Why Legacy Backup Solutions Fall Short

of Federal Agencies' Resilience Requirements

Zerto

Introduction

Federal agencies are undergoing digital transformation to improve operations and refine constituent services. Conditioned by the ease of doing business with private sector companies such as Amazon, Microsoft, and Google, as well as datacenter providers like Equinix, consumers have come to expect new levels of customer service—with all the efficiency and immediacy that entails. In their efforts to meet these evolving expectations, federal agencies have started investing in cloud services and new business management technologies to improve agility and meet the demands of 24-hour digital access.

As they do so, agencies must take exceptional care to protect their assets and data. Considering the types of sensitive, legally protected data they handle regarding citizens and organizations, federal entities need robust protection against data breaches and prevalent cyber threats such as ransomware. At the same time, agencies must balance data protection with efficient, agile operations, which require achieving and maintaining IT and cyber resilience.

Resilience allows agencies to protect, replicate and recover data without interfering with their normal operations. As defined by IDC, "the three key tenets of… resilience are the ability to protect data during planned disruptive events, effectively react to unplanned events, and accelerate data-oriented business initiatives." In other words, resilience is necessary to handle whatever IT challenges may arise, all while supporting, not hindering, progress.

Currently, however, federal agencies largely rely on legacy data protection solutions that do not meet the definition of resilience. An IDC study of IT resilience in the private sector found that "as many as 50 percent of organizations could not survive a disaster event." While the study did not formally poll federal agencies, often government entities lag behind non-government organizations in implementing digital transformation and new technologies. This is often due to stove-piped divisions within the federal agencies that limit inter-agency collaboration and IT modernization, reduce total cost of ownership (TCO) for IT assets, and manage multiple IT operations under a single-pane of glass.

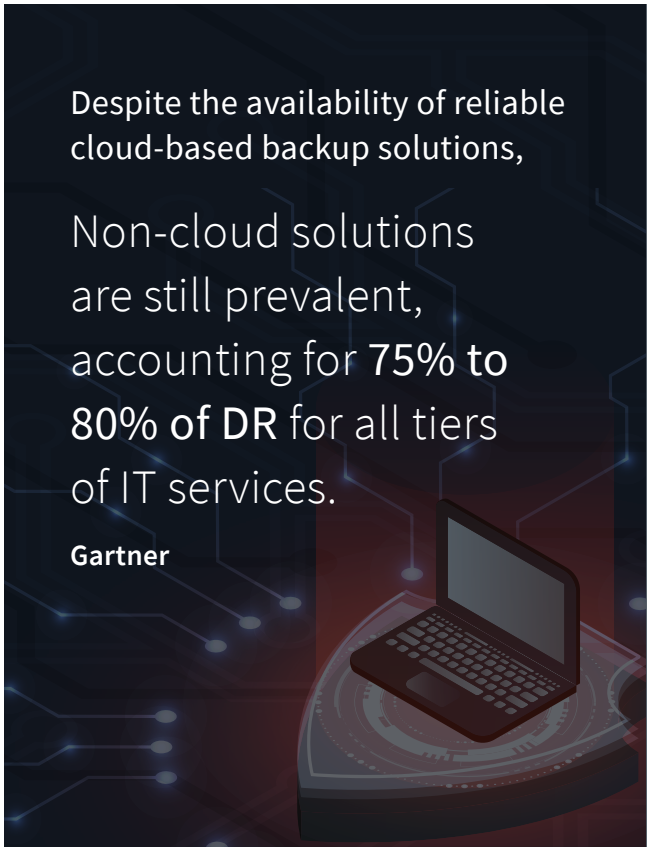
This means that many agencies, as well as half of private sector entities, are not protecting their data as well as they should, testing their disaster recovery (DR) environments or benefiting from an automated IT resilience platform. Due to the stringent requirements outlined within every agency's contingency plans or risk management frameworks (RMFs), however, this clearly needs to change. Agencies need an IT resilience strategy that revolves around continuous data protection (CDP) and replication, with granularity of recovery points within seconds—not hours or days—as well as application consistency to make the recovery process as efficient and effective as possible. With this approach, agencies can see the benefits of more automation, orchestration, and continuity of operations as NIST defines it today in SP 800-34

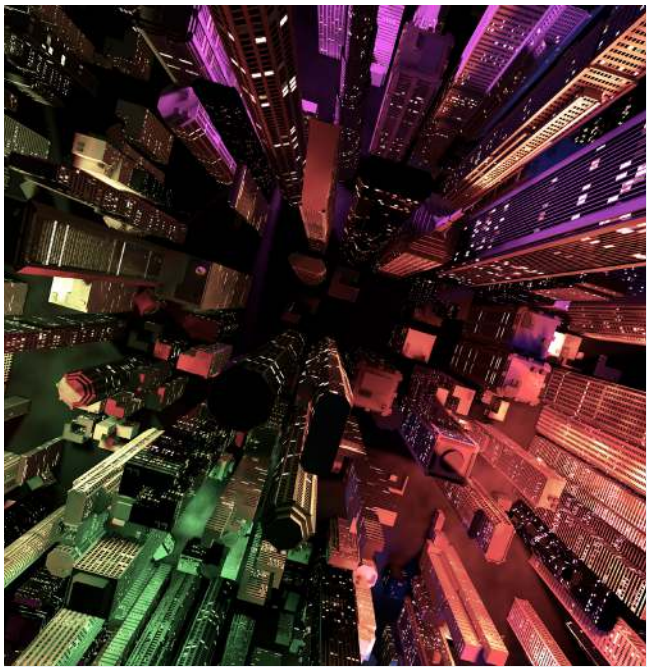
Legacy Data Protection Challenges

As federal agencies undergo digital transformation to boost their agility and availability, they need to review technologies used for their data protection strategies, particularly for effective disaster recovery (DR). Many federal agencies rely on backup technology to protect their data. But traditional data backup technology has experienced minimal change in nearly four decades, making it ineffective and exposing the potential for data loss and protection gaps. The process essentially consists of copying data from production environments after business hours and storing it in a different location, where it sits until it is needed. Data backup typically occurs during off-peak times because it is time-consuming, network heavy, and complex.

Despite the availability of reliable cloud-based backup solutions, non-cloud solutions are still prevalent, accounting for 75% to 80% of DR for all tiers of IT services, according to Gartner. Even more telling, as recently as 2019, 90% of organizations were still using tape backup in some capacity, according to an IT Pro Today report.

The problem with tape and most disc-based backup approaches is that restoring data takes a long time—possibly days or weeks. Additionally, backups occur on a nightly basis, leaving potential data losses of up to 24 hours. In the fast-paced, dynamic environments that deliver digital access, 24/7 availability is a firm business requirement. From one moment to the next, access and availability can be cut off as a result of a cyber-attack, causing the target to scramble for mitigation and service restoration. Ransomware attacks have become especially prevalent in recent years, at times causing major disruptions in major cities such as Atlanta and Baltimore. Government agencies and specific industries are on high alert. A recent Department of Homeland Security alert says threat actors "are targeting the Healthcare and Public Health (HPH) sector with TrickBot and BazarLoader malware, often leading to ransomware attacks, data theft, and the disruption of healthcare services."





To address ransomware, phishing, and other cyber threats, federal agencies must take decisive steps to prevent attacks and implement a solid data recovery strategy to prevent damage to their productivity, services, and reputation. If they continue to rely on traditional backup-based data protection, agencies will not be able to achieve continuous data protection nor address disaster recovery challenges and requirements as they evolve because of numerous shortcomings:

Performance Issues

Scheduling data backups outside of business hours prevents interruption of day-to-day operations and user productivity. Backup solutions use agents in the operating system or snapshots on virtual machines (VMs) to copy data directly from production systems and route it across the network. If the process isn't scheduled during off-peak times, it can cause slowdowns and interruptions, frustrating and paralyzing end-users.

Increasing Complexity

Backups are resource-intensive and must be scheduled at different times for different resources to avoid interference with each other. The more an IT environment grows, the more complex the backup process becomes, often necessitating dedicated physical systems to handle increasing data volumes and specialized roles in the IT team to run them.

Lack of Granularity

Traditional data backup models cannot deliver the granularity required by an agency that places a premium on agility and availability. Backups are periodic by nature and typically are scheduled once a day to avoid degrading performance. If data needs to be recovered, the last available copy can be as old as 24 hours, and a significant amount of data can be lost since the last backup.

Poor Reliability

Many applications in today's environments are spread across multiple VMs, with specific roles and dependencies on other applications in different locations. This setup results in complex application chains that create inconsistencies in recovery. If the backup for one VM is scheduled for midnight and another for 5 a.m., when a restore of both VMs is needed it can take hours to complete.

Resilience Requirements

Once the shortcomings of traditional DR are understood, it becomes clear why federal agencies need a new strategy to achieve IT resilience. As part of their digitization efforts, agencies are implementing cloud-first strategies that replace (or add to) on-premises environments with hybrid, multi-cloud environments that deliver the functionality, availability, and agility they need to modernize their services and operations.

To be truly resilient, agencies need tools and processes to effectively manage and gain visibility into data silos across their hybrid environments. As data grows, it's important to have a handle on where and how it is growing; otherwise, it's difficult to organize and harness the data in ways that seize opportunities to create and refine services. It's important to understand and anticipate the potential for complexity as the different components of hybrid environments evolve. Inevitably, the bigger the environment, the wider the cyberattack surface becomes—a reality that reinforces the acute need for a robust IT resilience strategy. That strategy should cover the following requirements:

Continuous Data Protection

In light of the cyber security risks and service demands that federal agencies are facing, the need for CDP is evident. With continuous data replication, recovery point objectives (RPOs) are within seconds, making it possible to replicate every change in real time without impacting the production environment or users. A scale-out architecture should be in place for replication so that environments with thousands of VMs get the protection they need.

Restoration Granularity

Agents and snapshots cannot deliver the granularity that today's environments demand. All of the changes that take place throughout the day should be replicated to a journal so they can be tracked back to a precise point in time with a granularity of seconds. This way, an agency can recover files, applications, VMs, and entire datacenters with the press of a virtual rewind button for a much faster restoration with virtually no data loss.

Application Consistency

Many applications today reside across multiple VMs with dependencies in other VMs that are geographically diverse. Regardless of location, applications must be protected as a cohesive, logical entity, with recovery points synced across all the VMs that contain data for the application. In this way, when a data restore is necessary, all VMs spin up simultaneously from that same cross-application recovery point.

Regulation Compliance

Short-term data recovery (up to 30 days) is critical for federal agencies in the event of data loss, but each agency also needs long-term retention strategies with different storage and recovery times to comply with relevant data privacy and archiving regulations. True resilience includes addressing this long-term requirement effectively. A platform with CDP and journaling makes it possible to protect and offload point-in-time copies to secondary storage targets as often as an agency deems it necessary to achieve compliance.

The Zerto Platform

Zerto's platform delivers advanced functionalities to meet federal agencies' resilience requirements. The platform addresses current data management and protection needs and scales to anticipate future needs, providing robust protection for agencies currently implementing digital transformation strategies.

The platform helps control costs and tidies up management by converging backup and DR functions into a single, easy-to-use solution. Often, organizations use multiple tools that are costly and complex to maintain and create unwanted redundancy—an IDC study revealed that 90% of respondents want solutions that converge backup and DR—exactly what Zerto delivers.

The Zerto platform solves the shortcomings of legacy platforms that perform restores too slowly and with too much at-risk data. Federal agencies looking to modernize their environments and achieve true resilience should consider these Zerto attributes:

Flexibility and Scalability

- The platform's continuous replication capability saves data in real time without degrading performance or requiring after-hours backup.
- A recovery journal powered by intelligent indexing and search enables data recovery in seconds. Every change is automatically recorded in the journal, making it possible to rewind to a point in time just prior to a data loss incident. Journaling also combines short- and long-term data retention in a continuum of searchable recovery points across data, files and VMs from any point in time, between seven seconds and seven years.

Orchestration and Automation

- With Zerto, it takes only a few clicks to recover files, VMs, applications, and even entire datacenters, thanks to user-friendly workflows that remain consistent no matter what hardware or cloud provider is being used.
- The ability to automate tasks and orchestrate them across the environment enables administrators to pre-define all of the steps needed to recover workloads. This simplifies the process and lets agencies plan and execute exactly what needs to happen following an incident.

Analytics and Control

- Zerto Analytics delivers a single comprehensive overview of the entire IT environment, regardless of the number of sites and clouds that make up the infrastructure.
- Administrators have access to real-time and historical analysis of the health and protection status of the agency's data and applications. Metrics available for review include average RPOs, network performance, and storage consumption.
- Intelligent dashboards deliver detailed data on trends and anomalies to help protect data, make changes as needed, and troubleshoot network issues.
- Analytics enables agencies to boost overall efficiency, make smarter decisions, and achieve and maintain IT resilience.

Conclusion

As federal agencies march forward on their journey of digital transformation, achieving and maintaining IT resilience is a must. They cannot rely on traditional backup solutions for DR to meet today's availability and security demands or anticipate how requirements will evolve in the future. Instead, they should consider how Zerto helps achieve and maintain resilience while controlling costs and simplifying processes. With Zerto, agencies can leave backup windows and painful migrations behind. By taking advantage of features such as journal-based recovery, continuous replication, and protection from data-loss incidents, agencies receive the tools they need to confidently carve a path into the digital future.

Zerto Versus Traditional Backup

Learn how legacy backup compares to Zerto's platform that uses continuous block-level replication to meet rapidly evolving demands for IT modernization, digital transformation, and an 'always on' digital experience.

DOWNLOAD PAPER

About Zerto

Zerto helps customers accelerate IT transformation through a single, scalable platform for cloud data management and protection. Built for enterprise scale, Zerto's simple, software-only platform uses continuous data protection to converge disaster recovery, backup, and data mobility and eliminate the risks and complexity of modernization and cloud adoption. Zerto enables an always-on customer experience by simplifying the protection, recovery, and mobility of applications and data across private, public, and hybrid clouds. Zerto is trusted by over 8,000 customers globally. **www.zerto.com**