

HOW TO TAKE A DATA-CENTRIC APPROACH TO CYBER RESILIENCE

To build a strong and resilient data center infrastructure, you need to start with data as the foundation. The challenge is that data is being generated at incredible rates, even as ransomware attacks are surging. The key? Transition to a unified data fabric based on modern, flash-based storage systems. This will improve the efficiency and flexibility of your operations, simplify data management to gain greater visibility into your data, and provide more secure stewardship of that data. Here's how that all comes together.

DATA UNDER ATTACK

Although the number of ransomware attacks leveled off a few years ago, they are rising again.

Government remains a high-profile target:

Infrastructure Sectors Affected by Ransomware



73%

Increase in ransomware attacks between 2022 and 2023

230M

Individuals impacted by ransomware attacks on agencies between 2018 and 2022

\$860M

The estimated overall cost of these attacks

The National Institute of Standards and Technology's (NIST) Cybersecurity Framework is built around five pillars:



IDENTIFY

Establish, communicate and monitor risk management strategy, expectations and policy



PROTECT

Understand current risks



DETECT

Use safeguards to manage risks



RESPOND

Find and analyze possible cyberattacks/compromises



RECOVER

Take actions regarding a detected cybersecurity incident

KEY CONSIDERATIONS IN DATA STORAGE

Modernizing data storage is a key step to building a foundation for data resilience. Benefits include:



Lower cost of ownership:

- Reducing rack space real estate and power and cooling requirements
- Optimizing resources through thin provisioning, deduplication, compression and compaction
- Storing "cold," or less-frequently used, data in the cloud



Scalability of capacity, performance:

- Nondisruptive scaling in a cluster without silos or data migration
- Unified support across different media and protocols, on premises or in the cloud
- Support for non-volatile memory express over Fibre Channel and Transmission Control Protocol connectivity



Availability, security and protection of data:

- Data security and ransomware solutions
- Simplified backup and recovery, ensuring apps resume seamlessly
- Business continuity and fast disaster recovery with zero data loss, zero downtime

THE FOUNDATION: FLASH STORAGE

The core of a modern data storage platform is flash storage, but flash storage alone is not enough. Other components and features include:



Nondisruptive operations that include hardware scalability and software upgrades

- Affordable flash for large-capacity, non-mission-critical workloads that don't require sub-millisecond performance
- Dedicated storage for storage-area network-based (SAN) workloads that require high performance, continuous availability and operational efficiency



A **hybrid cloud IT infrastructure** that enables you to simplify and integrate data management across on-premises and cloud environments. Use cases include:

- Storage of cold data
- Data backup solutions
- Disaster recovery



A **unified data management platform** that provides a common set of features across your on-premises and cloud storage systems, eliminating silos and supporting any data, anywhere.

A MODERN RANSOMWARE DEFENSE

Here are some ways a robust flash storage system and data management platform can help you address the NIST Cybersecurity Framework:



Protect

against internal and external threats by knowing what data you have, where it is stored, and has access to it and the level of protection required.



Detect

emerging threats through AI and machine learning, integrated virus-scanning software, autonomous ransomware protection and end-user behavior analysis.



Recover

data rapidly and minimize downtime by having the system automatically create recovery points and block compromised user accounts as soon as anomalous behavior is detected.

THE PATH FORWARD

Ransomware and other threats show no sign of abating. If anything, they are likely to worsen as malicious actors increase the lethality and velocity of their attacks with AI and Machine Learning. Legacy storage and data management platforms are not up to task.

ThunderCat and NetApp provide storage solutions that help agencies achieve the vision of a data-centric approach to cyber resilience. One key offering is NetApp ASA, all-flash SAN arrays for mission-critical workloads. Another is NetApp AFF C-Series, low-cost capacity flash storage for general use. Both are powered by NetApp ONTAP data management software.

Learn how to futureproof your storage environment with the NetApp Storage Lifecycle Program

Learn about NetApp's Ransomware Recovery Guarantee

