



NEWS RELEASE

New Research from NetApp Finds One in Five Companies Unable to Recover Data After Cyberattack

2024-12-04

SAN JOSE, Calif. – December 4, 2024 – NetApp® (NASDAQ: NTAP), the intelligent data infrastructure company, today announced the release of its latest report analyzing the state of cybersecurity and offering actionable insights to help organizations strengthen their cyber resiliency. The Futurum Group study, "**Cloud, Complexity, AI: The Triple Threat Demanding New Cyber Resilience Strategies**" sponsored by NetApp, provides a comprehensive analysis of evolving cyber threats and resiliency strategies.

The study, which surveyed over 1,300 cybersecurity leaders across industries worldwide, reveals that 54 percent of organizations experienced a cyberattack in the past 12 to 18 months, with one in five unable to recover lost data. The report highlights the urgent need for enterprises to leverage intelligent data infrastructure to address growing risks posed by sophisticated threats, operational complexity, and the challenges of hybrid multi-cloud environments.

"The findings clearly highlight the urgency for organizations to rethink their cybersecurity strategies in an era of escalating threats," said Gagan Gulati, General Manager for Data Services at NetApp. "To reduce risks and ensure faster recovery, businesses must adopt an intelligent data strategy that prioritizes secure-by-design infrastructures, embedding security at the core of their data management approach. With data as a company's most valuable asset, resilient storage solutions—such as those offered by NetApp—serve as the last line of defense in a comprehensive security strategy, safeguarding critical information and enabling long-term success in hybrid multi-cloud environments."

Key Findings:

- **Cloud Security Risks:** Misconfigurations and vulnerabilities in hybrid multi-cloud environments are now among the top threats, outpacing traditional attacks like ransomware. As organizations rely increasingly on hybrid cloud infrastructures, addressing these vulnerabilities is critical to maintaining data security and operational continuity.
- **Tool Sprawl Challenges:** Seventy percent of respondents use more than 40 cybersecurity tools, with 84 percent citing operational complexity as a major inhibitor to cyber resiliency. This complexity creates



protection gaps and inefficiencies, underscoring the need for tool consolidation and integrated solutions to streamline operations.

- **AI in Cybersecurity:** Forty percent of organizations are leveraging AI for threat detection, with plans to expand its use for automating response and recovery. AI's ability to identify and mitigate threats at scale is powerful, but balancing its use with managing false positives and ensuring robust human oversight is essential to its success.
- **Data Classification is Key:** Organizations with strong data classification frameworks recover from attacks more effectively, emphasizing its role as a cornerstone of cyber resiliency. This underscores the importance of embedding intelligent data infrastructure that not only classifies and protects data but also enables real-time anomaly detection and resilient recovery, enabling business continuity even in worst-case scenarios.
- **Increased Investment:** Over 90 percent of respondents plan to increase cybersecurity budgets in the next 12 to 18 months, focusing on integrated and proactive solutions. Proactive investment can address the rising cost of cyberattacks and the growing complexity of threats, ensuring resilience and operational trust.

NetApp's Intelligent Data Infrastructure framework helps organizations address the cyber resiliency challenges revealed in this report by enabling organizations to take a proactive approach to data protection. By leveraging advanced data classification, AI-driven threat detection, and integrated security measures, organizations can more easily implement stringent governance practices, detect and respond to threats in real-time, and maintain compliance with evolving industry standards. As highlighted by the report, organizations with resilient data infrastructure have seen significant improvements in recovery times and overall data security, demonstrating that it is a critical component in modern cybersecurity strategies.

"This survey sheds light on the critical role of visibility and data-centric strategies in navigating the evolving cybersecurity landscape," said Daniel Newman, CEO at The Futurum Group. "By harnessing intelligent data infrastructure solutions, organizations can better protect their assets, ensure recovery, and thrive amidst disruption."

The report emphasizes the critical role of AI and integrated technologies as game-changers in combating increasingly sophisticated attack vectors. By leveraging AI alongside robust data classification and consolidated toolchains, enterprises can mitigate risks more effectively, reduce response times, and enhance visibility across sprawling hybrid multi-cloud environments.

To explore the full findings of the Cybersecurity Visibility Study 2024 and discover how IT and Security leaders are thinking about challenges and opportunities shaping the future of cyber resilience in the enterprise, [read the report here](#).

Methodology

In Fall 2024, NetApp collaborated with Futurum Research to conduct a comprehensive survey of over 1,300 cybersecurity leaders worldwide. The respondents included C-Level executives, Vice Presidents, and Directors in IT and Security, representing a diverse range of industries. The report draws on insights from the survey, as well as 15 in-depth interviews with selected decision-makers, offering a detailed analysis of the challenges and

opportunities shaping the cybersecurity landscape today.

Additional Resources

- [Empowering Cyber Resilience in the Digital Age](#)
- [The State of Cyber Resiliency 2024/2025](#)
- [Cyber Resilience: The Most Secure Storage on the Planet](#)

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 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.

About The Futurum Group

The Futurum Group is the fastest-growing independent tech research, intelligence, media, and advisory firm. Its organic growth is driven by emerging technologies and innovation across its clientele of more than 260 global companies. Futurum covers twelve major technology sectors: AI & data analytics, cloud, telecom, policy, consumer electronics, enterprise applications, security, semiconductors, workplace collaboration, sustainability, and CX. In 2023 it has acquired half a dozen companies in areas of research, intelligence, media, and performance testing and validation.