



NEWS RELEASE

# NetApp Fights Ransomware in Real-Time with Built-In Artificial Intelligence on Enterprise Storage and Enhanced Cyber-Resiliency Solutions

2024-03-05

**SAN JOSE, Calif. – March 5, 2024** – NetApp® (NASDAQ: NTAP), the intelligent data infrastructure company, today announced cyber-resiliency capabilities that will equip customers to better protect and recover their data in the face of ransomware threats. NetApp is one of the first to integrate artificial intelligence (AI) and machine learning (ML) directly into enterprise primary storage to fight ransomware in real-time. The NetApp cyber-resiliency capabilities protect both primary and secondary data for organizations whether it is stored on-premises or in the cloud.

Cybercriminals are increasingly aiming ransomware attacks at critical infrastructure and supply chains where operational disruptions can cost millions of dollars, according to [Forrester](#). As a result, 87 percent of C-suite and board-level executives ranked ransomware as a high, or the top, priority for their organization, according to the [NetApp 2023 Data Complexity report](#). When cybercriminals breach perimeters, networks, and identities storage becomes the last line of defense for organizations' most critical data. With the threat of ransomware looming, organizations need solutions that not only protect their data but also quickly recover lost data and return to normal operations. NetApp is updating its cyber-resiliency solutions and leveraging the power of AI to give customers confidence that their data will be safe and accessible when they need it.

"NetApp is taking an aggressive and proactive approach to protecting our customers' data against cyber threats using artificial intelligence. We are the first storage vendor to explicitly and financially guarantee our data storage offerings against ransomware," said Mignona Cote, CSO at NetApp. "Today, we are furthering that leadership with updates that make defending data comprehensive, continuous, and simple for our customers."

NetApp is focused on designing data storage and management systems that maximize data protection and security while meeting data governance and compliance standards, with new updates that include:

- **ONTAP Autonomous Ransomware Protection with Artificial Intelligence (ARP/AI)** will spearhead the next generation of real-time enterprise storage ransomware protection, giving increased accuracy and performance required to detect and mitigate new, more sophisticated cyber threats. NetApp pioneered autonomous real-time detection of ransomware directly in primary enterprise storage three years ago. Now, NetApp will be leading the charge to use adaptive AI/ML models built directly into enterprise primary

storage to look at file-level signals in real-time to detect even the newest ransomware attacks with planned 99%+ precision and recall. NetApp will be offering the first technology preview of ARP/AI within the next quarter.

- **NetApp BlueXP Ransomware Protection**, now in public preview, provides a single control plane to intelligently coordinate and execute an end-to-end, workload-centric ransomware defense. Customers can now identify and protect critical workload data with a single click, accurately and automatically detect and respond to a potential attack, and recover workloads within minutes, safeguarding their valuable data and minimizing costly disruption.
- **Application-Aware Ransomware Protection via NetApp SnapCenter 5.0** offers immutable ransomware protection for applications. SnapCenter will now apply NetApp's leading ransomware protection technologies, previously used with unstructured data, to application-consistent backup. SnapCenter 5.0 includes support for key ONTAP features like tamperproof Snapshot copy locking, SnapLock protected volumes, and SnapMirror Business Continuity to enable more robust data protection for applications and virtual machines. SnapCenter 5.0 supports protection of applications on-premises with NetApp AFF, ASA, and FAS, as well as in the cloud.
- **NetApp BlueXP Disaster Recovery**, now generally available, offers seamless integration with VMware infrastructure and provides storage options for both on-premises and major public cloud environments. This comprehensive solution eliminates the need for separate standby disaster recovery (DR) infrastructure, reducing costs. With NetApp BlueXP disaster recovery, failover and failback processes are simplified, allowing smooth transitions from on-premises VMware infrastructure to the public cloud or to an on-premises data center.
- **NetApp Keystone Ransomware Recovery Guarantee** extends NetApp's current Ransomware Recovery Guarantee to our leading storage-as-a-service offering, NetApp Keystone. With this guarantee, NetApp will warrant snapshot data recovery in the event of a ransomware attack. If snapshot data copies can't be recovered through NetApp, we will offer compensation\*.

"Today's cybersecurity teams face the monumental task of protecting their companies' data from ever-evolving threats, especially ransomware," said Archana Venkatraman, Research Director, Cloud Data Management, IDC. "NetApp's approach of delivering a secure, unified storage infrastructure makes storage foundational for ransomware protection and reduces the burden on cybersecurity teams. Companies looking to fortify their cyber resiliency and shifting protection left will increasingly look to vendors that take a secure-by-design approach and develop unified storage and data services."

"Using NetApp in our Advanced Technology Center, we significantly simplified our replication process for VMware virtual machines and their underlying datastores to meet or exceed recovery benchmarks," said Derek Elbert, Solutions Architect at WWT. "With NetApp's solutions, we successfully established the recovery policies for cloud volumes workloads or virtual machines with no existing DR strategy, managing everything through NetApp BlueXP. This transforms how we operate disaster recovery for VMware."

"To store sensitive genomics and health data, we have to use the right technology with layers of security built in," said Mark Cowley, Deputy Director at Children's Cancer Institute. "With NetApp, we can be very confident that we are sharing the right data only to authorized researchers. The last line of defense is your weakest web-based system, so we've implemented role-based access and added resilience to all of our tools."

The latest cyber resiliency updates from NetApp empower organizations to proactively address cybersecurity

threats in complex hybrid and multicloud environments, leveraging AI to identify threats and prevent disruptions to their operations.

To learn more about the NetApp cyber-resiliency offerings visit: [www.netapp.com/cyber-resilience/](https://www.netapp.com/cyber-resilience/)

\*Specific terms and conditions will apply. Customers must apply for coverage by the guarantee.

#### **Additional Resources**

- [The Most Secure Storage on the Planet Gets Even Better](#)
- [Unveiling NetApp SnapCenter 5.0](#)

#### **About NetApp**

NetApp is the intelligent data infrastructure company, combining unified data storage, integrated data services, and CloudOps solutions 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 CloudOps solutions provide continuous optimization of performance and efficiency 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](https://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](https://www.netapp.com/TM) are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.