Futurum

Quantum

Modern Data Protection for Modern Threats: A Strategic Blueprint for Cyber Resilience

MAY 2025

Introduction

Continuous business operations are a CEO priority, and ensuring cyber resilience is a critical element of this strategy. This focus places pressure on IT managers and security teams to optimize their organizations' data privacy, data security, and overall ability to mitigate against data loss and downtime when a breach occurs. This is no easy feat, as several trends are converging and amplifying the pressure on data protection and recovery strategies.

First is exponential data growth; with the digital transformation of entire industries, for example, retail and mass media, plus the explosion of non-stop video, digital media, and other digital sensor data sources, more data is being created than ever before. At the same time, data retention requirements are also ever-growing; with advanced analytics and machine learning, data is presumed to be valuable, thus being stored for longer periods of time. Moreover, there is the onslaught of cyberattacks. Data is being attacked in more ways than ever before, and these attacks are increasingly difficult to detect.

Simply put, cyberattacks have become inevitable, despite best efforts by organizations and industry bodies. Against this backdrop, it has become critical to evolve to a more proactive and resilient strategy that not only protects the perimeter, but also hardens the entirety of the IT infrastructure—as reflected in Version 2.0 of the NIST Cyber Resilience Framework.

But what exactly is cyber resilience? In Futurum's definition, it is the ability to mitigate the amount of data loss and downtime following a cyber incident. For example, we are seeing backup copies being scanned for viruses, and backup copies being tested and validated for their ability to be recovered. Steps still need to be taken to prevent cyberattacks from occurring, but it is equally important to optimize the ability to withstand and bounce back from attacks as quickly as possible. It has become clear that this need for cyber resilience imposes new demands on backup data copies, evolving the critical criteria that we look for in data protection infrastructure.

Data Protection Evolves to Cyber Resilience

While it is true that modern data protection encompasses far more than just creating backups, the availability of clean backups is the foundational starting point for recovery from cyberattacks. This is where the creation of immutable backups that cannot be tampered with comes in.

Furthermore, the speed of backup jobs matters, as fast backup performance shortens backup windows and enables the ability to create more recovery points, which subsequently helps to minimize the amount of data loss. In other words, fast and frequent backup jobs are needed to meet aggressive recovery point objectives (RPOs), especially for high-value and sensitive data. At the same time, high-performance recovery improves recovery time objectives (RTOs), minimizing the amount of downtime of critical business services.

Performance is also important to increase preparedness for the eventuality of an attack and the need to quickly recover. This requires fast performance that transforms backup copy repositories from a static to an actively accessed resource; for example, the increasing requirements to periodically read backup data sets to scan for malware and to test recovery operations. From this standpoint, tested recovery plans and integration across security event management software and backup software to optimize recovery from incidents are also critical.

Complementing immutable, available backups and high-performance protection and recovery, the ability to support the range of data protection software platforms in use by typical organizations is also important to facilitating recoverability, and as a result, cyber resiliency. At the same time, the option for flexible purchasing models including Capex, Opex, and As-a-Service options supports the ability to quickly adapt to evolving requirements, and to ensure continuous protection of data.

Minimizing the Impact of Data Breaches With All-Flash Recovery

Performance constraints have long been a barrier to effective backup and recovery strategies. Hosting backups on all-flash storage helps to meet demanding performance requirements for backup and recovery jobs as well as for data hygiene requirements.

Advantages of All-Flash Backup Systems:

- **High-Speed Ingest:** Meets tight backup windows for near-continuous recovery points.
- **Fast Recovery:** Enables near-instant recovery of mission-critical systems—even when the infrastructure footprint is large.
- **Proactive Data Engagement:** Transforms backup from static storage into an active dataset for enhanced threat detection and validation.
    - Identify malware with proactive, real-time virus scanning by the backup software.
    - More consistently validate backup data sets and testing of recovery procedures.

All-flash is becoming a necessity for environments that demand rapid and reliable recovery. While all-flash solutions typically have a slightly higher upfront cost than some disk-based alternatives, the investment is quickly offset by lower risk of data loss and reduced business disruption during a breach. Storing only the most recent backup copies to smaller capacity all-flash appliances based on Quad-level cell (QLC) drives also mitigate costs when integrated with disk-based solutions for the long-term retention of backups. With these advantages acknowledged, it is also valuable to employ advanced deduplication and other data reduction techniques across backup workstreams to optimize cost efficiencies by reducing the required storage footprint. Additionally, best practices such as encryption of data at-rest and in-flight still apply.

Rounding Out Cyber Resilience With Offsite and Offline

While fast backup and recovery performance is critical, equally as critical is adopting a multi-faceted data protection strategy that employs multiple backup copies that are distributed and heterogeneous. The "3-2-1" backup rule is a long-held industry best practice, which prescribes for three copies of data (one production and two backups) to be stored on two different types of storage, with one copy stored offsite for protection against local disasters. In the pursuit for cyber resilience, it has also become a best practice for one data copy to be stored offline, so that attackers cannot access it.

Object storage is an ideal option from the standpoint of cyber-resilient retention storage because it can be designed for immutability and versioning, both of which help to prevent malicious tampering. Also important to note is the fact that object storage may be configured to be geo-redundant, which ensures that unaffected, clean copies of the data exist in a separate, geographically isolated location—as a result, limiting the blast radius of the attack. Geo-redundancy also enables replication and failover to another region, which supports business continuity; if the primary site is compromised, operations can resume from the secondary location with minimal disruption.

Tape storage is an ideal medium for the third, air-gapped copy in a cyber-resilient architecture. Stored offline, it is inherently isolated if ransomware, malware, or administrative errors compromise online data sets.

Moreover, tape is engineered for long-term data integrity, durability, and fault tolerance. Cartridges are resistant to bit rot and environmental degradation, as data remains untouched until needed. Advanced error correction codes (ECC) and checksums ensure high reliability, often exceeding that of disk-based storage.

Tape also supports immutable Write Once Read Many (WORM) formats, which protect data from tampering or accidental deletion. In larger deployments, tape libraries offer redundancy and fault tolerance, including multiple drives and robotics to avoid single points of failure, and the ability to store duplicate copies on separate cartridges and even erasure-coded copies that further increase durability.

Finally, tape implementations can overcome the complexity of data rebalancing or frequent migrations common in disk environments used for long-term retention. This simplicity helps reduce operational overhead and the risk of human error over the long term, making tape a strong asset for secure, durable data retention.

Futurum notes that object and tape storage may be used in conjunction with each other, with the object store serving as an intelligent front end and cold data being tiered to tape on a policy-driven basis. This supports the ability to balance performance and cost requirements.

Overview of Quantum Portfolio

Quantum offers a comprehensive suite of immutable and encrypted data protection technologies designed to work cohesively in support of modern cyber resilience requirements:

- DXi Data Protection Appliances: High-performance, deduplication-optimized systems for fast ingest and restore operations.
- ActiveScale Object Storage: Scalable, multi-tiered storage platform configurable to include flash, disk, and tape resources, amenable to fast local recovery, offsite secondary copies, and long-term retention solutions.
- Scalar Tape Libraries: Enterprise-class tape solutions offering air-gapped protection and lowest cost long-term archiving.
- Deployment models and consumption models are flexible, spanning traditional infrastructure and managed and hosted services, supporting a range of organizational needs and budgets.

Conclusion

The pressing reality of cyberattacks necessitates a shift in mindset and infrastructure: from reactive data protection to proactive recovery readiness.

An ideal strategy for cyber resilience includes:

- High-performance all-flash systems for fast local backup and recovery
- A layered retention strategy leveraging hard disk and tape mediums
- Continuous scanning, validation, and testing
- Flexible consumption models to adapt to changing threats and requirements.

Organizations that invest in a unified, performance-optimized, and security-conscious data protection architecture will be best positioned to minimize the impact of cyber threats and ensure long-term operational continuity.

Quantum's portfolio aligns well with the emerging resilience-oriented architecture. The seamless integration of flash, disk, and tape—combined with data security features—positions it as a robust platform for hybrid and multi-cloud IT environments.

Important Information About This Report

AUTHORS

Krista Case
Research Director, Cybersecurity | The Futurum Group

PUBLISHER

Daniel Newman
CEO | The Futurum Group

INQUIRIES

Contact us if you would like to discuss this report and The Futurum Group will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts, but must be cited in context, displaying author's name, author's title, and "The Futurum Group." Non-press and non-analysts must receive prior written permission by The Futurum Group for any citations.

LICENSING

DISCLOSURES

The Futurum Group provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

Quantum

ABOUT QUANTUM

Quantum delivers comprehensive data lifecycle management solutions built for the demands of the AI era. With over four decades of experience, we help organizations harness the power of unstructured data, supporting high-speed ingest, secure backup and protection, and low-cost, scalable archives. From life sciences and government to media, financial services, and manufacturing, the world's leading innovators trust Quantum to keep their data protected, accessible, and ready to deliver value. For more information, visit www.quantum.com

Futurum

ABOUT THE FUTURUM GROUP

The Futurum Group is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.