SOLUTION BRIEF

Modern Data Protection for Critical Infrastructure

Protecting state and local governments against critical service interruptions and data loss from cyberattacks.

From turning on the lights and running the faucet to commuting to work, Americans have an expectation that there will always be power, clean water, transportation services, and other critical infrastructure services that are used in everyday life. Critical infrastructure provides the services that ensure the security, health, safety, and well-being of all Americans. Cybersecurity threats to critical infrastructure are one of the most significant strategic risks to the continued operation of these fundamental services.

State and local government agencies responsible for maintaining critical infrastructure know that keeping these systems operating smoothly and continuously is no easy task. Critical infrastructure is increasingly becoming a favorite target for cybercriminals looking to exploit the vital services citizens rely on.

Bad Actors Are Relentless—and Increasingly Sophisticated

In 2022, 106 state or municipal government agencies were affected by ransomware, based largely on publicly available reports. Since not all incidents are made public, the true number of incidents in all sectors of the economy is—and has always been—higher than reported. State and local government organizations reported one of the highest rates of data encryption following an attack, with almost three-quarters (72%) of respondents saying that the adversaries succeeded in encrypting data. Only 20% of state and local government organizations were able to stop the attacks before data could be encrypted. According to a recent survey, 82% of state and local government respondents said their organizational ability to operate was impacted by the ransomware attacks.

As recent world events have shown, international conflicts can begin with cyberattacks that cause disruptions to critical infrastructure, which can cripple state and local government operations. In an interconnected world, a cyberattack can have far-reaching

Rapid Recovery

Get mission-critical data back online fast.

Immutability

Pure SafeMode creates secure backups that can't be eradicated, modified, or encrypted.

Cost Effective

Achieve 30% to 60% lower total cost of ownership and get twice the data reduction and less risk with Evergreen.

consequences. Nation-states and their proxies, transnational criminal organizations, and even domestic cyber criminals use sophisticated and malicious tactics to undermine critical infrastructure.

Across the government, attention has been focused on cyber threats targeting critical infrastructure. In 2022, Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency, called on U.S. critical infrastructure operators to put their "shields up" and be prepared for cyberattacks. And the American Rescue Plan Act provides cybersecurity funding for state and local agencies. In addition, funding from the State and Local Cybersecurity Grant Program and the Tribal Cybersecurity Grant Program helps eligible entities address cybersecurity risks and threats to information systems owned or operated by—or on behalf of—state, local and territorial governments.

Building Data Protection into Government Cyber Defense

Data protection is an essential component of any cyber defense and mitigation plan and should be viewed as more than just creating a backup as an insurance policy against an attack. Backups should be the last line of defense. Many backups just aren't fast enough to get an agency back online after a total shutdown. That's why organizations need to take a serious look at next-generation backup solutions—implementing architectures that can help them address every angle, mitigate every risk, and give them every chance to be as resilient as possible. Modern data protection is resilient, fast, simple, and cost-effective, and can be established across platforms and technologies to deliver efficient protection of critical data and applications, with fast restores.

Pure Storage® works with leading data protection partners to deliver solutions that support government entities before, during, and after an attack. Backup, replication, snapshot management, and other data protection features are integrated with both Pure Storage FlashArray™ and FlashBlade®.

Minimize Loss of Data and Service through Preparation

While every cyberattack looks different, there are actions state and local governments can take to minimize the risk of an attack and prepare to respond quickly during and after an attack to restore essential services—or ensure they never go down at all.

Before an Attack: Close Security Gaps

Agency architectures should be built with resiliency and durability in mind. Pure Storage can help by providing access to a large pool of analytics data and the fastest analytics processing to identify threats.

Although it's not possible to guard against every known security threat, knowing the common vulnerabilities that cyber attackers exploit can help state and local government technology teams create the right plan to minimize risk before an attack occurs. Here are five critical ways to proactively bolster defenses before an attack:

1. Perform good data hygiene on systems. Unsupported operating systems and unpatched software open the door for malware infections and other attacker exploits.
2. Implement multi-factor authentication and admin credential vaulting for all systems.
3. Provide consistent logging across the entire environment, and then protect those logs against hackers.

4. Implement a fast analytics platform to help identify signs of threat actors in the environment.
5. Run regular security awareness training with a focus on ransomware and other cyber threats.

Modern cyberattacks are now targeting backups—modifying or completely wiping them out. The importance of cyber resiliency and the need for faster recoveries from ransomware is more important than ever. The solution calls for immutable backups that cannot be compromised. Technology teams can secure their agency before an attack by implementing Pure Storage SafeMode™ snapshots, which locks down the critical data needed to recover from an attack quickly. Since SafeMode snapshots are immutable, they can't be corrupted or encrypted by an attacker. When SafeMode is enabled, backups cannot be destroyed—even if admin credentials are compromised. SafeMode is available with both FlashBlade and FlashArray.

It takes less than a millisecond for SafeMode to create a few persistent data structures, and snapshot policies can be configured to cover frequency and retention, along with the ability to send snapshots to a variety of destinations.

During an Attack: Fast Restore with SafeMode

It's one thing to prepare for an attack. It's another to methodically work through the steps to minimize damage and speed recovery during an attack. Pure Storage provides always-on, data at rest encryption, with no performance overhead or management required, and eliminates the ability for protected data to be modified or deleted, thus ensuring recoverability during an attack.

Here are steps state and local governments can take during an attack to minimize disruption of critical services:

1. Contain the attack and lock down the environment. At the first sign of a breach, isolate impacted systems on the network by disconnecting them completely or quarantining them in a private network enclave.
2. Mobilize emergency response teams and launch internal and external communication plans.
3. Begin the forensic process.
4. Move to a staged recovery environment.

With SafeMode, agencies can start recovering immediately with immutable data backups that hackers can't access, enabling technology teams to get back online quickly.

After an Attack: Recovering with Pure Storage

Knowing the immediate steps to take after an attack's initial stages can help to minimize loss, cost, and risk. Pure Storage offers the industry's fastest recovery rates for backed-up data (petabytes per day) and supports fast forensic recovery processes through instant, space-saving snapshots. For traditional backups, Pure FlashBlade provides incredible restore speeds—up to three or more times faster restore than disk or hybrid products.

Here are steps to take in the immediate wake of an attack:

1. Prioritize systems for recovery and restoration efforts.
2. Continue forensic efforts and work in tandem with the proper authorities, your cyber insurance provider, and any regulatory agencies.
3. Begin recovery efforts by restoring to an offline sandbox environment that allows teams to identify and eradicate malware infections.

Achieve Financial Flexibilty, Agility, and Energy Efficiency

Eliminate the complexity and cost associated with storage administration with a sustainable storage as-a-service (STaaS) subscription that provides financial flexibility and operational agility, while mitigating IT risk. State and local government budgets are tight. Modern data protection from Pure Storage includes a cloud-like acquisition model that enables agencies to focus on innovation rather than having to manage day-to-day storage administration tasks.

Agencies can purchase Pure solutions via traditional capital expenditures, but they are also available via subscription. With Evergreen//One™ we remove the concept of infrastructure and replace it with a service where customers can subscribe to the consumption, performance, and service levels they need—when and where they need it.

Evergreen//One combines the agility and flexibility of public cloud storage with the security and performance of an all-flash infrastructure. This guaranteed, SLA-driven storage service improves how data is stored, mobilized, and protected. All SLAs and commitments are continuously met. We guarantee performance, capacity, availability, no planned downtime, and energy efficiency.

The Most Comprehensive Data Storage Subscriptions

Delivering the most comprehensive data storage subscriptions, the Pure Storage Evergreen® portfolio offers unequaled choice and flexibility in how you purchase and consume storage—all based on the proven, non-disruptive Evergreen architecture that keeps technology up-to-date seamlessly, with no disruptive upgrades. Achieve 30% to 60% lower total cost of ownership and get twice the data reduction with less risk. Pure Storage modern data protection is flexible and ongoing, ensuring that agencies have access to the latest technology updates, so your data is always secure.

Making Data Protection Modern

Knowing the challenges you'll face first, and the immediate steps you can take during and after an attack, can help agencies safeguard data and ensure continuity of critical infrastructure operations. Your bottom line is minimizing the damage done and getting up and running quickly after an attack—and Pure Storage is here to help.

Additional Resources

- Find out more about Pure's modern data protection solutions.
- Learn about resiliency architectures and how to build one.
- Read how the City of New Orleans got back online quickly and securely following a ransomware attack.
- Explore Portworx® backup for disaster recovery.
- Get the ransomware survival kit for state and local governments.

PS2252-02 02/2024