Cyber Resilience In Action

Benchmarking Global Enterprise Readiness Across Secure / Detect / Recover
Insight Discussion
November 2025

DELL Technologies

•Objectives and Firmographics

•The Cyber Resilience Gap

•Secure

•Detect

•Recover

•Complexity, Culture and What’s Next

Agenda

Business objectives

To position Dell as a thought leader and strategic partner for cyber resilience

Research objectives

- Assess the maturity and integration of cyber resilience strategies
- Evaluate the effectiveness of organizations' secure, detect and recovery practices
- Understand barriers to improving cyber resilience, including skill gaps, budget, and complexity
- Explore how organizations are securing their IT environment and protecting data from ransomware threats

Who did we interview?

Respondents were interviewed in July and October 2025

850 IT decision makers from global organizations

Organizations with 1,000+ employees

Organizations from a range of public and private industries

Respondents are:
Board members; C-level
Senior managers
Mid-level managers

DELL Technologies

Key findings

39%

of organizations have a fully established and continuously optimized cyber resilience strategy

Continuous optimization is key - without it, strategies can quickly become outdated against evolving threats leaving organizations at greater risk

46%

recognize their backup data is not as well protected as it should be

Strengthening backup protection is essential to ensure recovery remains possible when primary systems are compromised.

Secure

30%

use a comprehensive platform for threat detection across network, backup, and primary storage

Without unified detection, threat visibility and response times can be slower, increasing the risk of undetected breaches.

Detect

55%

of those who conducted simulated cyberattacks monthly or more frequently successfully recovered from a drill/cyber incident

Frequent testing helps teams prepare for the real deal. Teams that are unprepared risk delayed response and recovery when it matters most.

Recover

63%

think leadership overestimates their organization's readiness for a major cyber event

Overconfidence can stall investments, delay response planning, and leave critical vulnerabilities unaddressed.

Section 1: The Cyber Resilience Gap

Understanding the problem and the urgency to evolve

DELLTechnologies

Continuously optimizing resilience strategies improves recovery, yet success is not guarenteed

99.5%

Have a cyber resilience strategy of some form

39%

believe it to be fully established and continuously optimized (a mature strategy)

57%

did not contain and recover effectively during their last test or incident

Organizations with mature cyber resilience strategies are **2.6 times more likely to recover** successfully

65% Vs. **25%**

63%

believe **leadership overestimates their readiness** for a major cyber event

Why this matters now

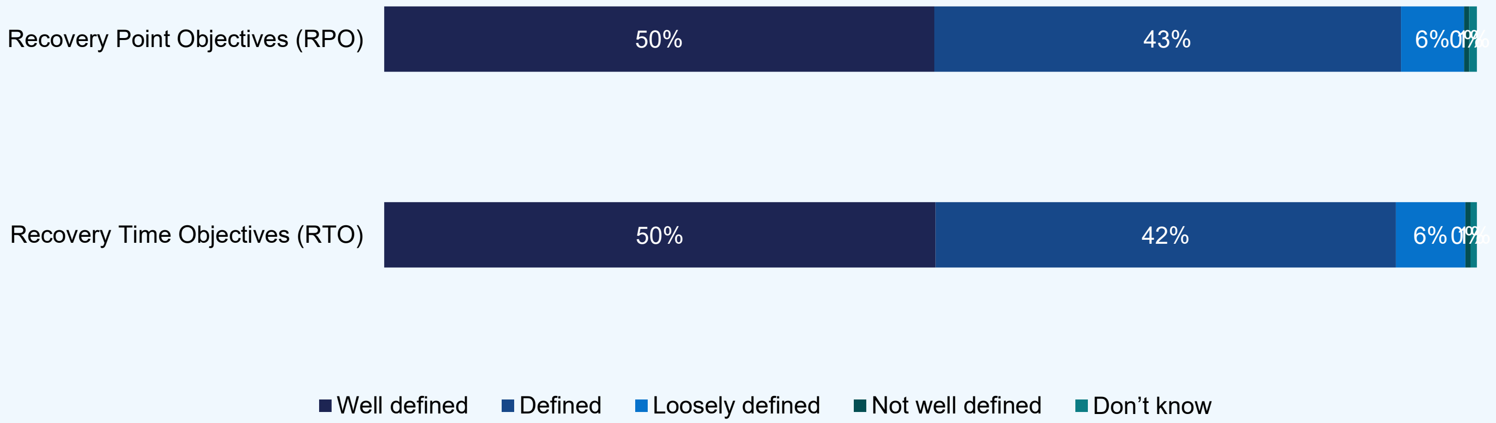
97%

Agree their organization needs to continually strengthen security as threats evolve

78%

believe their organization focuses more on preventing attacks than preparing to recover from them

The extent that organizations have defined:



32%

Have **both areas** well defined

Of those with a mature cyber resilience strategy

58%

Have both well-defined RTO and RPO

DELL Technologies

Section 2: Secure

Preventing attacks and hardening the digital estate

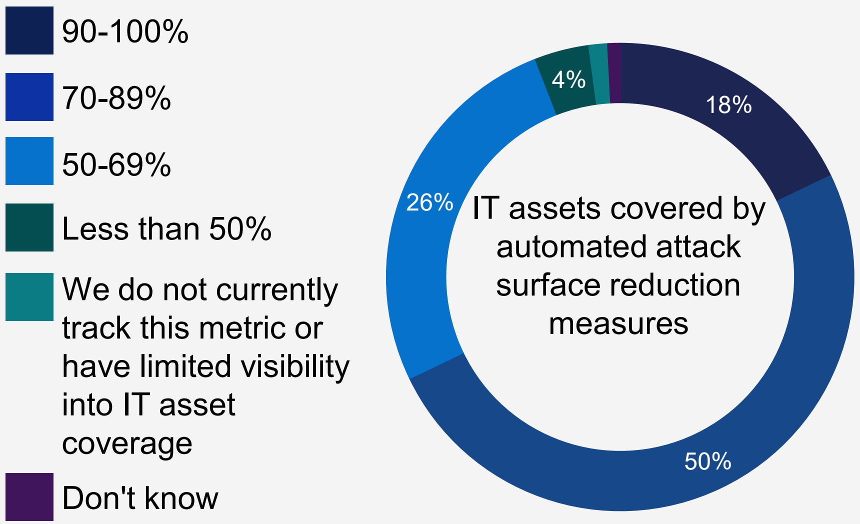
Visibility Gaps and Protection shortfalls

46%

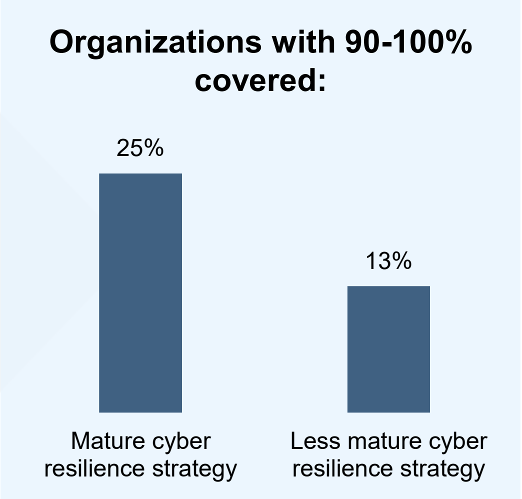
admit their backup data is not as well protected as it should be

NA	**59%**
EMEA	**43%**
LATAM	**41%**
APJ	**39%**

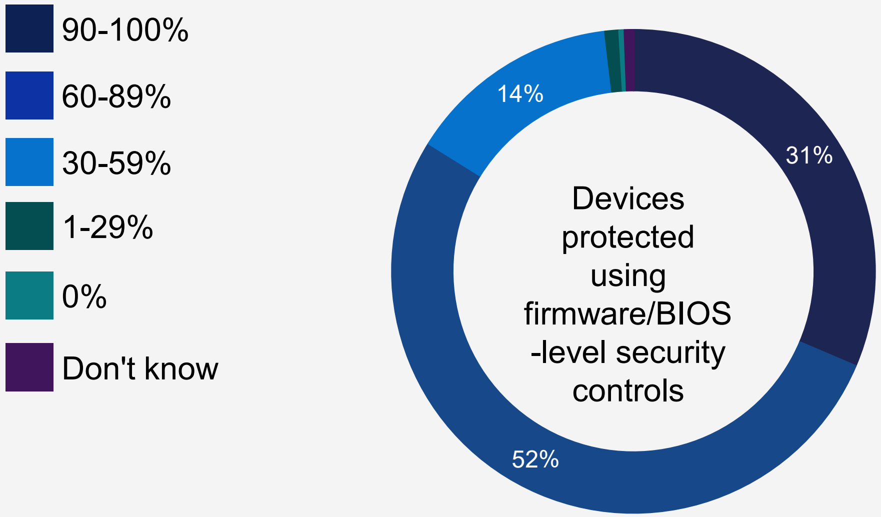
Continuous optimization does not eliminate coverage gaps, but it does give organizations a critical edge in resilience



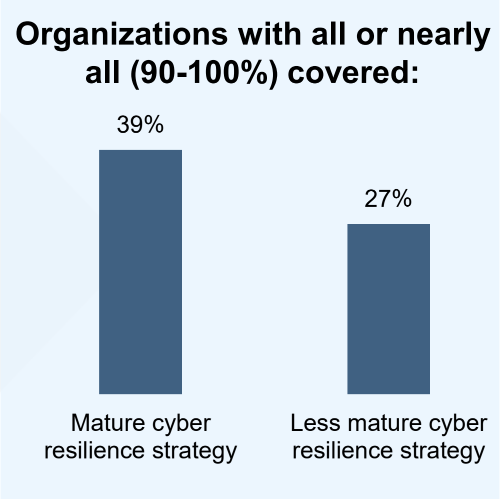
IT assets covered by automated attack surface reduction measures



Organizations with 90-100% covered:



Devices protected using firmware/BIOS -level security controls



Organizations with all or nearly all (90-100%) covered:

From pre-deployment integrity to post-attack recovery: strengthen both ends of security

Processes/Methods used by organizations to ensure the integrity of IT hardware/software

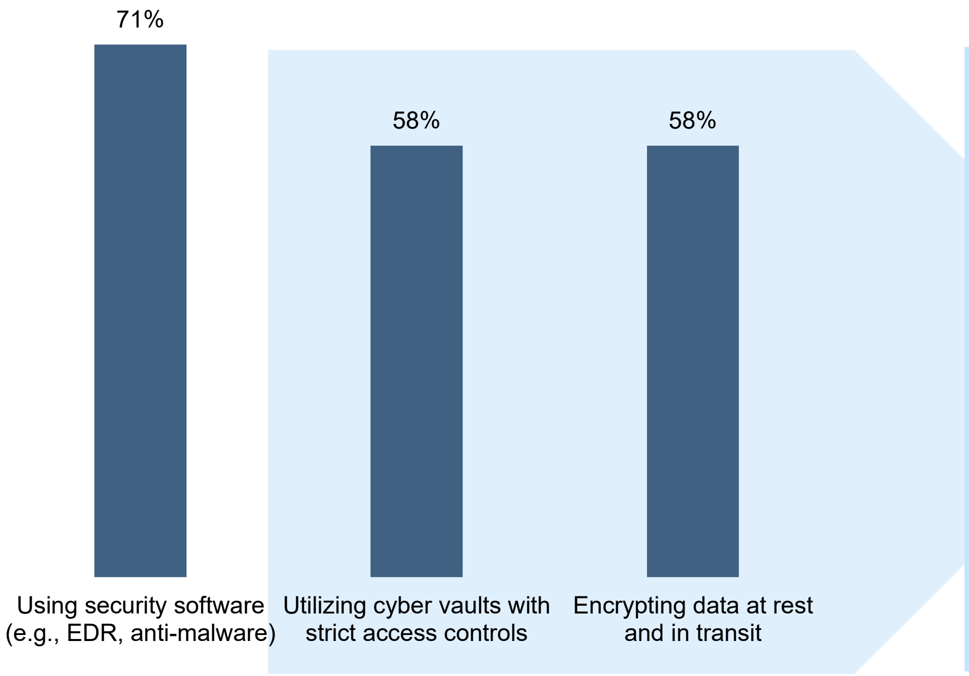
72%

rely on vendors for certifications and attestations and for systems with embedded tools that verify component integrity

64%

perform internal audits or manual reviews during staging/deployment

Methods used by organizations to secure critical data from ransomware attacks



Organizations with mature resilience strategies more likely to use:

- **Data encryption (59% vs 57%)**
- **Cyber vaults (63% vs 55%)**

than organizations with less mature resilience strategies

Section 3: Detect

Spotting and responding to threats before impact

Utilizing AI and automation could uncover threats before they compromise backups

38%

of organizations use AI/ML tools with proactive mitigation and response playbooks

Organizations with a mature cyber resilience strategy **3.1X more** likely to do this

65% Vs. **21%**

48%

of organizations use **AI/ML extensively to scan backup data** for indicators of compromise

Extensive use of AI/ML occurs **2.3X as often in organizations with a mature cyber resilience strategy**

72% Vs. **32%**

83%

believe threat actors are **increasingly attacking backups** during ransomware attacks

62% are prioritizing investing in automation and AI/ML powered threat detection

DELLTechnologies

Incomplete visibility increases risk

54%

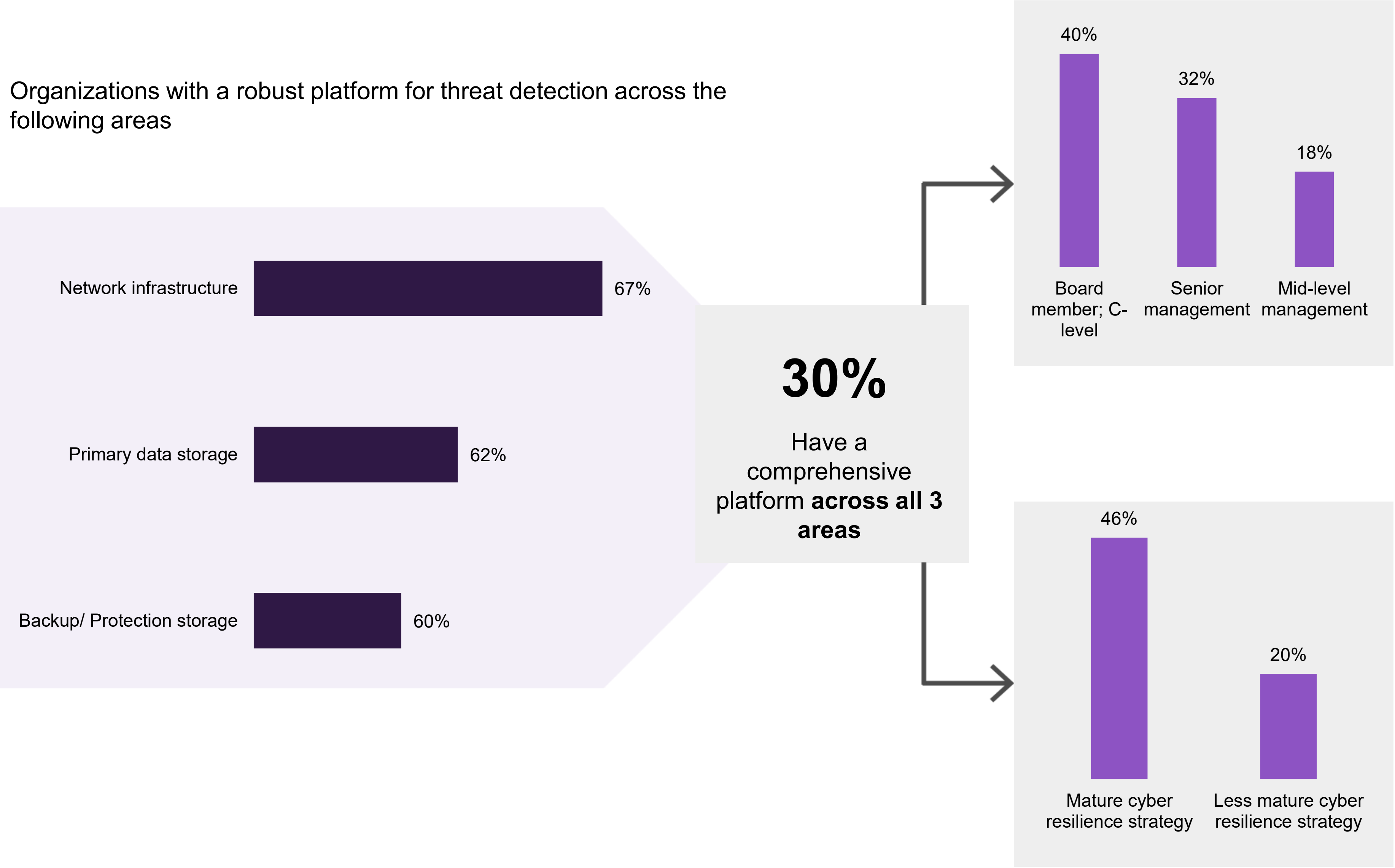
say they have high visibility into suspicious activity or compromised data within their backup systems

74% Organizations with a mature cyber resilience strategy

Vs

42% of organizations with a less mature cyber resilience strategy

Organizations with a robust platform for threat detection across the following areas



30%

Have a comprehensive platform **across all 3 areas**

DELLTechnologies

Section 4: Recover

Bouncing back fast, and within SLA expectations

State of recovery: many organizations meet targets, but continued improvement is essential to keep pace with the threat landscape

40%

successfully contained and recovered with minimal impact

With **board members (**53%**)** more likely to state this than **mid-level managers (**30%**)**

54%

of organizations met their **RTO/RPO targets**

By position: Board members (66%) Vs Mid-level management (45%)

#4

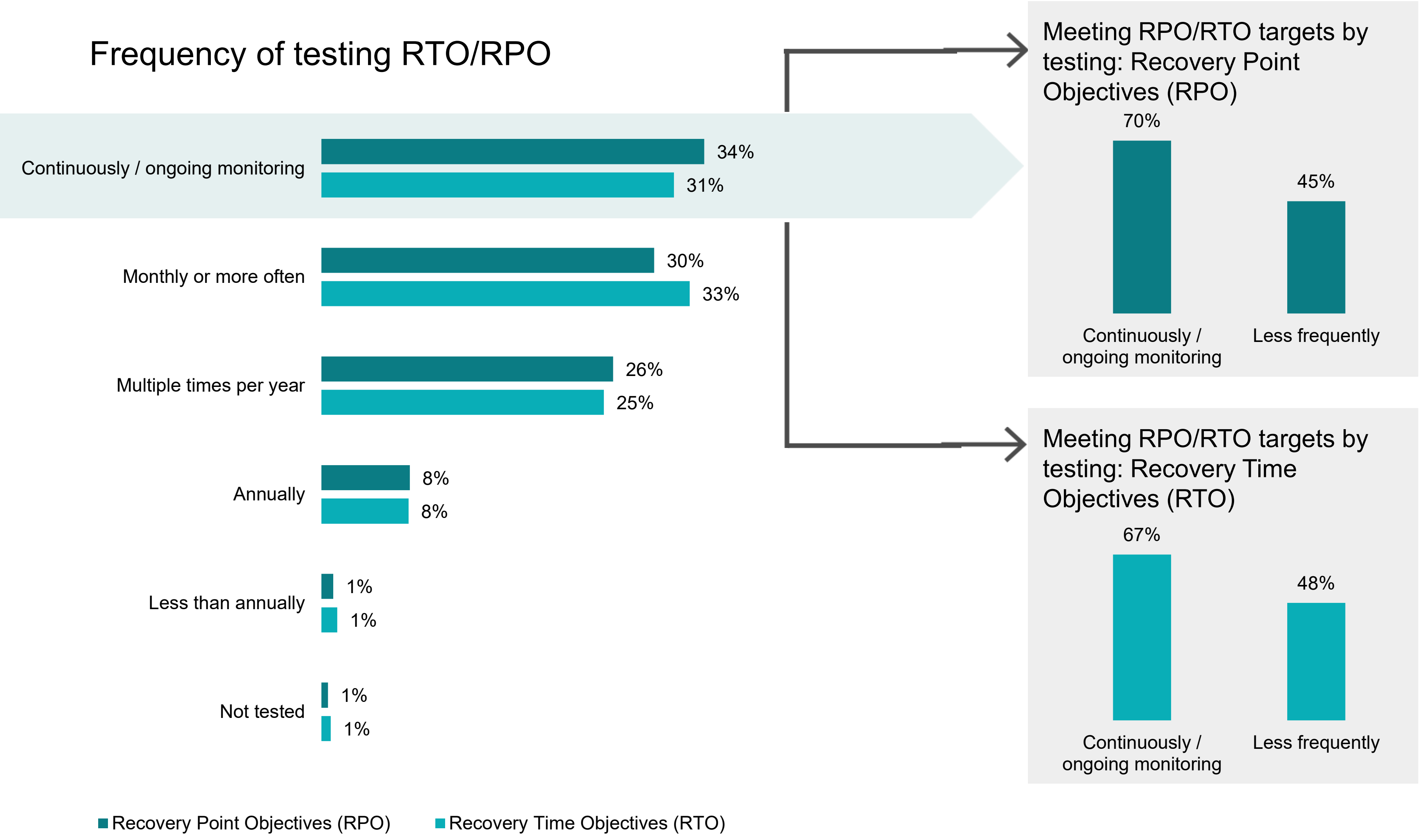
Primary driver of cybersecurity investment is a **recent cyber incident or near miss** at our organization

57% are enhancing resilience capabilities to **meet regulatory or compliance requirements**

Testing is crucial to resilience, giving organizations a better chance to recover

Frequent testing could improve recovery

> Ultimately, a culture of alertness and constant improvement is what builds resilience.
>
> *Snr Manager, Consumer Services organization, Brazil*



Frequency of testing RTO/RPO

Meeting RPO/RTO targets by testing: Recovery Point Objectives (RPO)

Meeting RPO/RTO targets by testing: Recovery Time Objectives (RTO)

Testing is fundamental to resilience

48%

Stated their organization's cybersecurity testing does not realistically simulate modern attack techniques

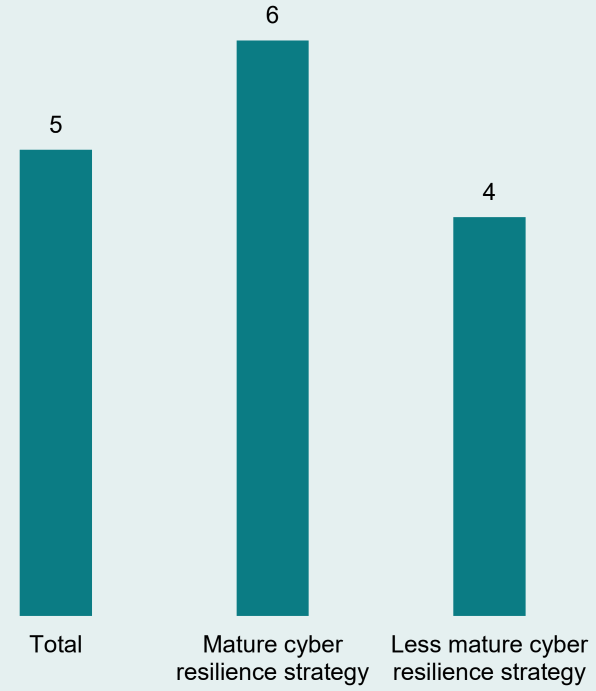
53% of board members; C-Level

Vs

48% of mid-level management

Regular practice is key to boosting recovery, but organizations should continuously plan for evolving threats

Average times per year organization conducts simulated cyberattacks



55%

of those who conducted simulated cyberattacks **monthly or more frequently successfully recovered** from a drill/cyber incident

35%

of those who conducted simulated cyberattacks **less than monthly successfully recovered** from a drill/cyber incident

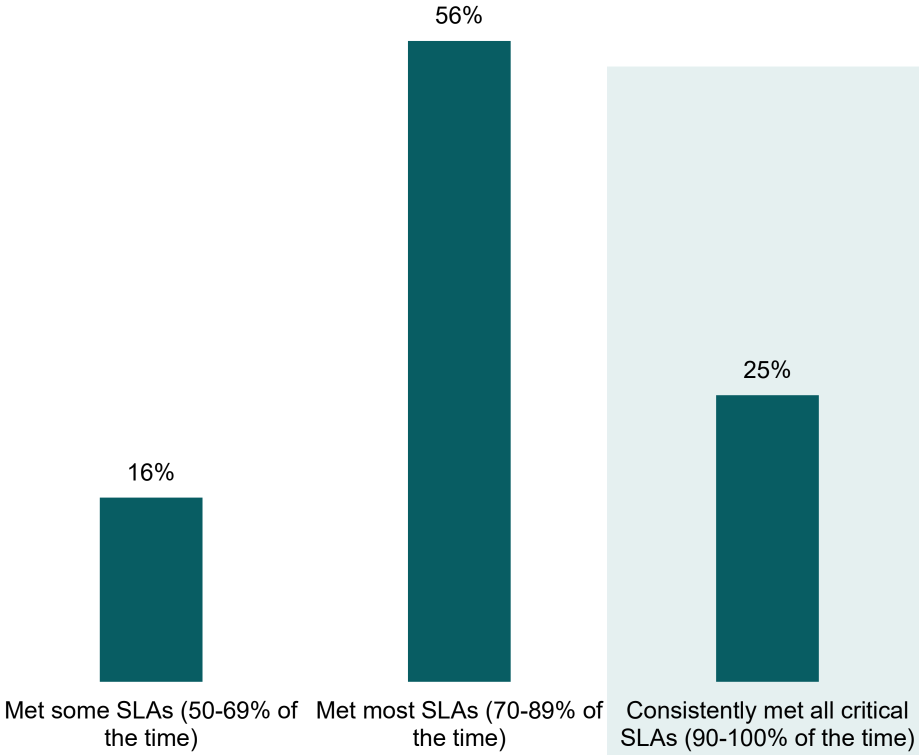
> *The need to test and evaluate holistically across all potential threat surfaces rather than focusing on point coverage/testing.*
>
> Snr Manager, IT Technology and Telecoms, UK

> *Cyber attacks remind us how important it is to conduct regular security drills.*
>
> *Security awareness training has been strengthened, enabling every employee to identify potential threats.*
>
> Board Member, Construction and properties, Australia

DELL Technologies

SLAs are the proof point: organizations with mature strategies deliver on recovery promises

Frequency of organizations meeting SLAs for critical system recovery

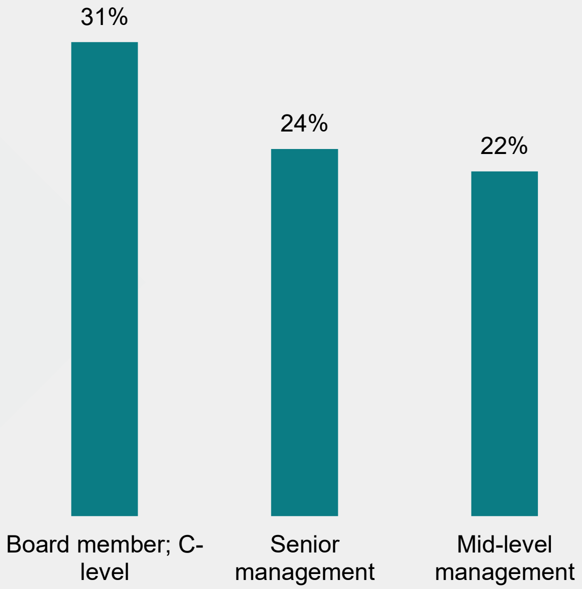


2x

Organizations with mature cyber resilience strategies are more likely to consistently meet their SLAs

36% Vs. **18%**

By position:



Section 5: Complexity, culture and what's next

Organizational barriers and future investment plans

DELL Technologies

Complexity, skills gaps, and overconfidence threaten cyber resilience, but AI and training could assist

Top challenges:

Complex IT environment	49%
Budget limitations	42%
Lack of skilled staff	39%
Vendor/ tool fragmentation	38%
Low executive prioritization	23%

Larger organizations more likely to face this:

50%	5,000 or more employees
50%	3,000-4,999 employees
46%	1,000-2,999 employees

63%

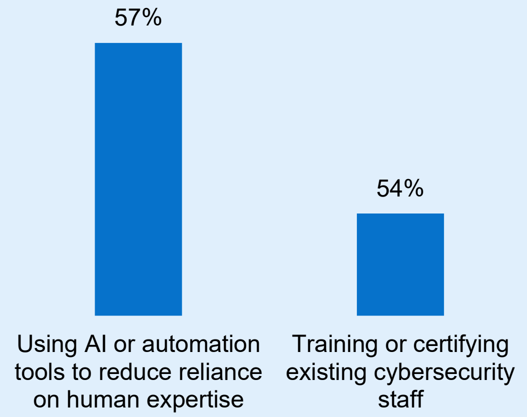
think leadership overestimates their organization’s readiness for a major cyber event

96%

Acknowledge they have shortfalls in their cybersecurity skills or expertise

BUT...

Organizations are acting through:



Looking ahead to investments

#1

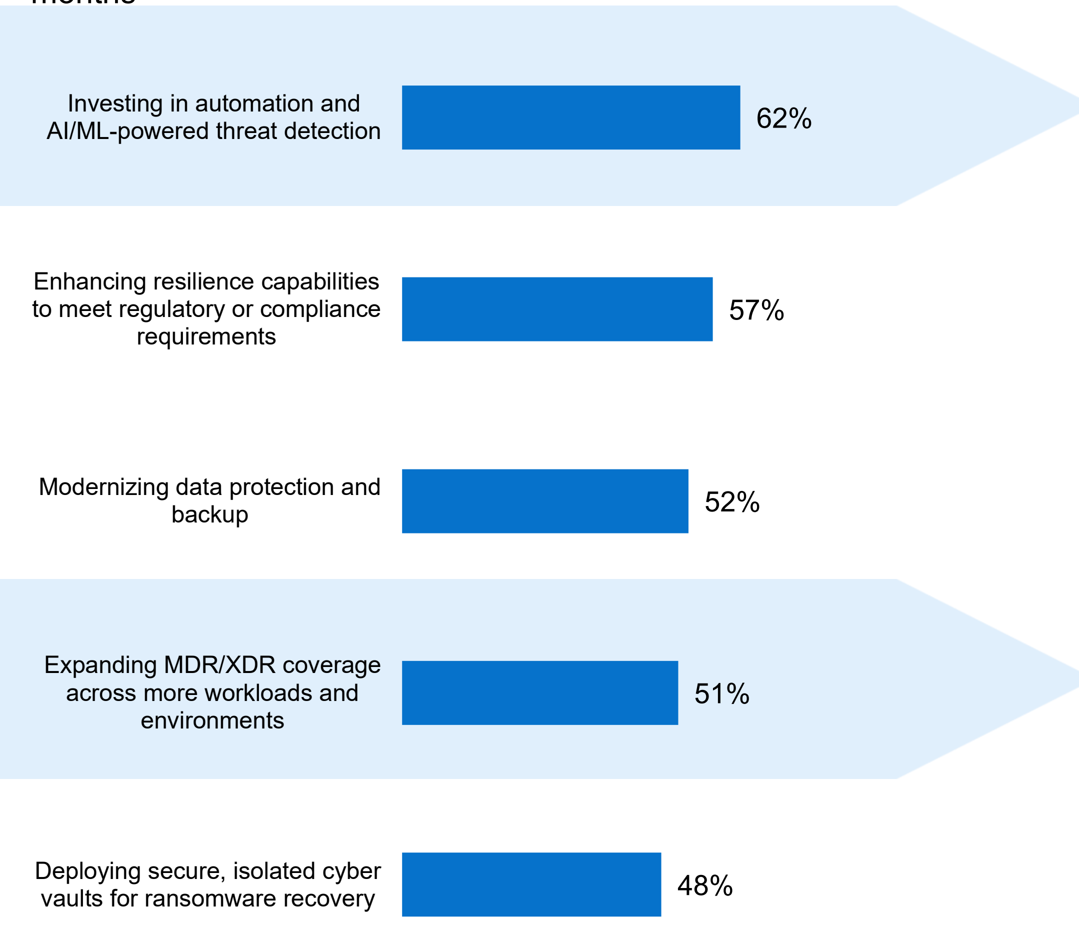
Driver of investment is the evolving threat landscape

97%

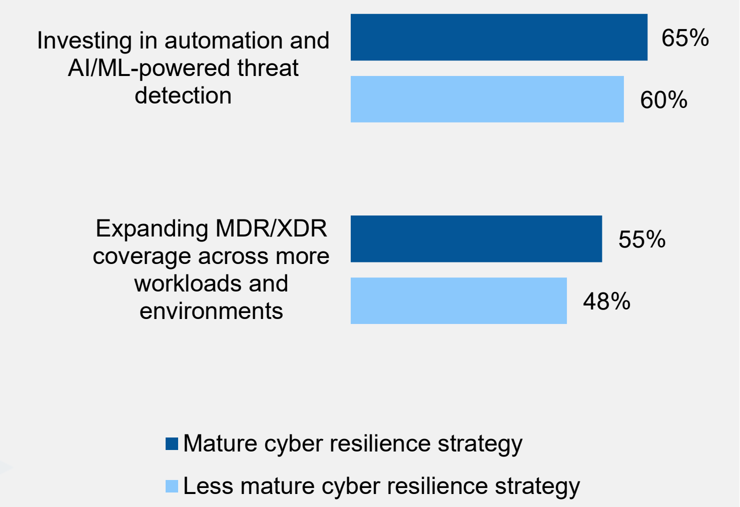
“My organization needs to continually strengthen its security as threats evolve”

To maintain a mature stance, continuous investment and optimization is the way forward

Prioritized cyber resilience investments over the next 12 months



Mature cyber resilient organizations are continuously investing



Key takeaways

Dell Technologies

Key findings

39%

of organizations have a fully established and continuously optimized cyber resilience strategy

Continuous optimization is key - without it, strategies can quickly become outdated against evolving threats leaving organizations at greater risk

46%

recognize their backup data is not as well protected as it should be

Strengthening backup protection is essential to ensure recovery remains possible when primary systems are compromised.

Secure

30%

use a comprehensive platform for threat detection across network, backup, and primary storage

Without unified detection, threat visibility and response times can be slower, increasing the risk of undetected breaches.

Detect

55%

of those who conducted simulated cyberattacks monthly or more frequently successfully recovered from a drill/cyber incident

Frequent testing helps teams prepare for the real deal. Teams that are unprepared risk delayed response and recovery when it matters most.

Recover

63%

think leadership overestimates their organization's readiness for a major cyber event

Overconfidence can stall investments, delay response planning, and leave critical vulnerabilities unaddressed.

DELL Technologies