White Paper

How Local Governments Can Use Hybrid Cloud Storage to Prevent Ransomware Attacks

zadara

It took Baltimore's city government three months before they could send out their first water bills to their customers while facing an $18 million in direct costs and lost revenue. Riviera Beach, Fla., approved the payment of nearly $600,000 and Lake City, Fla., agreed to pay $460,000. In Texas, 23 municipalities were recently hit — likely because small towns are more vulnerable than larger ones.

Underfunded and Vulnerable

Local governments often lack the technology and resources to combat such attacks. Underfunded budgets, outdated technology and lack of training in current best practices combine to create the perfect storm. Several of the cities attacked found their technology, which should be replaced every four or five years, was being stretched to double its life expectancy.

Increasingly sophisticated criminals are demanding payments that fall just under what cyber-insurance covers, making it more likely that a ransom will be paid. Their game is to target the most vulnerable, which is why they go after state and local governments. Unfortunately, the only choice for some victims of a ransomware attack is to pay the ransom if they ever want access to their data again. They also face the prospect of delaying access to online payment tools, court records, 911 systems and much more.

A Roadmap with Built-in Protection from Ransomware

Last year, at the NCTA Cyber Prevention Tech Talk presented by the FBI, a team of experts provided a list of five steps every IT organization should follow to reduce cyber-attacks:

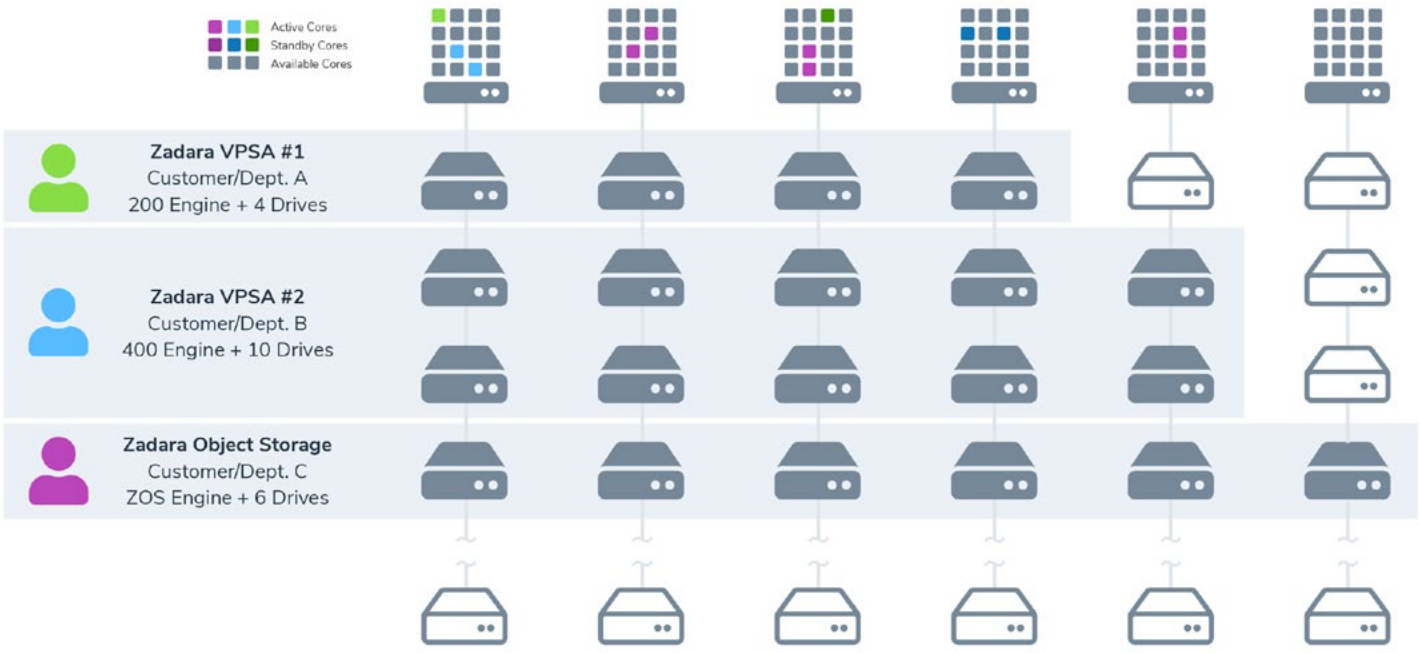
1. Isolate
2. Monitor
3. Test
4. Upgrade
5. Plan

Based on their research, the FBI concluded that the majority of IT systems lack basic protection, and that there are significant challenges to implementing these guidelines. Nevertheless, IT organizations can significantly improve their defenses against a ransomware attack without the need to make costly or disruptive changes to their infrastructure.

Fully-Managed Backup and Protection

Zadara enables local governments to quickly (and affordably) adopt a more effective approach to data storage and management. The Zadara approach offers two key advantages to governments that want to successfully stay ahead of the criminals. First, Zadara gives IT managers and administrators a highly affordable, 100%-OpEx solution that is both technically sophisticated and simple to administer. Second, and just as important, Zadara's team of data storage and management experts is available 24/7, to monitor and respond to threats to your data.

Of course, Zadara offers all the availability, security, and functionality you expect in enterprise storage. Dedicated HDDs and SSDs (including NVMe), in-flight and at-rest encryption, snapshots, mirroring, HA and more. High-performance block, file and object storage within a unique multi-tenant architecture that delivers 100% resource isolation, giving you the power to create multiple storage tiers with consistent and predictable performance, even in shared environments. And the platform is architected with redundancy at every level, ensuring a safe and secure enterprise storage solution.



Guideline #1: Isolate

With storage, isolation of critical data, such as financial data, from day-to-day operations and user shares, as well as test and dev, is the first step to more effective protection. If one system becomes infected, the others are safe from contamination. To prevent data crosstalk and commingling of assets, Zadara's patented architecture isolates resources in Virtual Private Storage Arrays (VPSAs), comprised of physical drives, vCPUs and networking. This way, isolation occurs naturally within a private VLANs. Further isolation is employed by using SR-IOV technology to isolate core infrastructure from VPSAs.

Server records specify which hosts have access to what share. Within a VPSA, share isolation is implemented with server records. This can be configured as a one-to-one or many-to-one relationship using subnet or CIDR notation.

Guideline #2: Monitor

Monitoring your systems is a key part of a ransomware defense strategy, but it is time-consuming and requires expertise. With Zadara you can offload this duty to our staff of IT and storage experts dedicated to protecting your data. The Zadara Hybrid Storage Cloud includes an out-of-band management layer isolated from the VPSAs. The management layer provides our operations team a way to monitor and rapidly respond to issues that may arise. For example, over-utilization of pools and performance are often leading indicators of infection. These indicators are monitored and can be configured for early detection of issues.

Ransomware viruses read files and rewrite them in encrypted format. This attack will have higher I/O activity and pool growth. Zadara VPSA's built-in system monitoring – when enabled – can provide an early warning system, sending email alerts when suspicious activity is detected.

Two Triggers that Should be Set

- I/O's Per Second (IOPS)
- Pool Size Utilization growth due to large Local Snapshots

A common trick employed by ransomware is to rename of files with a ".lock" suffix. Zadara has Docker-enabled VPSA controllers which allow you to run apps on the VPSA. Using apps which trigger on the renaming of files provides early detection of an ongoing attack. Visit GitHub to view our public Docker repository for a few examples.

Guideline #3: Test

Penetration testing is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit. Penetration testing can be automated with software applications or performed manually. To ensure there are no open doors or exploits that can enable unauthorized entry our storage experts routinely perform penetration testing on cloud deployments.

In addition, Zadara is SOC2 compliant. SOC 2 compliance is a component of the American Institute of CPAs (AICPA)'s Service Organization Control reporting platform. Its goal is to make sure that systems are set up so they assure security, availability, processing integrity, confidentiality, and privacy of customer data. SOC 2 is both a technical audit and a requirement that comprehensive information security policies and procedures be written and followed.

Guideline #4: Upgrade

The nature of any complex system is that, without intervention, entropy will occur, and data storage systems are no exception. It is imperative that bug fixes and security patches be applied, in a timely fashion, to ensure that protective measures do not become obsolete and easily exploited. Zadara's storage services are architected for non-stop operation, including non-disruptive updates. These upgrades are are applied by Zadara support operations staff, in consultation with users, as part of the storage service.

Guideline #5: Plan

In a ransomware attack, the criminals gain access to your backups, which they overwrite or erase. Painful experience has shown that existing backup policies are ill-equipped to provide adequate ransomware protection. Most pre-ransomware backup policies dictate two copies,

both on the same media type, and both in one location. This policy is referred to as 2-1-1. Even a strategy of 3-2-1, (three copies, two media types, and one offsite location), may be inadequate. An additional, isolated copy is necessary ('3-2-1-1') for complete backup protection.

Zadara's VPSAs offer integrated Backup to Object Store protection that allows for rapid recovery of data in the event of an attack. Redirect-on-write snapshots provide a write-once-read-many (WORM) drive capability that inhibits ransomware from obliterating data. Employed with file growth rate detection methods described below, data is protected early to reduce or eliminate costly recovery.

To ensure dependable backups, redundancy is key. Multiple backup configuration strategies like the following can help an organization navigate the risk of ransomware and keep service levels high without data loss.

2-1-1 (For non-critical data)

Copy 1: VPSA Volume or Share

Copy 2: Local Snapshots or Backup to Object Storage

3-2-1 (For critical data)

Copy 1: VPSA Volume or Share

Copy 2: Local Snapshots or Snapshot Mirror to Remote VPSA, Media Type #1

Copy 3: Backup to Object Storage, Media Type #2, Offsite

3-2-1-1 (For critical data and Disaster Recovery)

Copy 1: VPSA Volume or Share

Copy 2: Local Snapshots to Remote VPSA, Media Type #1

Copy 3: Snapshot Mirror to Remote VPSA, Media Type #1

Copy 4: Backup to Object Storage, Media Type #2, Offsite

Start Now and Take Control

Don't wait until it's too late. Using the guidelines from the FBI you can create a roadmap to protect your data against ransomware. Contact Zadara to find how we can help protect you from cyber-crimes.

Transform your business with zero-risk enterprise storage.
Zadara transforms storage-related costs from a variable mix of equipment and management expenses to a predictable, on-demand, pay-per-use, elastic service that greatly simplifies planning, streamlines budgeting, and improves return on investment (ROI). Find out how zero-risk enterprise storage can help you transform your business. Call or email today.

+1 949 251 0360
sales@zadara.com
www.zadara.com