A modern approach to **data protection**

Agencies can build a robust, comprehensive strategy for achieving cyber resilience by incorporating data isolation and immutability

Jason Proctor
Dell

Cloud technology opens up enhanced capabilities to protect one of the most important resources that government agencies have: their data. Those capabilities include maintaining archive copies, establishing or further extending best practices for data backup, and creating an isolated and immutable copy of data that is recoverable should there be a cyber incident.

In fact, isolation and immutability are essential techniques that can help agencies protect critical data from ransomware and other sophisticated threats. The overarching goal is to achieve cyber resilience, which is a combination of information security, data protection and cyber recovery.

Information security can be achieved by following guidance such as the National Institute of Standards and Technology's Cybersecurity Framework. In addition, the Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities Catalog helps federal agencies remedy those vulnerabilities as they are identified. Cyber resilience also involves endpoint security, employee education and application security.

Layering in automation and encryption

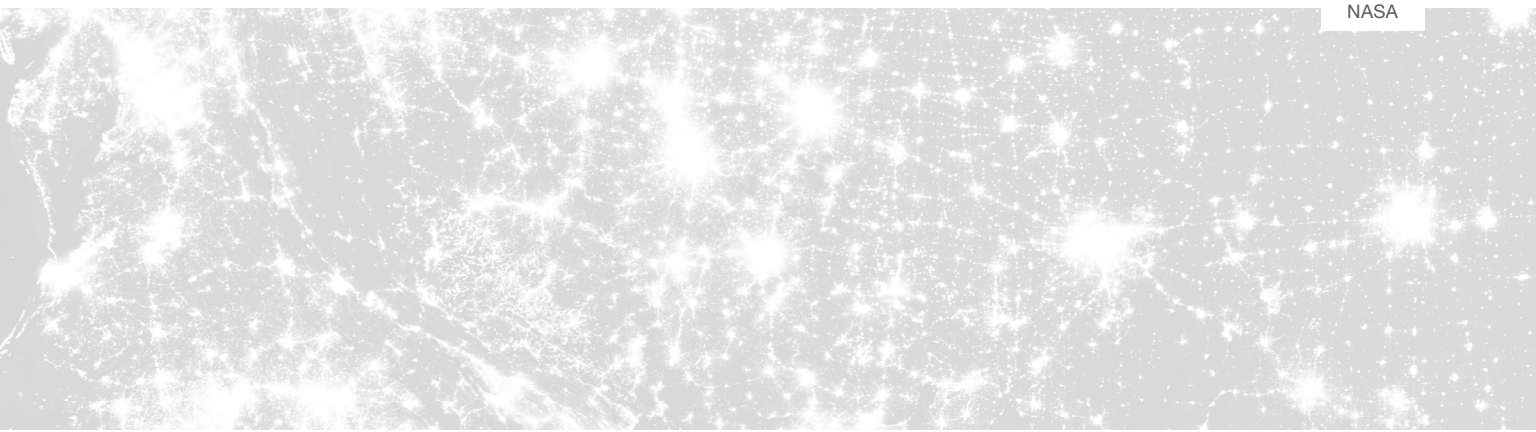
Such guidance exists to help agencies create barriers that will stop most threats before they have a chance to get a foothold in IT environments. If hackers do get in, however, they will almost certainly go after government data. Best practices for data protection include adopting a zero trust architecture to prevent unauthorized access. In addition, Dell offers a "security officer" setting so if a hacker were to access a government system and try to run a destructive command, a system of checks and balances would halt that action before it can be executed.

Furthermore, automation and encryption can boost agencies' ability to protect sensitive data. Automation ensures consistency in how that data is protected by removing the potential for human error. Encryption adds another layer of protection so that even if data falls into the wrong hands, it cannot be readily accessed.

Blocking external and internal threats

The third component of resilience is cyber recovery. In all the guidance on recovering data after a cybersecurity incident, the one big differentiator is isolation — a physical and logical separation of data from the production domain. Isolation gives agencies the ability to recover their data should a cyber incident take place.

In addition, when data is offline, agencies have the ability to run full content analytics against that data to identify any compromises due



NASA

> In all the guidance on recovering data after a cybersecurity incident, **the one big differentiator is isolation** — a physical and logical separation of data from the production domain."

to malware. Rather than being in a reactive state, agencies can move into a proactive state and examine data as it comes in. If a compromise is identified, the system can alert the IT team and provide the forensics to remediate it.

Immutability is another key element of cyber recovery because it prevents data from being changed, altered or deleted for a specified period of time. Because the approach is time-based, agencies also need to protect the source of time so that bad actors can't forward the clock to eliminate the data-retention lock.

Combined with isolation, immutability gives agencies the power to protect the integrity of the environment in which data is stored while protecting the integrity of the data as well. It is an effective approach for preventing external and internal actors from being able to compromise an agency's data-protection environment.

Taken together, all those activities add up to a robust strategy for cyber resilience. ■

Jason Proctor is advisory systems engineer for cyber resilience at Dell Technologies.