Novel Threat Detection and Response Report: Presenting 20 Novel Use Cases

Market Presentation

Chris Kissel

Research Vice President
Security and Trust

December 2025

This IDC excerpt features: NetApp

About this Excerpt

The content for this excerpt was taken directly from "**Novel Threat Detection and Response Report: Presenting 20 Novel Use Cases**" (11/12/2025, Doc #US53936425).

Abstract

This IDC Market Presentation highlights the key findings from IDC's study on novel threat detection and response — technologies that take a genuinely different approach to identifying or disrupting threats, representing risk, or responding to adversarial behavior beyond what conventional tools deliver. The goal was not to build an exhaustive market map or rank the "best" solutions but to surface real examples of new thinking that can help security teams stay ahead of an adversary that is accelerating its tactics with AI-driven tools.

To keep the study grounded, vendors needed to demonstrate concrete use cases and a clear connection between their novelty and improvements in detection or response. The scoring model — novelty, uniqueness, and potential impact — was intentionally simple. It provides enough structure to identify standout approaches without overcomplicating an area that is evolving quickly.

© 2025 IDC

Distribution is forbidden without written consent of IDC. All rights reserved.

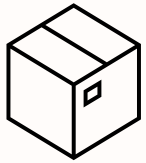
Representative Vendors

This is a representative sample of vendors included in the study's use cases and is not a comprehensive market list

© 2025 IDC

Distribution is forbidden without written consent of IDC. All rights reserved.

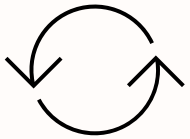
Technology and Vendor Profile: NetApp Ransomware Resilience



Storage

Detection

Response



Recovery

Technology Definition

- NetApp would be known by many as a storage vendor. However, NetApp Ransomware Resilience includes detection and response (NetApp INSIGHT), enterprise data collection, and an Isolated Recovery Environment which also includes an up to $5 million guarantee that files/data will be restored without malware if there is an attack.
- Ransomware detection is particularly interesting. While there are multiple ways to find ransomware IOC, understand that what triggers an attack is that it begins with staging data for encryption and then the encrypted data. Network storage accepts data in 4KB blocks. The storage layer occurs in real-time in what is essentially a digital twin. NetApp has both write-on and read-on file capabilities.
- Regarding detections, NetApp has three unique advantages. First, NetApp constantly monitors the data meaning is if there is any alteration to the file, NetApp will catch it. Ransomware has a kill-chain, and at the point of an IOC, NetApp produces a high-fidelity alert. Secondly, NetApp INSIGHT can use file entropy (byte sequence) and monitoring of file extensions/headers to find IOC. Lastly, for all intents and purposes, encrypting packets is a positive, zero-trust best practice, but NetApp good lists and bad lists encryption protocols.
- Businesses are vulnerable to double–extortion. The adversary not only gets a foothold into the network to begin with, but the attacker also either captures the backup files and/or disaster recovery restoration and may encrypt those as well. NetApp provides a $5 million guarantee that the files can be restored without malware attached.

Source: https://www.netapp.com/cyber-resilience/ransomware-protection/

© 2025 IDC Distribution is forbidden without written consent of IDC. All rights reserved.

Use Cases: NetApp Ransomware Resilience

High fidelity alerts

- Thinking about it logically, the data layer is the best detection layer. Perhaps the most relevant metric NetApp adheres to is self-imposed. Working with SE Labs, NetApp validated they would find new malware in 99% of simulations (including zero-day attacks). Additionally, SE Labs validated that 99% of the alerts initiated from INSIGHT were true positive alerts.

Safe recovery after a ransomware attack

- NetApp can isolate suspected data in place, detect any maliciously encrypted data and hunt for the malware to remove it before recovering the latest un-encrypted copies of every file. As mentioned earlier, NetApp provides a $5 million guarantee that it will restore a client's last known good version of its data malware-free.

Ease of use

- Several things are attractive about NetApp INSIGHT. Because it is looking for anomalies in data and data-related sessions, there is value out of the box—UBA can play a part later. INSIGHT is SaaS deployed and resides in the storage OS introducing no new latencies. Security analysts do not need additional training. Lastly, there is no need for dedicated computing resources and businesses of all sizes can benefit.

SOC friendly

- NetApp enables storage admin and security engineers to perform end-to-end drills and generates reports to demonstrate readiness. It goes back to alert fidelity, NetApp INSIGHT provides precise and actionable alerts for action in tools like SIEM, SOAR, antivirus, firewalls and detection and response platforms.

© 2025 IDC Distribution is forbidden without written consent of IDC. All rights reserved.

Key Takeaways: NetApp Ransomware Resilience

Using the storage layer to detect ransomware makes sense in that the storage layer sees packets as they come and data alteration or entropy are nearly indisputable IOC.

5

Novelty

- At the heart of this is the monitoring of data in real-time. The adversary cannot enact ransomware without altering data in stages.
- UBA detections rely on the meta-conditions outside of the encrypted packet. NetApp sees the data within the packet AND can apply UBA for additional fidelity.
- Ransomware Resilience uses NetApp's existing storage OS which cannot be bypassed by the adversary.
- The NetApp isolated recovery environment occurs in real-time and provides local restoration faster than disaster recovery systems.

5

Uniqueness in Market

- The combination of data visibility and network procedure protocols is accurate and provides redundancy.
- Storage occurs in real-time—INSIGHT provides real-time autonomous detections in any environment even mobile and OT.
- As a SaaS deployment, the data never leaves the customer's environment. The technology only requires a small virtual machine to implement.
- Enhanced triage includes: the actor; the exact file and number of files infected; where the threat actor went; and what happened in what time sequence.

5

Potential Impact

- NetApp Ransomware Resilience stops encryption attacks before they cause significant damage and reduces the risk of data loss.
- These actions require no human intervention—both the detections and the response can be autonomous.
- NetApp provides guided clean data recovery without the risk of re-infection.
- The snapshots are immutable.

© 2025 IDC Distribution is forbidden without written consent of IDC. All rights reserved.

NTD&R Spectrum Wrap Up

Company	Technology	Novelty	Uniqueness in Market	Potential Impact
Gigamon	Precryption	5	5	5
Flare	Account Take Over Detection & Response	5	5	5
NetApp	Ransomware Resilience	5	5	5
ExtraHop	Lateral Movement	5	5	5
Contrast Security	Application Detection & Response	5	4	5
Cisco	XDR Incident Scoring & Prioritization	5	4	5
Cisco	XDR Cloud Detections	5	4	4
Imperum	Autonomous SecOps & Investigation	5	4	5
Sophos	Adaptive Attack Protection (AAP)	5	4	5
Sophos	CryptoGuard	5	4	5
Darktrace	Autonomous Response	5	4	5
Infoblox	Threat Defense	5	4	5
Lumen	IP Backbone Detection & Response	5	4	5
Permiso	Identity Risk Prioritization	4	4	5
Recorded Future	Intelligence Platform	4	4	5
GreyNoise	Intelligence Detection & Response	5	4	4
Corelight	Flow Monitoring Sensor	5	4	4
NETSCOUT	Arbor Adaptive DDoS for Threat Detection	5	4	4
iCOUNTER	Personalized Threat Intelligence	4	4	5
OpenText	Core Threat Detection & Response	4	4	4

© 2025 IDC Distribution is forbidden without written consent of IDC. All rights reserved.