Ransomware Isn’t Slowing, But Governments Have a Way Out

Baltimore, Albany, Lake City, New Orleans—these are just a handful of cities that have suffered a ransomware attack. Cyber crime attacks are particularly menacing to state and local governments. They must ensure that vital services such as public safety remain available 24×7, while they’re seeing their resources stretched increasingly thin. Governments make ideal attack targets for two reasons:

- Cybercriminals understand that state and local governments must be “always on duty” and would need to resolve a ransom issue quickly
- State and local cyber defenses may not be as robust as Federal agencies and large corporate enterprises.

The Need for Both Offense and Defense

The threat of a ransomware attack necessitates not only a strong defense, but an equally strong offense. We often see organizations focus heavily on protecting entry points to data and ensuring data is backed up frequently. These are important steps. But it is equally important that state and local governments can get back on their feet after an attack, and do so quickly. Backup data is useful only if it is accessible when you need it the most.

Ransomware attacks can put stress on existing data-protection infrastructure built on legacy architectures, such as disk and tape, more than expected. For organizations already struggling to meet recovery service-level agreements, a ransomware attack can exacerbate the situation with additional downtime.

Additionally, backup systems and data can be compromised, requiring reinstallation and reconfiguration of backup solutions before beginning data recovery. Windows and Linux systems are both at risk.

Reducing Threats to the Data Protection Infrastructure

To reduce the threats posed by ransomware to data protection infrastructure, create read-only snapshots of backup data and associated metadata catalogs after performing a full backup. You can recover data directly from these snapshots, mitigating the effects of ransomware.

Pure Storage® offers SafeMode™ snapshots, a built-in feature that provides protection against ransomware and rogue admins because snapshots are protected natively, outside admin control. Ransomware can't delete, modify, or encrypt SafeMode snapshots. They enable rapid recovery via a massively parallel architecture and elastic performance that scales with data to speed backup.

With SafeMode, recovering data following a ransomware attack is a four-step process:

1. Delete compromised data.
2. Reinstall backup software.
3. Point backup software at metadata catalog in SafeMode snapshot.
4. Begin recovery.

With a constantly evolving threat climate, ransomware protection or recovery will never be as easy as 1-2-3. But with daily vigilance and thorough preparation, state and local governments can thwart attacks or significantly mitigate their effects.

Learn more about Pure Storage SafeMode.