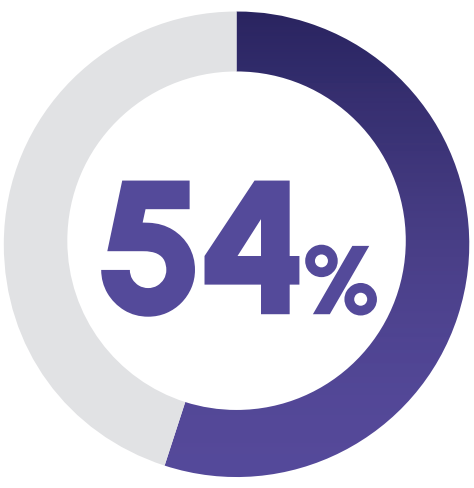
Futurum

NetApp®

The State of Cyber-Resiliency 2024/2025

The Case for a More Intelligent Approach to Data Infrastructure and Services

DATA UNDER SIEGE

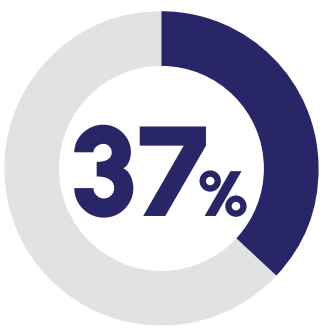


More than half of enterprises experienced a cyber-attack in the last 12-18 months.

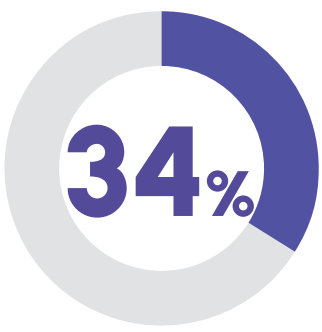
- One in five were unable to recover data.
- More than half were unable to prioritize their recovery operations based on the importance of their data – at least not easily.

But what are customers struggling with, specifically?

Top two challenges relating to cyber-resiliency:



Difficulty in identifying and prioritizing the most critical data for recovery



Data sprawl across hybrid multicloud environments

Slow time-to-detection

HYBRID MULTICLOUD HEADACHES

Approximately 90% of organizations are using a hybrid cloud environment.

Migration to a hybrid multicloud operating model was selected by nearly 40% of respondents as having the most material impact on their organization's cyber-resiliency.

Security risks related to usage of cloud environments ranked as the top threat across the world, being noted by 38%-40% of survey respondents.

As hybrid multi-cloud becomes the norm, data silos, visibility and protection gaps, and operational complexities inhibit cyber-resiliency.

CYBERESCURITY TOOLCHAIN SPRAWL ESCALATES THE ISSUE

70% of respondents indicated that their organization is using more than 40 tools for cybersecurity. **and** **84%** indicated that this vast number of tools is a problem when it comes to cyber-resiliency.

93% intend to use more capabilities that are built-in/native to your information infrastructure over the next 12-18 months.

Consolidating functionalities into fewer tools – especially via a simpler, more unified primary storage layer across hybrid multicloud – can help to streamline operations and avoid protection gaps.

DATA CLASSIFICATION TO THE FOREFRONT

More than 60% of the time, identification of compromised data was respondents' top issue slowing recovery.

Of the organizations that could not recover, only 20% had data classification – whereas more than half (52%) of organizations that could recover their data had data classification.

Data Classification is the lynchpin when it comes to optimizing defenses against cyber-attacks, and to getting critical business services back online following an attack. This is because it is foundational to aligning the most critical and sensitive data with required protection policies - and prioritizing this data for recovery.

HOW TO KEEP PACE MOVING FORWARD

AI-based detection technologies topped the list of tools in use for cyber-resiliency today (40%) and the top investment area in the future (30%), particularly for the primary production environment

Detecting attacks, with high precision, as quickly as possible is required in order to keep pace with continually changing and more sophisticated attack vectors. More intelligent, AI-enabled data services can help. To be effective, these models must be continuously updated in tandem with emerging threat vectors.

Futurum

NetApp®

The Futurum Group is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.

The Futurum Group LLC | futurumgroup.com | (833) 722-5337 | © 2024 The Futurum Group. All rights reserved.