White paper

+1.857.444.8500
nasuni.com | sales@nasuni.com

Ransomware Defense for State & Local Governments: How to Recover Faster with Cost-Effective Cloud File Services

NASUNI

State and local governments, small businesses, and large organizations are changing the way they prepare for ransomware attacks. While the focus on preventing attacks continues, forward-thinking organizations have accepted that no defense is impenetrable, and that any solid ransomware strategy must include a robust, reliable, and testable recovery plan. This white paper reviews the standard methods of protecting data against ransomware and highlights the features an organization should look for in a ransomware recovery solution.

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."

The Expanding Reach of Ransomware

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." These attacks impact hospitals, school districts, state and local governments, and businesses of all kinds, from small local operations to global multinational corporations.

- 22 cities in Texas were simultaneously under attack by ransomware at one point in the summer of 2019.
- 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.

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.

Why Ransomware is Difficult to Prevent for State and Local Governments

The FBI details several recommendations for protecting your organization 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 and offices, these guidelines are difficult to adhere to for several reasons, including:

Number of Users

When you have hundreds or thousands of workers, there is a greater likelihood that one or two of them 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 organizations 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 an organization 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 the ransom, in part because there is no guarantee that the attackers will provide working keys to decrypt your data. Some state and local governments have chosen to pay their attackers, however, reasoning that the cost of recovering their maliciously encrypted data 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.

Traditional Backup Recovery is Not Enough

A data protection solution with good Recovery Point Objectives and Recovery Time Objectives allows organizations to restore access to recent versions of data and return to business as usual without having to pay the ransom. In addition to its efforts to educate organizations on ransomware prevention, the FBI stresses the importance of having a robust, reliable, and testable backup process in place.

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

Yet even this approach can be flawed, for the following reasons:

- 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 do recover will be out of date. Instead of recovering recent data, you will only restore older files, and employees will have lost all the intervening work.
- Slow Recoveries: The more files involved, the larger the risk of a slow recovery. The latest ransomware variants spread quickly through networked systems, infecting every folder and file they can touch. Restoring high volumes of files can take days to 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.

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 deserve.

Rapid Ransomware Recovery with Cloud File Services

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

A key advantage of moving to a cloud file services platform is the ability to rapidly restore files after a ransomware attack. Restoration can take place across multiple sites to recovery point objectives as close as minutes before the attack.

As you evaluate the cloud file services offerings on the market, consider platforms that deliver data protection with the following features:

Controllable: Your organization should be able to control or set your RPOs and RTOs according to the needs of your business. Furthermore, recoveries should be scalable, working across many sites simultaneously. Organizations should not have to restore one site or local government office at a time.

Testable: A strong ransomware recovery solution must be testable. Your chosen cloud file services platform should allow you to verify the speed and ease of the restore process, and the viability of cloud versions.

WORM-based: 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 (WORM) storage. Files should be chunked, encrypted, sent to the cloud securely, and stored as immutable objects in a secure cloud volume.

Multi-site: Your chosen cloud file services platform should work effectively at any scale, from a few local offices to hundreds of global locations. If the infection spreads throughout your network, you should be able to restore hundreds of sites, Windows File Servers, and machines simultaneously, working through one management console.

Continuous: A strong cloud file services platform should be continuous, with no "window" or time lapse. This ensures that recent copies of files will always be available and minimizes data loss and/or loss of productivity.

Automatic: Data protection against ransomware should not require constant oversight or management. Files should be continuously versioned to the cloud, and stored securely as WORM objects, without the need for human maintenance.

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.

The threat of ransomware is not diminishing. The rise of ransomware-as-a-service offerings, which allow anyone to utilize the malicious code, suggest that these infections will become more prevalent. Educating your end users and taking steps to protect your systems against infilitration are an essential piece of a good ransomware defense strategy. But as hackers increasingly target public sector organizations, traditional backup is no longer a viable option. Backup is overpriced, difficult to manage, and often ineffective against the latest ransomware strains. Cloud file services offers a stronger, more cost-effective alternative that allows state and local governments to recover faster from ransomware attacks and return to business as usual.

Want to learn more?

800-208-3418
+44 (0)20 7788 8297 (EMEA)
sales@nasuni.com

NASUNI.
One Marina Park Drive
Boston, Massachusetts 02210
United States
www.nasuni.com
SAL-0063 04/20