PRESIDIO® FEDERAL

IBM Gold Partner

TAKING A 'BYTE' OUT OF DATA THREATS

In the aftermath of a ransomware attack, how long does it take your agency to recover?

iStock | traffic_analyzer

DATA THREATS are on the rise. According to IBM Security's X-Force Threat Intelligence Index 2024, 32% of all incidents "involved data theft and leak." With threat actors increasingly viewing data as a digital gold mine, federal security and storage teams must work together to protect data and recover clean copies if changed, modified, destroyed, erased or encrypted.

"In a lot of cyber resiliency scenarios, security, infrastructure, application and storage teams are working together to try and recover to a secure point in time," said Christopher Vollmar, world wide storage and data resiliency architect for IBM. "Based on work from IBM Research, we are able to use storage to enhance our understanding of what's happening and get a clearer picture into when a data corruption attack is happening which can help us minimize the impact zone."

While storage or data support won't replace security, the benefits of leveraging insights from these teams can enhance the fidelity of information that security teams are getting and increase operational resiliency for an organization.

"Linking storage and security together, in the event of data leakage or a cyberattack, can not only help security teams react at speed but integrating that security tooling with storage to take a last, best, immutable copy can also enhance recovery speeds and minimize my data loss," said Vollmar.

However, tools alone do not lead to true resilience. Policies must define baseline goals and actions. Therefore, before onboarding any new tool, federal leaders should strive to:

IDENTIFY CRITICAL WORKLOADS — What is your minimum viable enterprise? Federal leaders should know what systems are mission-critical and the different applications that support them.

CALCULATE ACCEPTABLE DATA LOSS — How much data would you lose over two hours? Calculate the amount of data lost and the potential impact to the organization. Understanding this can help teams establish a schedule for creating secure, immutable copies stored on primary and secondary storage arrays.

Once agencies answer these fundamental questions, pinpointing workloads and determining acceptable data loss, technologists can deploy cutting-edge solutions like IBM's FlashSystem to:

- **DECREASE** the mean time to identify and respond
- **ENHANCE** threat intelligence using machine learning to analyze individual signals sent from drives
- **INCREASE** data resilience through the creation of Safeguarded, immutable copies across multiple points in time

"We're supporting innovation across the entire value chain," said Vollmar. "If I can identify and make secure, immutable copies of those volumes, and the system can give me enhanced threat detection, then I'm aware if I'm starting to lose those volumes. Safeguarded Copies give me the ability to recover at the speed I need because I can test on an array and use automation to get valid copies back into production faster."

BEYOND SIMPLE STORAGE

While FlashSystem's core capability centers around secure data storage, its' advantages extend far beyond. When combined with automation, security engineers can leverage FlashSystem to build cyber vaults with rigorous two-person integrity checks to confirm data access — insulating systems from common attack vectors such as stolen credentials.

"It's about how do I better protect my environment. How do I not only improve the zero trust frameworks that I'm working toward but also lock down systems so I continue to reduce the ability for threat actors to try to get in?" said Vollmar.

The IBM Storage team also conducts security and resilience assessments, where leaders and employees can ask specific questions regarding their environments. During these sessions, no tooling is installed; rather, the attendee-driven conversation ends with a 10-page report containing technical recommendations, as well as product and vendor-agnostic solutions based on technology stack reviews.

As agencies start tying security and infrastructure together, solutions like IBM Storage can help teams get a deeper, more precise understanding of the steps and activities needed to increase resilience and effectively take a "byte" out of today's cyber threats.

Ensure your agency's data remains secure and resilient in the face of rising threats. Reach out to Presidio Federal and IBM to learn more about how FlashSystem and X-Force can bolster your defense strategy.
https://presidiofederal.com/partners/ibm/

PRESIDIO® FEDERAL

IBM Gold Partner