E-BOOK

Ransomware Defense for State & Local Government: A 3-Part Strategy

NASUNI®

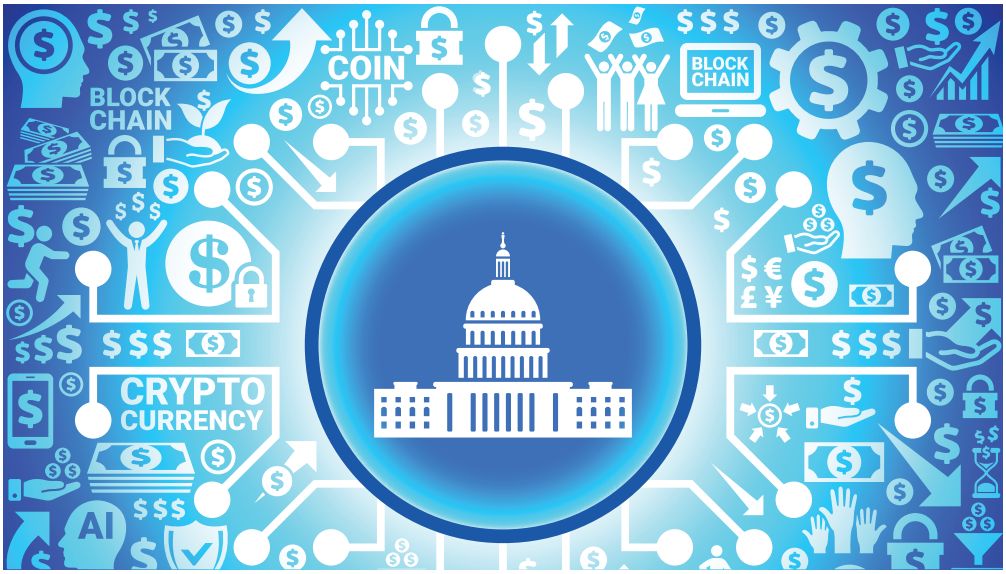

Table of Contents

State and local governments are changing the way they prepare for ransomware attacks on their files. While the focus on preventing attacks continues, forward-thinking IT leaders have accepted that no defense is impenetrable and are adopting a three-prong strategy that includes a robust, reliable, and testable recovery plan. This ebook outlines a best-practice approach for protecting file data against ransomware and highlights the features that IT should look for in a ransomware recovery solution.

Once ransomware finds its way into a system, the malware encrypts data on local hardware and backups, and even spreads to other networked computers and distant locations. Some attacks are **powerful enough to impact dozens** of globally distributed offices within a few hours.

The Expanding Ransomware Threat

According to the U.S. Government's Cybersecurity and Infrastructure Assurance Agency (CISA): "Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. These attacks impact hospitals, school districts, state and local governments, and businesses of all kinds."

- In 2020, at least 2,354 government, healthcare facilities and schools in the United States were affected by ransomware.
- The Washington D.C., Metropolitan Police Department was held up for $4M in ransom for a gang database, and personal data of police personnel and informants.
- An attack on the city of Baltimore, Maryland impacted 10,000 computers and multiple city departments.
- Two counties in Florida paid $1.2M to hackers to restore access to their encrypted data.

The unfortunate truth is that traditional and even state-of-the-art cloud backup **does not guarantee** the kind of recoveries that state and local governments require.

Don't Create a Single Point of Failure

To be ready for a ransomware attack, IT needs a "best-of-breed" strategy to prevent, detect, and recover from an attack. Prevention technology from companies like Cisco, Check Point and Palo Alto provide a perimeter layer to protect the network infrastructure using advanced firewall technologies and Layer 7 application profiling. If ransomware sneaks through the prevention layer, software solutions from companies like McAfee, Norton, and Varonis can also help by trying to detect malicious activity. Unfortunately, ever-evolving ransomware sometimes slips past these layers and by the time an attack is detected, a percentage of files will already have been encrypted. Backups and snapshots provide the last line of defense to recover files and neutralize the attack to minimize data loss and avoid paying a ransom. Deciding on a prevention and detection technology is relatively straight-forward, however thinking about a file recovery solution may not be as easy as it looks.

Ransomware Three-Part Strategy

Network & Endpoint Security | Antivirus & Email Scanning | Backup & Snapshots

This is a partial list of tools available that provide prevention, detection, and recovery of ransomware.

Traditional Backups and Snapshots are Not Good Enough

The FBI stresses the importance of having a robust, reliable, and testable backup process in place to be ready for ransomware. Traditional backups and snapshots fall short of this goal for the following reasons:

The FBI stresses the **importance of having a robust, reliable, and testable backup process** in place.

- **Long Backup Windows:** If you only have the capacity to push backups once a week, or you have a long backup window, there is a risk that the files you recover will be out of date. Instead of recovering recent data, you will only be able to restore older files, and employees will have lost all their intervening work.
- **Timed Strikes:** In some cases, the malware lies dormant for weeks or even months before attacking, rendering traditional backup recovery techniques ineffective.
- **Slow Recoveries:** The more files involved, the slower the recovery period. The latest ransomware variants spread quickly through networked systems, infecting every folder and file they touch. Restoring high volumes of files can take days, even weeks.
- **Distributed Attacks:** Ransomware now has the capacity to infect dozens or even hundreds of locations in just a few hours. Managing the recovery process across multiple sites is a slow and arduous task even with a centralized cloud backup solution.
- **Differing Solutions:** If different state and local offices rely on varying approaches to backup and data protection, the degree of difficulty associated with manually recovering data through these solutions increases exponentially.
- **Lack of Data Protection:** Small state and municipal offices sometimes rely on data protection that is too outdated to be effective. Backup can also be deemed too expensive and difficult to manage, so these smaller offices are left without any data protection all.

In order to find a better file backup solution, you have to move to a modern way of storing files, instead of relying on older Windows File Servers and NAS arrays.

Switch to Cloud File Storage with Built-in File Protection

As ransomware has evolved, so has the cloud. An increasing number of state and local governments are modernizing their file storage and data protection infrastructure by reducing their reliance on local hardware and utilizing the cloud.

A key advantage of moving to a cloud file storage solution - Nasuni, for example - is the ability to rapidly recover files after a ransomware attack that make it through your prevention and detection layers. A robust solution should be able to restore multiple office locations to recovery point objectives (RPOs) as close as a few minutes before the attack. As you evaluate the cloud file storage vendors in the market, consider those that deliver data protection with the following:

Fast Restores: A modern cloud file storage solution can recover millions of files within minutes. Be sure you can test this capability BEFORE needing to do so in the real world.

Flexible RPOs: You should be able to set your RPOs and RTOs according to the needs of your agency or department. Furthermore, recoveries should be scalable, working across department and office locations simultaneously. IT should not have to restore one office at a time, which creates long delays to getting back online.

Testable: A strong ransomware recovery solution must be testable. Your chosen cloud file storage solution should allow you to verify the speed and ease of the restore process at any time to instill confidence.

WORM Storage: The newest ransomware strains can infect online backups, so you should look for a data protection plan that relies on strong encryption and "write once, read many" storage. Best practices are for files to be chunked, encrypted, sent to the cloud securely, and stored as immutable objects.

Multi-office: If a ransomware infection spreads throughout your network, you should be able to restore millions of files in minutes - not hours or days or even weeks - through one management console.

Continuous Protection: A solid cloud file storage solution should be continuous, with no "window" or time lapse where data can be lost. This ensures that recent copies of files will always be available and minimizes loss of productivity.

Automatic: Data protection against ransomware should not require constant oversight or management. Once configured and set, you should be able to rely on it without the need for constant human maintenance.

Surgical Restores: Many snapshot solutions can only recover an entire volume of files, not specific files or directories. That means people will lose work if they were not infected and the volume gets restored from the previous week's snapshot. Look for a solution that has the granularity to restore files, directories, or entire volumes.

Cost-effective: Finally, a cloud file services platform should offer significant cost savings relative to the cost of storing and protecting file data using traditional storage and backup.

Why Ransomware is Difficult to Prevent for State and Local Governments

The FBI details several recommendations for protecting against these attacks and minimizing the likelihood of a ransomware infection. These include strengthening firewalls, updating systems frequently, and teaching employees to avoid suspicious websites and resist clicking on unusual links. Unfortunately, in the case of state and local governments across multiple office locations, these guidelines are difficult to adhere to for several reasons, including:

Number of Users
When there are hundreds or thousands of workers, there is a greater likelihood that one or two of them may click on an unusual link in an email or visit an odd website that secretly has drive-by downloading, in which the malware infects a computer without a click.

Antiquated Technology
State and local government and municipalities are often forced to rely on out-of-date machines and servers that do not have the latest upgrades and patches that might prevent ransomware attacks.

More Sophisticated Attacks
Ransomware itself is constantly evolving and attackers are finding new and creative ways into systems, so even if IT strengthens its defenses against one known variant, there is always a chance that another one will appear with a means of evading those defenses.

The FBI advises those impacted by ransomware to avoid paying a ransom, in part because there is no guarantee that the attackers will provide working keys to decrypt the data. Statistically, there is an 80% chance of being re-attacked if the ransom is paid. However, there are examples of state and local governments that have chosen to pay their attackers, reasoning that the cost of recovering their encrypted files would be far greater than the ransom demand. Baltimore, for example, incurred an estimated $18M in costs attempting to restore its systems. These decisions to pay have had the unfortunate effect of identifying state and municipal governments, along with hospitals, as good targets for ransomware attacks.

The FBI's Cyber Crime division defines ransomware as "an **insidious type of malware** that encrypts, or locks, valuable digital files and demands a ransom to release them."

Conclusion

A solid ransomware strategy for state and local governments should involve a best-of-breed approach to try and prevent and detect malware before it gets into file stores. To be ready for a worst-case scenario, preemptively deploying a modern cloud file storage solution with fast, granular file recovery built in will provide a last-line-of-defense.

NASUNI

ABOUT NASUNI CORPORATION

Nasuni provides modern cloud file storage, powered by the world's only cloud-native global file system. Nasuni is a cloud replacement for traditional network attached storage (NAS) and file server silos, consolidating file data in instantly expandable cloud object storage at a fraction of the cost. Nasuni also eliminates the need for complex legacy backup and disaster recovery infrastructure, dramatically simplifying IT administration. Nasuni is headquartered in Boston, Massachusetts, USA. For more information, visit www.nasuni.com.

NORTH AMERICA HEADQUARTERS
Boston, MA | +1 (857)444.8500

UNITED KINGDOM
London, England | +44 20 3695 7895