when the pandemic hit want to continue to work from home permanently, at least part of the time.

74%

of IT decision-makers say a remote workforce increases the risk of cyberthreats.

33%

of all folders on an organization's servers are open to everyone in the organization.

15%

of respondents to a survey said they were able to recover 100% of their data in Office 365.

>30%

of cyber incidents in the public sector take years to discover.

45%

of federal agencies store mission-critical data in the cloud. That number rises to 52% for state and local agencies.

40%

of local and municipal chief information security officers (CISOs) say they feel only somewhat confident that their information assets are adequately protected from cyberattacks targeting local government and public higher education entities.

10%

of attacks on public sector organizations in 2021 involved ransomware.

40%

of best practices the Federal Data Strategy are aimed at helping agencies leverage the value of and protect federal and federally sponsored data.

Agencies Seek Platform-Agnostic Data Protection

Challenge: Multi-Cloud Complexities

While a multi-cloud environment provides many benefits, it can complicate data protection. Here's why.

- **Cloud solutions alone don't protect against all forms of data loss.** More agencies are relying on cloud-based apps like Microsoft Office 365, Google Workspace and Workday. While these apps offer some level of protection, they operate in a shared responsibility model, which means the customer owns the data and is responsible for protecting it. For example, if a user deletes a file from SharePoint, Office 365 administrators have about three months to recover the file. After that, it is purged from the recycle bin and can't be restored. The same is true of the cloud platform itself, which operates in the same shared responsibility model.

- **Legacy data protection doesn't work as well in the cloud.** While it's tempting to use the same tools and techniques that have worked in on-premises environments to secure data in the cloud, it's not always a good idea. These tools are not designed to protect next-generation SaaS applications and require significant integration to make it work.

- **Ensuring data protection across multiple clouds and a hybrid workforce isn't easy.** It's not uncommon today for some employees to work remotely while others work in the office. No matter where they are located, all employees need to access data across multiple platforms, making effective data security hard to achieve. That's especially true when users are relying on different tools with different capabilities in different locations.

- **When data is dispersed among multiple clouds, compliance is more challenging.** With multiple clouds, it's more difficult to determine where data lives and what level of compliance should be applied. Data spillage—when a file type ends up in an environment that doesn't have the right security posture—also can compromise compliance. This makes it more important than ever to be able to discover files and data wherever they happen to be.

Solution: Cloud-Native Data Protection

Applications and data in the cloud are best protected by solutions optimized for the cloud environment—flexible, scalable, cloud-agnostic; able to handle microservices and containers, and to provide data portability.

"The typical multi-cloud environment today means data is in multiple locations, which can result in real challenges around visibility, management and data protection," said Brad Montgomery, Director of Dell's Federal Data Protection presales team. "With a cloud-native solution that can protect not only cloud data but on-premises data and data on endpoints, agencies can drastically reduce risk."

When considering a cloud-native data protection solution, look for these features:

Comprehensive security: In addition to complying with the Federal Risk and Authorization Management Program (FedRAMP), the solution should enable secure access with modern techniques like multi-factor encryption and role-based authentication. For federal agencies, compatibility with authentication mechanisms like the Common Access Card is also important.

Fast and full data recovery in case of breach or other disasters: An effective data protection solution should be able to store data in an immutable format, which means that it can't be deleted or modified. It should also isolate data in an air-gapped vault, and preserve data integrity and confidentiality with layers of security and controls. These features, combined with machine learning to help identify suspicious activity, enable organizations to recover known good data quickly.

Support for compliance and data governance: To ensure data isn't misused, agencies must follow specific compliance and data governance requirements, such as the Federal Information Security Management Act and various data privacy regulations, as well as agency-specific data policies. One way to ensure compliance is to choose a solution with federated search capabilities, which can locate sensitive files and emails quickly using metadata and can provide defensible delete, which enables deletion of files and emails from both the data source and storage.

Best Practices

Have multiple security checks and balances to protect cloud workloads.

Identity and access management, vulnerability scanning, continuous monitoring, micro-segmentation — these are all critical parts of keeping workloads safe in the cloud. But that's only part of the solution. To ensure full protection, it's important to ensure data is protected in a zero-trust architecture that includes both logical and infrastructure components to ensure users are authentic and that requests are valid. As a final check, make sure your solution is secure to the highest level required, which includes both FedRAMP and Microsoft 365 Government Community Cloud High.

Automate wherever possible.

While IT teams are used to manually configuring workloads, provisioning resources, and monitoring and remediating issues, those processes become much more complicated in the cloud. You can reduce their workloads by automating data protection, making it possible to more quickly discover and protect databases, virtual machines, file systems and containers, and by using a common policy engine to automate compliance and governance across workloads. Automation also can extend to recovery workflows, orchestrating failover, failback and testing to speed and disaster recovery.

Go for the smartest data protection solution you can find.

The mechanics of data protection solutions are important, but it's the intelligence woven throughout the solution that makes all the difference. For example, cloud-based monitoring and analytics powered by artificial intelligence and machine learning reduce the time it takes to pinpoint effective actions. When a dataset is flagged as potentially compromised, that same intelligence ensures data integrity during the investigative process. Beyond data protection, AI and machine learning also can help identify potential issues that could impact productivity, including capacity limits and utilization and performance latency spikes.

Make sure to include endpoint protection in your cloud protection infrastructure.

In today's hybrid work environment, data can't be fully protected if that protection doesn't include endpoints—and that means not only desktops and laptops, but smartphones and tablets. While there are plenty of endpoint protection solutions available, rolling all data protection into one platform, all visible with one console, centralizes and solidifies that protection. This approach ensures data security is built in at all levels so that if a breach occurs, data can be deleted remotely from devices.

"Agencies today need assurance that all of their data, regardless of where it's traveling or where it lives, is protected at all times. The only way to ensure that today is by being able to protect multiple workloads from a single console, on a single platform, with a single user interface, with a single set of reports, regardless of where your data lives."

– Brad Montgomery, Director of Dell's Federal Data Protection presales team

Case Study: Reducing Ransomware, Increasing Peace of Mind

After noticing a substantial increase in ransomware throughout the public sector, the information security team for a state in the central U.S. needed to find a way to ensure all data was protected. It became such a priority that the state allocated emergency funds immediately, with the expectation that the project could get underway within weeks.

Once the team got to work, it discovered that its current systems weren't protecting its Microsoft Office365 or Salesforce.com implementations. The local government focused on a way to address those shortcomings, along with other on-premises and cloud workloads.

The team ultimately settled on Dell Technologies' SaaS-based PowerProtect Backup Service, which covered all required workloads, and provided licenses for more than 55,000 Office365 users and 4,500 Salesforce.com users. The solution also covered 4,500 Salesforce.com sandbox seeding licenses, which provide a sandbox environment for making and testing changes, and train users on those changes before making them available in production.

Since PowerProtect Backup Service has been implemented, all offices across the organization have central data protection for cloud application and end-user devices, aligning with regional policies. In addition, engineering time previously spent supporting backup and archiving has been virtually eliminated. Overall, cloud-native scalability and security has decreased costs and provided significant peace of mind.

HOW DELL AND CARAHSOFT HELP

As a digital transformation leader, Dell Technologies provides end-to-end technology solutions that help organizations deal with today's realities while preparing them for what's next. That means increasing agility, empowering the workforce and innovating with data, all while maintaining the highest levels of security.

Dell EMC PowerProtect Backup Service is one example of how Dell Technologies prioritizes data protection. The cloud-based data protection solution, powered by Druva, centralizes data protection of virtualized environments, databases, file servers and storage (NAS). It also provides eDiscovery, data security and compliance capabilities network-attached to help reduce risk and ensure data adheres to corporate data governance requirements. Agencies also can use PowerProtect Backup Service to protect data residing on endpoint devices.

More specifically, PowerProtect Backup Service provides:

- Centralized monitoring and management
- Automated, no-touch feature updates
- Regulatory compliance
- Source-side deduplication
- Encryption in transit and at rest
- Cloud-to-cloud backup and restore

Dell Technologies' partner, Carahsoft, is a top-performing GSA Schedule holder and trusted government IT solutions provider. Together, Dell Technologies and Carahsoft have been providing data protection solutions to federal, state and local agencies since 2018.

Learn more: www.delltechnologies.com/federal

Conclusion

As agencies embrace the cloud model, they must find better ways to ensure data is fully protected across multiple clouds, even when accessed by users in multiple locations, in a world where security can never be taken for granted.

Cloud-native data protection addresses these issues by protecting data across clouds, including data in critical SaaS applications and on endpoints. This helps ensure data is protected and can be recovered when needed.

ABOUT DELL TECHNOLOGIES

Dell Technologies helps organizations and individuals build their digital future and transform how they work, live and play. The company provides customers with the industry's broadest and most innovative technology and services portfolio for the data era.

Learn more:
delltechnologies.com/federal

ABOUT CARAHSOFT

Carahsoft is The Trusted Government IT Solutions Provider®. Our technology manufacturers and reseller partners are committed to providing IT products, services and training to support Government agencies as well as Healthcare and education organizations. As the Master Government Aggregator®, Carahsoft holds over 100 State contracts and cooperative purchasing vehicles, including NASPO ValuePoint, OMNIA Partners, PEPPM and GSA, to meet the technology needs of State and Local Governments across the U.S.

Visit www.carahsoft.com, follow @Carahsoft, or email sales@carahsoft.com for more information.

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim 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 connect and improve government.

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

govloop.com | @govloop

govloop

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

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop