



NEWS RELEASE

# NetApp First to Embed Data Breach Detection into Enterprise Data Storage

2025-10-14

New capabilities reinforce NetApp as the most secure storage on the planet

SAN JOSE, Calif.--(BUSINESS WIRE)-- NetApp® (NASDAQ: NTAP), the Intelligent Data Infrastructure company, today announced new industry-leading cyber resilience capabilities that further strengthen the most secure storage on the planet. The newly enhanced and renamed NetApp Ransomware Resilience service enables customers to make their data infrastructure a leading part of their comprehensive security strategy with integrated AI-powered ransomware detection and two new capabilities: a first-in-the-industry ability for enterprise storage to detect data breaches; and isolated recovery environments to enable safe and clean recovery of mission-critical data.

As enterprises face their most pressing challenges—AI innovation, data modernization, cyber resilience, and cloud transformation—they need a secure, reliable, and efficient data infrastructure. While investments in AI are creating unprecedented opportunity for enterprises, they are also expanding their attack surfaces. NetApp makes data infrastructure a critical part of enterprise security strategy, leveraging AI to protect enterprise data and eliminate operational disruption.

"To effectively protect your data from a cyberattack, you need to know it happened as early as possible to take action," said Gagan Gulati, Senior Vice President and General Manager, Data Services at NetApp. "With new AI-powered capabilities to detect early indicators of data exfiltration attempts on top of our existing leading capabilities to detect ransomware attacks on both structured and unstructured data, we're making enterprise data even safer. Storage is the last line of defense to protect our customers' most valuable asset—data—and we are constantly innovating on top of the most secure storage on the planet."

Key cyber-resilience updates from NetApp include:

- **NetApp Ransomware Resilience:** Formerly called the NetApp Ransomware Protection service, NetApp Ransomware Resilience makes protecting and recovering ONTAP workloads from ransomware attacks easier, faster, and more effective without requiring deep security expertise or training. The newly enhanced Ransomware Resilience service helps drive comprehensive, orchestrated, workload-centric ransomware defense across file and block storage all via a single control plane.
- **Data Breach Detection:** NetApp Ransomware Resilience now includes data breach detection, an AI-driven

capability that identifies anomalous user and file system behaviors that are early indicators of potential data exfiltration and thus a breach attempt. Upon identification, Ransomware Resilience automatically alerts the customer via their security information and event management (SIEM) solution, arming them with forensics to enable decisive and swift action. By proactively identifying breaches, NetApp customers can block further unauthorized transfer of sensitive data, stopping cyber threats before they can cause extensive unauthorized data exposure.

- **Isolated Recovery Environments:** NetApp Ransomware Resilience is also introducing isolated recovery environments to ensure safe and malware-free workload recovery. An isolated recovery environment utilizes deep and proprietary AI-powered scanning to precisely identify maliciously impacted data and the point at which it was modified. Ransomware Resilience then guides the customer through the workload restoration process for a fast and easy malware-free recovery of the most recent safe data, preventing reinfection.

These enhancements extend NetApp's existing leadership in cyber resilience, complementing existing capabilities such as AI-powered detection built directly into ONTAP. The award-winning NetApp ONTAP Autonomous Ransomware Protection with Artificial Intelligence (ARP/AI)—which now fully supports data stored in both file and block protocols—has demonstrated 99 percent detection of tested, advanced full-file encryption ransomware attacks with zero false positives in external testing and validation, indicating a strong ability to operate in a business context without contributing to alert fatigue.

"NetApp embraces a secure-by-design approach that positions its storage solutions not just as a last line of defense against cyber threats, but also as an early line of defense," said Philip Bues, Sr. Research Manager, Cloud Security and Confidential Computing at IDC. "As malicious actors continue to evolve, adding techniques such as double extortion to their ransomware attack patterns, today's announcements show that NetApp is keeping pace to back up its claim as one of the industry's most secure storage platforms. The new data breach detection capability gives enterprises a critical advance warning enabling them to stop and respond to cyber threats before they impact the business. It demonstrates that NetApp is more than a storage company, it is an invested, trusted partner that is addressing the most pressing priorities of its customers."

Today, NetApp announced other updates across its portfolio including **enhanced AI capabilities** which deliver on the company's AI vision by unifying high-performance storage and intelligent data services into a secure and scalable offering.

To learn about these updates and others across the NetApp portfolio, visit: <https://www.netapp.com/product-updates>

At NetApp INSIGHT 2025 in Las Vegas, October 14–16, NetApp will present sessions and demos, showcasing how it is driving transformation across industries. Tune in to the keynote sessions at: <https://www.netapp.com/insight/>

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, and our research indicates NetApp technology has resulted in a high degree of detection for certain file encryption-based ransomware attacks.

## Additional Resources

- [Cyber Resilience: The Most Secure Storage on the Planet](#)
- [Why Your Storage is Your Last—and First—Line of Defense](#)

## About NetApp

For more than three decades, NetApp has helped the world's leading organizations navigate change – from the rise of enterprise storage to the intelligent era defined by data and AI. Today, NetApp is the Intelligent Data Infrastructure company, helping customers turn data into a catalyst for innovation, resilience, and growth.

At the heart of that infrastructure is the NetApp data platform – the unified, enterprise-grade, intelligent foundation that connects, protects, and activates data across every cloud, workload, and environment. Built on the proven power of NetApp ONTAP, our leading data management software and OS, and enhanced by automation through the AI Data Engine and AFX, it delivers observability, resilience, and intelligence at scale.

Disaggregated by design, the NetApp data platform separates storage, services, and control so enterprises can modernize faster, scale efficiently, and innovate without lock-in. As the only enterprise storage platform natively embedded in the world's largest clouds, it gives organizations the freedom to run any workload anywhere with consistent performance, governance, and protection.

With NetApp, data is always ready – ready to defend against threats, ready to power AI, and ready to drive the next breakthrough. That's why the world's most forward-thinking enterprises trust NetApp to turn intelligence into advantage.

Learn more at [www.netapp.com](http://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](http://www.netapp.com/TM) are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

### Media Contact:

Kenya Hayes  
NetApp  
[kenya.hayes@netapp.com](mailto:kenya.hayes@netapp.com)

### Investor Contact:

Kris Newton  
NetApp  
[kris.newton@netapp.com](mailto:kris.newton@netapp.com)

Source: NetApp