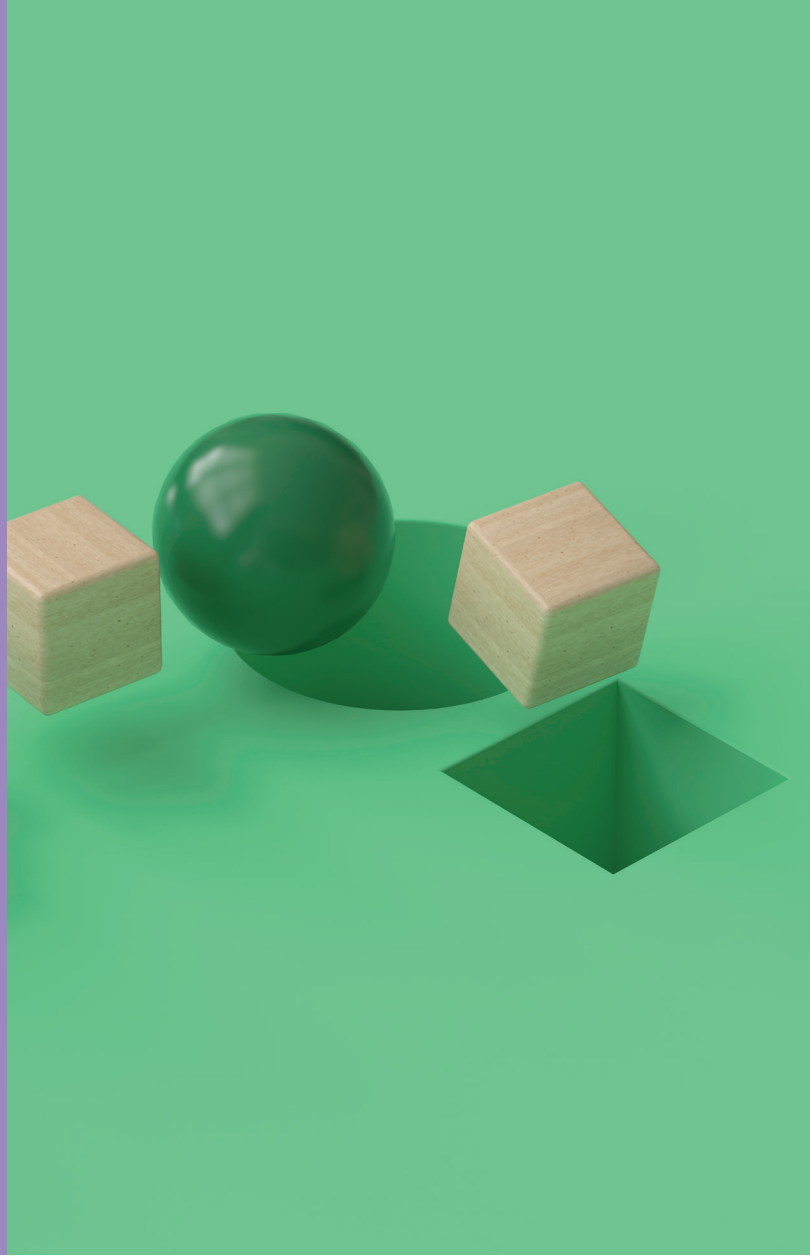
ISSUE BRIEF

Battling Breaches: Agencies Must Focus on Cause, not Symptoms for Data-Centric Security



immixGroup
An Arrow Company

MeriTalk
Improving the Outcomes of Government IT

NetApp

After several high-profile data breaches involving Federal agencies and an overnight acceleration into remote work, Federal IT leadership found themselves quickly rethinking their cybersecurity posture. But, lasting change can't happen instantaneously. It is a journey.

To reach the security level needed to ward off persistent intruders, agencies need to leave legacy technologies behind and implement comprehensive information security and resiliency practices. According to findings from a recent survey polling Federal IT, State, and Local Government leaders, 75 percent said they wished their organization had constructed a more thoughtful data strategy before migrating to hybrid cloud.

In this new reality, agencies are discovering challenges in monitoring and understanding their data – from where it's located to who has access. Pivoting to a data-centric security approach enables Federal agencies to control their data effectively and efficiently.

Hand-in-Hand – Data and Security Management

Phasing out the old "castle-and-moat" security framework, new approaches are gaining momentum. Teams are no longer simply securing the network but are operating under the assumption that no one is to be trusted, and the **data itself must now be secured – whether it's on-prem, in transit, or in the cloud**. In a recent interview on taking a data-centric approach to security, Michael Hommer, Solution Architect, Data Center architectures at NetApp said, "An approach gaining a lot of momentum is Zero Trust, where the concept is to trust no one and verify everything." This shift is even more critical as the number of access points has grown rapidly due to the increase in remote work.

Top Zero-Trust Security Practices

- Know where your data resides
- Classify your data
- Dispose of unnecessary data securely
- Understand who should have access to which data classifications
- Monitor data access and alert when aberrations occur
- Encrypt data at rest and data in flight
- Segment data access and apply the principle of least privilege to enforce access controls
- Use multifactor authentication for administrative and data access

Source

While a data-centric approach to security is efficient and effective, the speed of the shift presents challenges. In the same survey, only 30 percent of respondents said that their organization's hybrid cloud strategy has been able to keep pace with accelerated adoption due to the COVID-19 pandemic. This is largely in part due to the lack of a thoughtfully constructed data strategy before cloud migration, and therefore ineffective management and security of data across environments.

Further, when moving to a new security framework, agencies often encounter insufficient collaboration amongst IT teams. Teams are splintered – with one group focused on security and another on storage and data management, for example. A collaborative partnership is beneficial to ensure a smooth transition where teams understand their roles and implication of activities.

When moving to a data-centric Zero Trust security framework, deploying the right technology and honing in on the right strategy is critical for a seamless and effective transition. “If agencies hone in on what’s most important and focus their efforts on providing maximum protection, they’ll get an even bigger return on their investment than if they use a blanket approach,” Hommer said. To help, agencies can benefit from a trusted partner to facilitate framework adoption and provide the necessary tools and expertise to help agencies IT teams adjust seamlessly.

Asking the Hard Questions – Thoroughly Examining the Protect Surface

For a successful implementation of this new framework, agencies must ask themselves the hard questions about their current data situation. This starts by taking inventory of data – determining where it resides and what classification of protection it has based on its value. Agencies can then dispose of any data that is no longer needed and understand who should have access to the data that remains.

What steps have Federal government leaders taken to manage data in hybrid cloud environments?

48% maintained in-house data storage for sensitive data

43% implemented data redundancy across multiple cloud providers or data centers

41% invested in a robust data management architecture

Source

These steps allow IT teams to implement the right tools and controls for successful security management. From applying the principle of least privilege to access controls to using multifactor authentication or encryption, a good data management practice is key in setting up strong data security and enacting a Zero Trust security framework.

Laying the Foundation

Once agencies have a grasp of their attack surface, what is the next step? They must consider the data security lifecycle – protect, detect, and recover. This is where agencies can leverage the Zero Trust framework. It acknowledges that security controls should be as close to the data as possible; gone are the days of focusing solely on a single network perimeter’s security. **By putting security controls closer to their data, agencies get a bigger return on their investment** leveraging resources better without using additional tactics and controls.

The essence of Zero Trust is to trust no one and verify everything. No user inside or outside an agency network is trusted automatically. Strict identity verification is required, and several strategies and

protections such as multifactor authentication and data segmentation are in place to protect critical data. Taking steps to ensure the storage device is hardened enables protection of valuable and sensitive agency data.

NetApp's Portfolio of Solutions Includes:

- NetApp Snapshot copies and integrations
- Write once, ready many (WORM) storage
- Data replication
- Multifactor authentication
- Encryption
  - Data at rest
    - Software-based
    - Hardware-based
    - Dual layered with software and hardware-based
  - Data in flight
    - Management and control plane
    - Data plane
    - Replication
- Software validation
  - When upgrading
  - At boot
- Audit logging using the FPolicy Zero Trust Engine and the NetApp partner ecosystem for user behavioral analytics
- Secure-purge
- Secure multitenancy (SMT)
- Automated anomaly detection and response policies
- Forensics and user audit reporting

Source

As the Federal workforce continues to work remotely, it's imperative that agencies take steps to dig-in and monitor their data. This becomes even more important as security certifications such as the Cybersecurity Maturity Model Certification (CMMC) are required for agencies. Security is the number one priority when moving to hybrid cloud environments, according to public sector IT professionals – and expanding continuous monitoring capabilities and improving consistency between data-security on-prem and in the cloud is vital to securing agency networks and systems.

Consistently and **effectively monitoring and managing data enables IT teams to spot anomalies and take quick action** to fix the situation in a data breach or ransomware attack. In the past, recovery of data from these events could take up to 15 days. But with the right security controls and monitoring capabilities in place, detection and recovery can be achieved in less than an hour.

Never Trust, Always Verify

Good data management breeds good security management, and adopting a data-centric approach enables Federal agencies to optimize performance and security– thwarting attackers and mitigating threats wherever they emerge. "Think of a well-stocked store," Hommer said, "If the shelves are neatly organized, anything missing or out of place can be identified quickly. The same concept applies to a data-centric approach to security. Agencies must get organized and understand their data."

Partnering with a trusted supplier like NetApp can alleviate the challenges that come with this transition. With their expertise in data storage, protection, and management, IT leaders have the solutions at their fingertips – no matter where they are in their data security journey.