

Security, Risk & Resilience

NetApp Shares Their Playbook for Public Sector Data Resilience

How organizations can strengthen protection, recovery, and trust in an era of growing risk.



January 2026

Summary

Public sector leaders face mounting pressure to secure and modernize their data environments, all while balancing limited budgets, lean teams, and complex legacy systems. This playbook breaks down what true data resilience looks like, why it matters, and how to build it step-by-step.

You'll learn the **five building blocks** of a resilient data strategy, **explore a roadmap for practical implementation**, and see how small, incremental actions can lead to major gains in uptime, security, and confidence.

Rather than focusing on tools or technology alone, this guide centers on outcomes: **continuity of service, constituent trust, and long-term modernization.**



At NetApp, we help public sector organizations protect, recover, and optimize their data, wherever it lives. From immutable backups to intelligent automation and embedded breach detection, our solutions make it easier to modernize securely and deliver on your mission with confidence.

Because resilience isn't just about technology. It's about ensuring continuity for the people who depend on it.



Why Data Resilience Matters Now

Public sector organizations are managing more data than ever. And in many cases, it's spread across disconnected systems, aging infrastructure, and new cloud tools that don't always speak the same language.

Resilience isn't just about preventing cyberattacks or system failures. It's about ensuring continuity for the people who rely on government services every day, whether that means processing payments, issuing permits, or dispatching emergency crews.

In short, data resilience means your organization can withstand disruption without losing data, productivity, or public trust.

The Building Blocks of a Resilient Data Strategy



The path to data resilience doesn't start with a single product or platform. It starts with a few key capabilities that work together to keep your information protected, recoverable, and ready to serve your mission. Below are five foundational practices that state and local leaders can focus on today.

1. Immutability: Protecting Data That Can't Be Changed

What it is:

Immutability means data can be written once and never altered, even by an administrator. It's like a sealed vault: you can open it to make a copy, but no one can tamper with the original.

Why it matters:

When ransomware strikes, it often targets backups first. Immutable storage ensures there's always a clean version to recover from — no ransom, no downtime.

In practice:

Many organizations still store backups on the same systems as live data, which leaves them exposed if those systems are compromised. By creating immutable copies, IT teams can isolate their most critical information and guarantee a known-good version always exists. Without immutability, cities and counties have lost weeks of police evidence, case records, and permit data after ransomware encrypted both primary and backup environments, forcing complete rebuilds that take weeks instead of hours.

The Building Blocks of a Resilient Data Strategy

2. Replication and Backup: Creating Reliable Copies Across Locations

What it is:

Replication automatically creates copies of data in multiple places: on-prem, in the cloud, or in secondary data centers. If one location fails, the others take over.

Why it matters:

For agencies serving constituents across wide geographic areas, downtime isn't an option. Replication minimizes service disruption and data loss even in the face of power outages, natural disasters, or attacks.

In practice:

Many organizations are setting up secondary data environments outside their primary region to ensure continuity. If a data center goes offline during a storm, services can fail over instantly to another site. Without this redundancy, public systems like property tax databases or 911 dispatch records can remain inaccessible for days, halting operations and eroding public trust.

3. Tiering: Storing Data Where It Makes the Most Sense

What it is:

Not all data is created equal. Some information — like active case files or utility usage data — is accessed constantly ("hot"). Other data — like archived footage or old payroll records — is accessed rarely ("cold"). Tiering automatically places data on the right type of storage depending on how often it's used.

Why it matters:

Public sector organizations generate huge volumes of data but often operate under tight budgets. Tiering helps control storage costs while maintaining access to critical records. It also keeps systems running faster by freeing up high-performance storage for active workloads.

In practice:

A common pattern we see is agencies storing everything — active and inactive data alike — on the same expensive, high-speed infrastructure. By tiering automatically, older data can move to lower-cost storage after a set period, reducing costs and improving performance. Without this balance, agencies can end up paying premium prices for data that hasn't been accessed in years, or worse, running out of space when active workloads grow unexpectedly.

The Building Blocks of a Resilient Data Strategy

4. Embedded Breach Detection: Catching Problems Before They Spread

What it is:

Traditional cybersecurity tools monitor the network. Embedded breach detection adds an extra layer by watching the data itself. It detects unusual patterns, like sudden spikes in file encryption or unexpected data movement, directly within the storage environment.

Why it matters:

The sooner a breach is caught, the less damage it can do. Detecting issues at the data layer gives IT teams an early warning system, helping them isolate and recover affected systems faster.

In practice:

Organizations that use storage-layer anomaly detection often identify threats before they escalate, such as unusual access to archive files or mass encryption of backup data. When that kind of visibility is missing, a single compromised account can silently encrypt thousands of files before anyone notices, turning a small issue into a full-scale outage or breach that takes weeks to unwind.

5. Automation and Orchestration: Doing More with the Same Staff

What it is:

Automation uses predefined policies to handle routine data protection tasks, like moving backups, verifying integrity, or restoring from snapshots. Orchestration connects those automated tasks across systems, reducing manual effort and human error.

Why it matters:

Government IT teams are under constant pressure to modernize, but rarely have the staff to match the mission. Automation allows teams to manage growing data environments efficiently while focusing their attention on modernization and innovation.

In practice:

Many IT teams still rely on manual verification and data recovery testing — processes that can take entire workdays and are easy to postpone. With policy-based automation, those processes run continuously in the background, reducing error risk and saving time. Without automation, we've seen agencies discover corrupted backups only when trying to restore them — at the exact moment when time matters most.

Together, these five building blocks form the backbone of a modern data resilience strategy. They help organizations reduce downtime, manage costs, and build long-term confidence in their ability to deliver for constituents, even when the unexpected happens.

Building Your Roadmap to Data Resilience

Data resilience isn't a single project or purchase. It's a gradual, methodical journey that strengthens your ability to protect and recover data without disrupting day-to-day operations. The key is to start small, build momentum, and prove value along the way.

Below is a step-by-step roadmap tailored for the public sector — one that fits real budgets, existing staff, and complex legacy environments.

Step 1: Assess What You Have and Where the Risk Lives

Every improvement starts with visibility. Map where your data actually resides: on-prem servers, cloud applications, edge devices, partner systems, and even staff laptops. Identify which data supports essential functions like payroll, licensing, or emergency response. From there, perform a “resilience audit.”

Ask:

- Which systems have recent, verified backups?
- Are critical records stored redundantly?
- How quickly could we recover key operations if hit today?

Many agencies find they're already resilient in some areas but not others. For example, they may have great network security but no immutable backups. The goal here isn't to score perfectly; it's to get an honest baseline.

Step 2: Prioritize What Matters Most

Not all data needs the same level of protection. Focus first on the information and systems that would cause the greatest disruption if lost.

- Mission-critical services: payroll, permitting, case management.
- Sensitive records: personally identifiable information (PII), law enforcement evidence, tax data.
- Time-sensitive operations: emergency dispatch, healthcare, elections.

By prioritizing impact instead of volume, agencies can invest in resilience strategically, protecting what's most vital first instead of spreading resources too thin.

Step 3: Establish Quick Wins

Large-scale modernization projects often stall because they feel overwhelming. Instead, identify low-risk actions that deliver immediate benefit.

- Automate one routine backup process.
- Add immutability for your most critical database.
- Set up replication for a single high-priority system.

These changes often show measurable impact within weeks — less downtime, faster recovery, and clear proof to leadership that resilience investments pay off.

Step 4: Scale Resilience Across Systems

Once initial wins are proven, extend those same principles to other environments, and standardize your approach.

- Use automation policies that apply across on-prem and cloud.
- Consolidate monitoring and breach detection into a single dashboard.
- Document processes so that every IT team member can execute them consistently.

Scaling this way builds organizational confidence and keeps data protection from being person-dependent.

Step 5: Review, Report, and Reinforce

Data resilience isn't "set it and forget it." Schedule recurring reviews, such as quarterly or semi-annual, to test recovery times, verify backups, and update policies as systems evolve. Tie those results to outcomes that matter to leadership: reduced downtime, lower storage costs, improved audit readiness, and constituent confidence. That data tells the story of modernization in measurable terms, helping secure ongoing funding and executive buy-in.

The Payoff: Confidence, Continuity, and Trust

When agencies build resilience step by step, they don't just prevent disruption, they gain control.

- Confidence that critical systems will recover quickly.
- Continuity of operations no matter what happens.
- Trust from constituents who rely on digital services every day.

And while technology underpins it all, the ultimate outcome is human: giving public servants and residents alike the assurance that essential services will be there when needed most.

Moving Forward: From Awareness to Action

Public sector leaders know that resilience isn't a luxury anymore; it's a responsibility. But building it doesn't have to mean replacing everything or taking on new risk. It starts with doing more with the data, infrastructure, and people you already have.

The organizations making the most progress aren't the ones with the biggest budgets — they're the ones putting the fundamentals in place: immutability, replication, automation, visibility, and policy-driven recovery.

That's where NetApp helps.

NetApp's data resilience technologies give IT teams the confidence to strengthen protection, reduce recovery time, and modernize securely, without heavy lift or unnecessary disruption. Whether it's defending against ransomware, improving backup reliability, or simplifying multi-cloud management, NetApp makes it easier to turn good intentions into measurable resilience.

Because resilience isn't just about technology. It's about ensuring continuity for the people who depend on it.

**Explore how
NetApp helps
public sector
organizations
build cyber
resilience.**



January 2026