Powering clients to a future shaped by growth

A Frost & Sullivan White Paper

A Government CIO's Guide to Modern Data Protection

Increasingly critical nature of data and security require advanced backup and recovery solutions

By: Roberta Gamble, Partner and Vice President, Frost & Sullivan

Sponsored By: Veeam

FROST & SULLIVAN

Contents

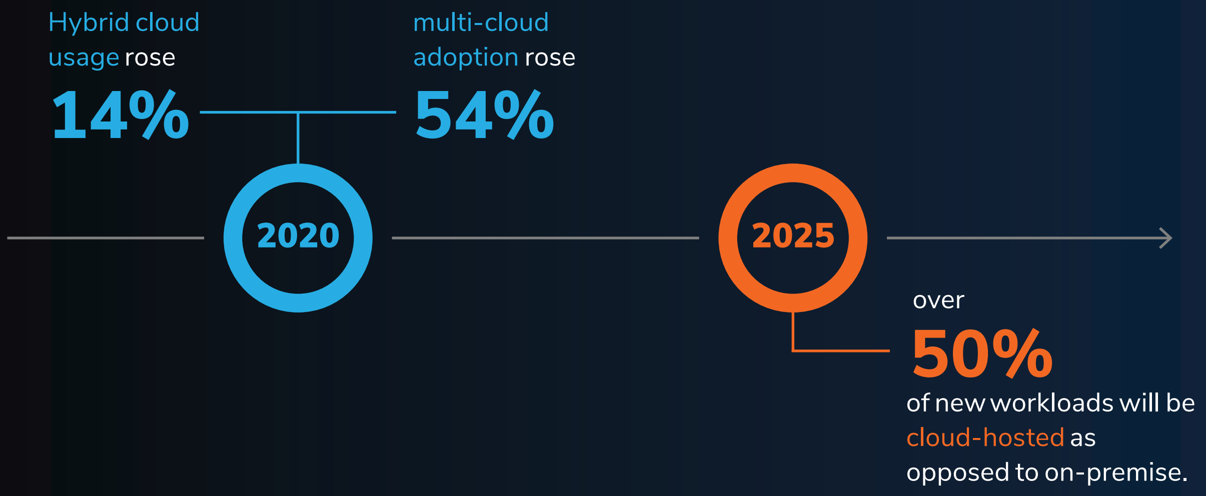
Protecting Data Needs Prioritizing in Today's Modern Government

Digital transformation has an increasing role to play in running the government. Smart Cities that digitally connect departments and can interact virtually with their constituents are a hallmark example of this trend. However, all state and local governments (SLG) have a growing reliance on information and analytics to improve safety, function more effectively, and create better living conditions for their residents.

State and local governments have similar concerns and vulnerabilities as their private sector counterparts. They store and manage large volumes of data from their residents, businesses, and internal departments. State governments are increasingly digitizing services such as taxes, licensing and registrations, and infrastructure management. Cities are employing sensors and connected devices through the Internet of Things (IoT) across infrastructure, such public transportation, traffic monitoring and public lighting. In more advanced cases, cities are using IoT devices to enhance safety and security, with solutions such as gunshot or crowd detection. Sensor data from buildings and streetlamps combined with advanced analytics are also create more efficient systems, such as predictive garbage collection or more responsive snow removal. Some cities have even built sophisticated integrated command and control centers (ICCC) to centralize their monitoring and response, from everyday operations to emergency situations.

The growing volume of information streaming into SLGs needs a high level of security. While federal government cyberattacks tend to grab headlines, state and local governments are a

Hybrid Cloud Usage Expands Rapidly


Hybrid cloud usage rose

14%

multi-cloud adoption rose

54%

over

50%

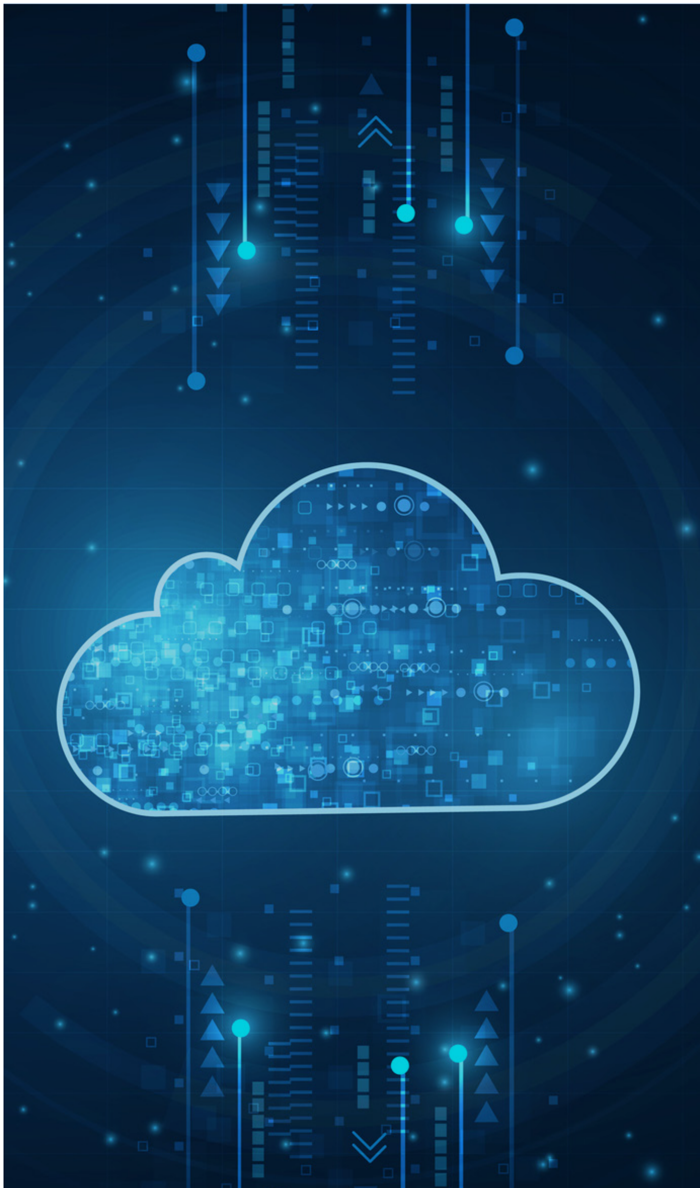
of new workloads will be cloud-hosted as opposed to on-premise.

Source: Results from the 2020 Frost & Sullivan Global Cloud User Survey, December 2020 growing target for criminals and rogue states. For example, SolarWinds Orion incident of 2020—the largest such hack to date—compromised state and local government data as well as US federal government data. In another incident, New Orleans had to declare a state of emergency due to a cyberattack in 2019. State and local governments strive to ensure their data is secure and impenetrable but can struggle with funding and the lack of in-house skillsets to help defend against these situations. These challenges make it critical that data recovery, backup, and management are front and center in a government's strategic cybersecurity and data management strategy.

Governments may believe that backup and recovery will be adequately covered within any data storage scenario, whether on-prem or in the cloud. However, this "set it and forget it" assumption can backfire, leaving organizations vulnerable to failures, cybersecurity breaches and rising data storage and maintenance cost. At present, data recovery rates for this sector are around 31%, and 69% of governments struggle with recovering data within a reasonable amount of time.[1]

Revisiting existing strategies, and placing a focus on data backup, recovery and management provides benefits that go beyond shoring up security. New solutions in the space now include cost saving, unified data protection, no matter where data resides, and that scale and change to meet new needs better than the static and antiquated systems of the past. Advanced data backup and recovery is fast and effective way SLGs can significantly improve the security of their data and systems, and do more with that information. As SLG-related data generation increases and the threat landscape worsens, working with the right partner can help protect critical applications, secure important data, and protect data and applications needed to build modern, healthier societies.

Frost & Sullivan research shows that the average organization juggles **three** different cloud providers



Data Protection Drives Resiliency

Risk mitigation is a key tenet for business continuity and resilience. While organizations typically retained their overarching modernization goals in 2020, strategies to meet those goals tended to focus more on resilience than growth: Frost & Sullivan research[2] shows that the top two priorities for businesses in 2020 were improving efficiency and enabling a better customer experience.

The changes brought forth by events in 2020 also resulted in a significant uptick in the volume and diversity of data being generated and streaming into organizations. The move to remote work meant new systems had to be in place that could accommodate thousands—even hundreds of thousands—of employees now logging in from new equipment or personal devices. In-person interactions, whether with customers or value chain partners, had to be virtualized, which required new tools, apps, and features and resulted in even more data. To capture, process, and utilize waves of new and different information, organizations turned to the cloud.

The cloud is seen as a leading strategy to ensure data hygiene and resiliency, but it also creates problems by obscuring organization visibility. On the one hand, 79% of IT professionals interviewed by Frost & Sullivan planned to improve their disaster recovery (DR) capabilities by moving to the cloud[3]. On the other hand, cloud usage can be ad-hoc rather than closely tied to an organization's strategic growth objectives, making it difficult for IT teams to identify and mitigate gaps in backup and recovery. As cloud usage expands, many organizations find themselves juggling multiple cloud providers: an average of three, per Frost & Sullivan research.

Cybersecurity attacks also rose precipitously in 2020. For example, detected and blocked attempts at ransomware rose 715% in the 12 months ending in June 2020 as compared to the 12 months prior[4]. The combination of growing security risks, rapid cloud adoption, and the lack of prioritizing data backup and recovery creates a tenuous situation that may result in unforeseen gaps, security vulnerabilities, and lost productivity.

Protecting and backing up data is among the most elemental responsibilities of IT, with the "3-2-1 rule" (three copies of the data in two different formats, plus one copy off-site) a common guideline that illustrates the need for spreading risk. However, even this redundancy is rapidly becoming insufficient. Leading IT departments are adding a "0"—creating a the 3-2-1-0 rule—to account for "zero errors." Frost & Sullivan research backs this, showing a strong trend towards "innovating to zero" meaning zero downtime, zero faults and failures, and implementing a zero-trust strategy.

As a result, engaging backup and disaster recovery suppliers is increasing as well, with 46% of companies anticipated to use a BaaS provider by 2023, up from 29% in 2020[5]. Despite this trend, current processes can be antiquated, and older systems are rife with risk: their reliance on manual tasks make them prone to human error, leading to efficacy gaps that leave data vulnerable.

Data storage costs are spiraling upwards as well, whether on-premises (on-prem) or related to unplanned cloud capacity growth. While the amount of data generated in 2020 was exceptional, the expansion of data generation has been ongoing for years and is not likely to abate. Systems may not have been built to withstand rapid increases in data or to handle information on the cloud, in multi- or hybrid cloud scenarios, and across different platforms and even formats.

The improvements that new and advanced solutions have over archaic ones are stark: for one, the cost and coverage picture is much better. Modern solutions that employ artificial intelligence (AI)-driven automation need less manpower to run, and responsive cloud storage keeps data costs in check—by some estimates, these solutions can be as much as 50% less[6] costly in terms of total cost of ownership than their older counterparts. Data management platforms can also increase IT efficiency by 30% and respond 73% faster to problems[7].

> “Data management platforms can also increase IT efficiency by 30% and respond 73% faster to problems.”
>
> – Veeam

In terms of performance, advanced archival solutions furnish much higher levels of data protection, reporting near-perfect RPO and RTO. Scalable cloud storage means comprehensive coverage across all infrastructures, platforms, and formats that are accessed and managed through a unified vantage point. It also means faster duplication and redundancy. The cloud's computing power is what allows AI-based automation to not only be more effective and efficient, but to learn and improve over time. Cross-platform capabilities go beyond providing improved organizational visibility to also include data mobility across platforms, further improving storage, access, and utilization.

Within the realm of data protection, advanced solutions provide better security, value, and the ability to grow and evolve with an organization. In more sophisticated scenarios, modern backup solutions can even help organizations reach into and leverage stored data to augment the growing tools that require vast amounts of information. Organizations are realizing that they need ways to utilize all data more intelligently.

From Automation to Autonomy: Managed Disaster Recovery (DR) takes Data Protection and Resiliency to the Next Level

Protection is non-negotiable, yet modern providers can do more than protect data: they can manage data intelligence and build data trust. Effective data management draws on automation to streamline critical functions such as backup scheduling, replication management, and file restoration orchestration. As noted earlier, a major benefit of automation is reduced human intervention. This lessens the risk of mistakes that can lead to anything from a missed update to a compliance infraction. It also removes a potential threat vector: an estimated 30% of data breaches have internal collaborators, whether intentional or not. Advanced systems are also more efficient. They are built to automatically find the quickest, most direct backup and recovery methods, reduce recovery times, increase data availability, and to simplify process management. Over time, AI-based solutions can determine the best place to store and retrieve data based on usage patterns.

While all data needs to be secure, some needs to be more secure: market performance trends used by an investment firm, for example, may not have the same security demands as a client's account information. Data is also accessed at different times and frequencies. Intelligent automation helps ensure that the right protection and access are optimally executed from the start. It can also learn how security needs evolve over time, based on changes in, for example, usage, policies, or regulations. Imagine the benefits that such a system would have brought to an organization implementing GDPR compliance or ensuring secure, effective data integration as part of an acquisition.

Intelligent automation can track, identify, record, and analyze issues to suggest event resolution strategies. When combined with real-time monitoring, it can accelerate response time and reduces outages and related downtime. Timely notification helps address any issues that the data management system itself cannot execute automatically. Over time, however, the system moves from automation to autonomy, detecting changes in the environment to recognize issues early on, even to the point of predicting a potential failure before it occurs. Advanced tools learn the likelihood of actions leading to certain events and how schedules, policies, and workloads should be managed to ensure complete recoverability. Advanced solutions add significant value through management, above and beyond critical backup and recovery services. Building intelligence through advanced orchestration and management creates greater trust in data, providing an avenue for strategies that more valuable than basic DR.

Beyond Management: Wielding Data's Potential

Perhaps the most exciting aspect of modern data backup, recovery, and management is unleashing the potential of underutilized data. Industry-leading data protection providers go beyond data backup and disaster recovery to include expanded and responsive storage, AI-driven management, and advanced analytics on a single platform. This is elevating backup and DR from playing a role in business continuity assurance to being fundamental to an organization's comprehensive data strategy.

Businesses should think beyond their data stores as simply a place to run to if and when disaster strikes. Rather than a cellar that contains copies of missing or corrupt information, comprehensive backup stores can be the ingredients of an entirely separate "test kitchen" for DevOps and DevTest teams.

Backup data can automate the environment requirement for update and patch testing and troubleshooting. It can deliver a protected production space where new apps can be run in a sandbox-type scenario. It can also be a near-real time resource for advanced analytics, reducing the need for multiple-data replication across the company.

> **“Businesses should think beyond their data stores as simply a place to run to if and when disaster strikes.”**

This is critical for external products as customer experience and ratings are often at the top of the list of organizational priorities. A Frost & Sullivan survey published in February, 2020[8] showed that customer satisfaction rates are the top metric organizations use to measure digital transformation success (44% of respondents), even more so than revenue increases (38%) or cost savings from automation (37%). Misfires on customer-facing upgrades or new apps can have lasting and detrimental effects on an organization.

Next Steps for Optimized Data Backup, Recovery, Management, and Dexterity

Finding new ways to unleash the value of information and insights is (or should be) on the mind of any IT team. Backup and recovery can be viewed as a stepping stone to a more comprehensive, secure, and actionable use of data, rather than a box-checking exercise that fails to recognize the data's potential value to an organization. Automated systems can free up precious IT resources, reduce compliance and audit reporting time, feed into trend and root-cause analysis, and build an autonomous and constantly improving back up system. Advanced systems can be integrated with active data and insights to create a better customer experience or new revenue stream and provide safe and accurate testing grounds that enable flawless app rollouts and upgrades.

While every business is on its own unique digital transformation path, there are a few staging points in which an organization can evaluate, regroup, plan, and execute a more secure and valuable data optimization strategy. Understanding how modern data protection helps protect, manage, and utilize data helps move an organization through these steps. Key questions an organization should ask itself are:

- **What is the current data protection strategy, if there is one?** Is data backup currently relegated to storage and recovery based on task, department, or infrastructure? Or, is there a cohesive program that encompasses all of these aspects without infringing on productivity?
- **What are the costs and time involved to execute current data strategies?** Are expensive IT resources being dedicated to rote or administrative tasks? Would there be value in reducing data recovery and access time exponentially?
- **What role does automation play with the internal or vendor-provided DR strategy?** And, are there tasks that could be improved upon by turning to AI-based solutions? For example, have any backup windows been missed, could compliance reporting or DR testing take less time, and might there be gaps across cloud and on-prem infrastructures?
- **Does the current data leveraging strategy include integrating insights across the organization?** Or, is backed up information gathering dust, only secured and stored for regulatory and security compliance?

State and local governments are increasingly familiar with the benefits that automation can bring to their processes, and often turn to the cloud to realize these results. They also are keenly aware of the regulations and responsibilities placed upon them to keep critical PII and government information secure no matter where backups reside. Relying on outdated legacy solutions can expose organizations to undue risk, as they rarely have the capabilities needed to recovery from cyber threats or the flexibility to scale with changing data protection needs.

Eliminating data protection gaps, engaging automation, and moving to an autonomous backup and recovery system improves productivity and creates robust institutional continuity. A vendor that can support numerous infrastructure types—with an agnostic platform that integrates advanced security and compliance features—helps SLGs organizations focus on their core activities, reduce risks, and be prepared for new and unforeseen challenges.

About Veeam

With more than a decade of innovation, Veeam® continues to distinguish itself as the industry leader for backup and data protection. While we started our company focused on protecting virtualized workloads, our breadth of capabilities now spans physical infrastructure to public clouds like AWS, Azure and GCP, Kubernetes, and SaaS workloads.

Our complete data management platform extends beyond core backup and recovery with monitoring, disaster recovery, data mobility across cloud and data centers, security focusing on ransomware protection, and data reuse capabilities. These key components take backup to the next level. Veeam's platform growth has resulted in a leadership position in every top tier analyst ranking, peer review platform, and growth that far outpaces any leading vendor in the market.

Learn more here.

Endnotes

1 Source: Veeam's Modern Data Protection for State and Local Government

2 Source: Frost & Sullivan's 2020 global cloud user survey

3 Source: Frost & Sullivan's Data Protection & Management in Light of COVID-19

4 Sources: Bitdefender, as reported by the University of South Florida

5 Source: Veeam

6 Source: Veeam

7 Source: Veeam

8 Source: Frost & Sullivan's 2021 Predictions—COVID-19 Accelerates CX Investments.

FROST & SULLIVAN