NetApp

NetApp Sets New Standard for Cybersecurity at the Storage Layer

2025-04-29

SAN JOSE, Calif. – April 29, 2025 – NetApp® (NASDAQ: NTAP), the intelligent data infrastructure company, today announced new data security capabilities that help customers strengthen their cyber resiliency. Security teams can now leverage NetApp, the most secure storage on the planet, to take a proactive approach to data security at the storage layer and strengthen their overall security posture.

Advancements in technology drive a cycle of innovation for cyber threats and cybersecurity countermeasures alike. The increasing accessibility of AI has enabled malicious actors to automate cyberattacks, requiring businesses to use machine learning to automate threat detection. And as quantum computing approaches viability, businesses urgently need to protect their data from malicious hackers who may look to steal and store sensitive information today, holding it for the promise of easily accessible quantum-powered decryption in the near future.

NetApp is a pioneer of comprehensive, secure-by-design intelligent data infrastructure, giving customers confidence in their ability to protect and access data without disruption backed by **a guarantee of 99.9999 percent availability**. Building on that track record, NetApp is announcing new cyber resiliency capabilities that augment and elevate in-depth security strategies for customers.

"Security teams need to factor storage into their security strategies because it is the last line of defense for their data and the right storage can play an active role in protecting the enterprise," said Gagan Gulati, Senior Vice President and General Manager, Data Services at NetApp. "Backup and recovery is an important part of security at the storage layer, but NetApp's comprehensive security capabilities expand the role of primary storage with built in automated ransomware detection and response that enable customers to take a proactive approach to keep their data secure. With built-in security capabilities that secure our customers' data on any workload, anywhere, NetApp has made storage as critical to a sound cybersecurity strategy as perimeter and endpoint security tools."

To help customers enhance their cyber resiliency at the storage layer, NetApp is releasing new data security capabilities including:

- **Post-Quantum Cryptography**: NetApp has embedded post-quantum cryptography into its storage portfolio for file and block workloads. NetApp's secure-by-design storage keeps its customers' data protected

against quantum threats, fostering confidence among customers, partners, and regulators. By leveraging encryption algorithms standardized by NIST—a globally recognized standards body and authority—businesses can rely on a defense that is thoroughly tested and capable of carrying them into the future with quantum-ready storage.

- **NetApp BlueXP Ransomware Protection Update**: Updates to BlueXP ransomware protection strengthen the service's ability to provide a comprehensive, orchestrated ransomware defense for NetApp ONTAP® workloads. The new features include ransomware-specific role-based access controls, which empower security teams with granular permissions tailored to combat ransomware threats effectively, and support for ransomware protection for native cloud workloads. These advancements provide enterprises with enhanced control and protection against ransomware, safeguarding critical data and maintaining operational resilience in an increasingly complex threat landscape.
- **NetApp BlueXP Backup and Recovery Workload Support**: NetApp BlueXP backup and recovery provides a simple, secure, and cost-effective integrated data protection service for ONTAP data. With these new updates, customers will benefit from a redesigned user interface that makes it easier to integrate and define a 3-2-1 data protection strategy for their workloads, including Microsoft SQL Server, VMware, and Kubernetes applications.
- **NetApp Security Professional Services**: NetApp is offering expanded professional security assessment and security hardening services to help customers evaluate and further tighten their security posture by enabling the built-in security capabilities in NetApp that help keep their data secure.

"Building resiliency against cyber-attacks into the data storage infrastructure has never been more important. Approximately 80 percent of respondents in our Cybersecurity Decision Maker IQ research indicated having experienced a significant security incident over the past 12 months, and 40 percent counted data loss and compromise as one of the most significant consequences of their organization's worst security incident," said Krista Case, Research Director for The Futurum Group. "NetApp is building critical cyber-resiliency capabilities into its data storage infrastructure and services, including granular role-based access controls to help thwart the onslaught of malicious access attempts, and quantum-safe data encryption capabilities."

These updates build on NetApp's comprehensive security capabilities that include security built-in, ransomware protection, backup, disaster recovery, data classification—all delivered via BlueXP ransomware protection. This SaaS-based control plane also includes features like SIEM integration to further enable connections between storage and overall security postures. Built-in security features like **NetApp ONTAP Autonomous Ransomware Protection with AI (ARP/AI)** protect customers from data loss and downtime by proactively detecting ransomware at the storage layer across the hybrid cloud, including **ARP for native cloud**. Later this year, NetApp will expand the cyber resiliency protection of ARP/AI to include block storage workloads.

To learn more about the updates to NetApp cyber resiliency capabilities, visit the NetApp booth #259 at the RSA Conference 2025, April 28-May 1 at the Moscone Center in San Francisco.

Statements by NetApp about unreleased offerings and future plans are for informational purposes only, are subject to change without notice, and should not be relied upon for purchasing or other decisions. Such statements do not constitute a commitment, obligation, guarantee, or warranty of any kind by NetApp, including about availability, functionality, pricing, or timing.

No ransomware detection or prevention system can completely guarantee safety from a ransomware attack.

Although it's possible that an attack might go undetected, NetApp technology acts as an important additional layer of defense.

Additional Resources

- **Beyond the Breach: Storage Turns Cyber Defense into Resilience**
- **The Post-Quantum Cryptography Countdown: Why your Data's Safety Net is Fraying**
- **Post-Quantum Cryptography: The Most Secure Storage on the Planet is Ready for the Quantum World**
- **BlueXP Ransomware Protection: Outsmart Ransomware**
- **BlueXP Backup and Recovery: Full Spectrum 3-2-1 Backup for ONTAP**
- **Data Security Services: Securing Your Data is Our Top Priority**

About NetApp

NetApp is the intelligent data infrastructure company, combining unified data storage, integrated data, operational and workload services to turn a world of disruption into opportunity for every customer. NetApp creates silo-free infrastructure, harnessing observability and AI to enable the industry's best data management. As the only enterprise-grade storage service natively embedded in the world's biggest clouds, our data storage delivers seamless flexibility. In addition, our data services create a data advantage through superior cyber resilience, governance, and application agility. Our operational and workload services provide continuous optimization of performance and efficiency for infrastructure and workloads through observability and AI. No matter the data type, workload, or environment, with NetApp you can transform your data infrastructure to realize your business possibilities. Learn more at **www.netapp.com** or follow us on **X**, **LinkedIn**, **Facebook**, and **Instagram**.

NETAPP, the NETAPP logo, and the marks listed at **www.netapp.com/TM** are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.