PRESIDIO FEDERAL

DELL Technologies
FEDERAL AUTHORIZED PARTNER

New Cybersecurity Realities Call for Comprehensive Data Modernization

Cyber attacks have become more common in the last two years as cyber criminals have taken advantage of the disruptions caused by the pandemic. In 2020 alone, the federal government recorded 30,819 incidents of cyber attacks. As the federal government embarks on its data modernization and cloud migration journeys, does this open the door for more cyber attacks?

In a recent *GovLoop* survey, sponsored by Presidio Federal and Dell Technologies, 47 percent of federal government respondents said that their agencies had experienced a breach in the past twelve months. While it may seem as though expanding the IT supply chain could lead to more cybersecurity vulnerabilities, Clark Anderson, Security Solution Architect at Presidio Federal explained how data modernization is actually a very strong weapon against cyber attacks. “Data modernization and cybersecurity are virtually synonymous with each other,” said Clark.

Prior to the rapid acceleration and adoption of cloud technology, the traditional method of keeping data safe rested in preserving files on backup software. While this was useful for accidental deletions or corruptions of data, backups were never intended to serve as a cybersecurity solution. Backups did little to prevent malware from being deposited into its networks – in fact, attacks on backups have been on the rise over the past few years, as hackers have found vulnerabilities in the networks that store

> *Data modernization and cybersecurity are virtually synonymous with each other.*
> -Clark Anderson, Security Solution Architect at Presidio Federal

Presidio Government Solutions | 12100 Sunset Hills Rd #300A | Reston, VA 20190 | T: 571-789-0390
www.presidiofederal.com

backups and implemented a variety of ways to threaten the security of the data.

"Government agencies often experience a cyber attack without knowing about it for months," said Clark. These circumstances drive what Clark believed to be three key components to a comprehensive data modernization and protection strategy. "It's about 'sync, copy lock, and analyze,'" said Clark.

First, data must be synced to a fully isolated, air-gapped vault. Then, it must be locked away in immutable and unchangeable copies. Third, data should be continually analyzed through machine learning and forensics tools to better identify threats. "Together, these three components make up a solid plan to make sure that data is protected against sophisticated, unforeseen attacks," said Clark.

Clark recommends that agencies pursue enterprise solutions that provide the full "sync, copy lock, and analyze" package. Each of these three components has many layers, and the centralization of these components in one solution set is helpful for agencies that might not have the resources or expertise to adequately execute on cybersecurity measures, including advanced AI-driven monitoring of their infrastructures against unexpected attacks. Cloud providers are also staying ahead of the game in keeping tools in compliance with cybersecurity standards such as NIST's Cybersecurity Framework, while providing the ongoing testing and training that are essential to successful technology implementation.

With many IT decision-makers concerned that their organization's existing data protection may not be adequate for coping with newer threats – it's up to agencies to invest in comprehensive data modernization strategies that keep up with new cyber realities.

"Each agency has the authority and autonomy to decide how they want to manage their own data solutions and cloud migrations," said Clark. "But for these measures to optimize cybersecurity, agencies should look at comprehensive solutions with solid security controls, advanced data protection analysis, and post-attack diagnostics."

To learn more about why federal agencies how data modernization drives cybersecurity, download the "Protecting Data at All Costs" market trends report from Presidio Federal and Dell Technologies here.