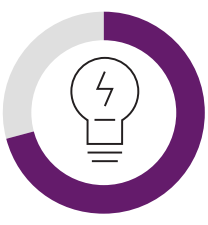
S&P Global
Market Intelligence

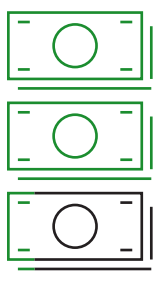
Why collaborative cybersecurity is the key to resilience

Discover why data resiliency now hinges on **IT and security teams working together** on system design, implementation and operations.

Outages have become commonplace.



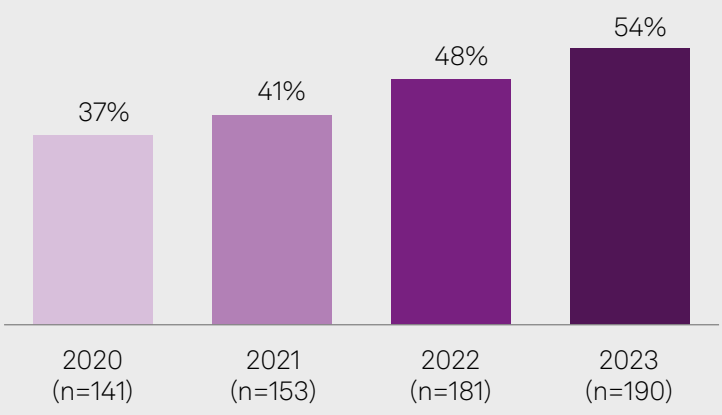
71%
of organizations have experienced a significant outage ...



... with almost a third affected within the past two years.

Q. When was the last time your organization experienced an outage that resulted in lost data or affected worker productivity?
Base: IT decision-makers whose organizations use on premises storage systems (n=262).
Source: 451 Research's Voice of the Enterprise: Storage, Disaster Recovery 2023.

Security teams are **overwhelmed**, and it's getting worse.



The percentage of alerts that security teams are unable to investigate in a typical day has risen by 6% per year since 2020, crossing 50% for the first time in 2023 — indicating the need to rethink backup and recovery systems and strategies.

Q. What percentage of SIEM/security analytics alerts are you unable to investigate in a typical day?
Base: Respondents who currently use SIEM security analytics.
Sources: 451 Research's Voice of the Enterprise: Information Security, Vendor Evaluations 2020, 2021; Security Operations 2022; Security Analytics & SecOps 2023.

Outages **cost** time and resources.

Longer response and recovery times translate into costly business impacts, such as system downtime, ransom payments and compliance issues.

$2.15 million
Mean cost of recent outages

70%
Of outages require moderate to significant effort to complete failback

29%
Of recent outages have been caused by a security issue such as ransomware

Q. Please estimate the total cost to your organization of its most recent outage or downtime (from outage to full recovery, including direct costs, opportunity costs, etc.).
Base: IT decision-makers whose organizations use on premises storage systems (n=262).
Q. How much effort is required to resume normal operations after a failure (i.e., a failback)?
Base: IT decision-makers whose organizations use on premises storage systems (n=260).
Q. What was the cause of your organization's most recent outage that resulted in lost data or affected worker productivity? Please select all that apply.
Base: IT decision-makers whose organizations experienced an outage/downtime that resulted in lost data or productivity (n=183).
Source: 451 Research's Voice of the Enterprise: Storage, Disaster Recovery 2023.

Collaboration to strengthen cyber resilience is the way forward.

US NIST CSF 2.0 outlines cybersecurity functions and desired outcomes to help organizations manage cybersecurity risks, including an emphasis on reducing silos and encouraging collaboration.

Protect and monitor devices and use automated backups to ensure data is recoverable. Encrypt data everywhere.

Detect potential cybersecurity issues by monitoring your networks, systems and facilities.

Respond by acting quickly when a cybersecurity incident has occurred.

Recover assets and operations after a security incident, including through effective storage practices.

Commissioned by

PURESTORAGE®
Uncomplicate Data Storage, Forever

Cyber resilience is more than just a strategic priority — it's a collective effort.

Discover how security and IT teams work together to keep data safe, prevent cyberattacks and quickly recover from disruptions in **Achieving cyber resilience requires teamwork report**.