NetApp | Gartner Peer Insights.

Cyber resilience: A new paradigm for protecting and securing data

There's an increased need for Security and IT teams to work together to protect their organizations from breaches. The differences between traditional security functions and data protection are becoming less prominent. Historically, the responsibilities of security professionals primarily involved perimeter and network security, end user devices, user account management, etc.

1. It's time for a new paradigm: cyber resilience (which includes data protection + data security).
2. Organizations need to protect data from the inside-out (Zero Trust principle).

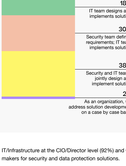
GPI and NetApp surveyed 200 IT leaders to learn how organizations manage readiness, response, and recovery from cyberattacks.

Data collection: April 29 – June 16, 2022

Respondents: 200 IT leaders

IT and security teams work together to address cyberthreats

38% of leaders reported that their security and IT teams design and implement solutions to address cyberthreats together.



How do teams within your organization primarily work to address cyberthreats such as ransomware?

IT/Infrastructure at the CIO/Director level (92%) and CISO (83%) are the primary decision makers for security and data protection solutions.

Who are the key decision makers (as opposed to influencers) when it comes to your security and data protection solutions?

Similarly, IT/Infrastructure (82%) and CISO (74%) were named as the top key influencers for security and data protection solutions.

Who are the key influencers when it comes to your security and data protection solutions?

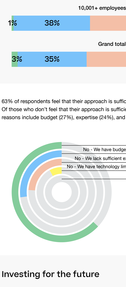
A layered security approach

Respondents primarily rely on backup software (77%), behavior analytics (68%), and logical air gap (47%) to protect and recover from cyberthreats.

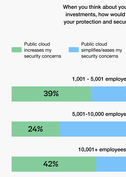
What solutions/tools do you rely on most to protect and recover data from cyberthreats such as ransomware?

- 36% A physical air gap solution (e.g. tape library)
- 35% Antivirus software
- 21% Native/built-in storage features (e.g. snapshots)
- 6% We don't have a well-defined solution
- 0% Other

Overall, 82% of IT leaders indicated that they use 3 or more data protection vendors. Respondents from organizations with more than 10,000 employees were nearly twice as likely to report more than 4 data protection vendors (13%) as compared to those with 1,001–5,001 employees (7%) and 5,001–10,000 employees (6%).



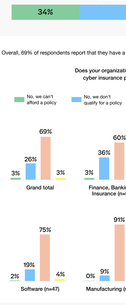
63% of respondents feel that their approach is sufficient enough to address cyber threats. Of those who don't feel that their approach is sufficient to address cyber threats, the reasons include budget (27%), expertise (24%), and technology limitations (8%).



Do you feel your approach is sufficient to address cyber threats such as ransomware?

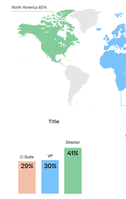
Investing for the future

Respondents from organizations with 5,001 to 10,000 employees are far more likely than others to trust public cloud. 71% of respondents from organizations with 5,001 to 10,000 employees report that public cloud simplifies/eases their security concerns.



Overall, 69% of respondents report that they have a cyber insurance policy in place.

Respondents plan to invest in data recovery (72%), zero-trust architecture (65%), ransomware detection (48%), and data classification (46%) in the next year.



To address the complex challenges of today's cyberthreats, a data-centric approach to security and protection is required.

Cyber resilience combines data protection with data security, so organizations can bounce back from a cyberattack. Even if an intruder manages to breach the perimeter or an insider takes malicious action, the data is covered, because it has protection that's built-in rather than bolted on as an afterthought.

NetApp® cyber-resilience solutions keep your data available and recoverable while detecting and thwarting threats before they can do harm. Learn more here: netapp.com/cyber-resilience

Respondent Breakdown

Gartner

Source: Gartner Peer Insights, Cyber Resilience survey