When Threats Become Smarter: Dell's Approach to Cyber Resilience

Secure, Detect and Recover Critical Data from AI-enabled Cyber Threats

Pasi Vainikka
Sr Systems Engineer
DELL Technologies

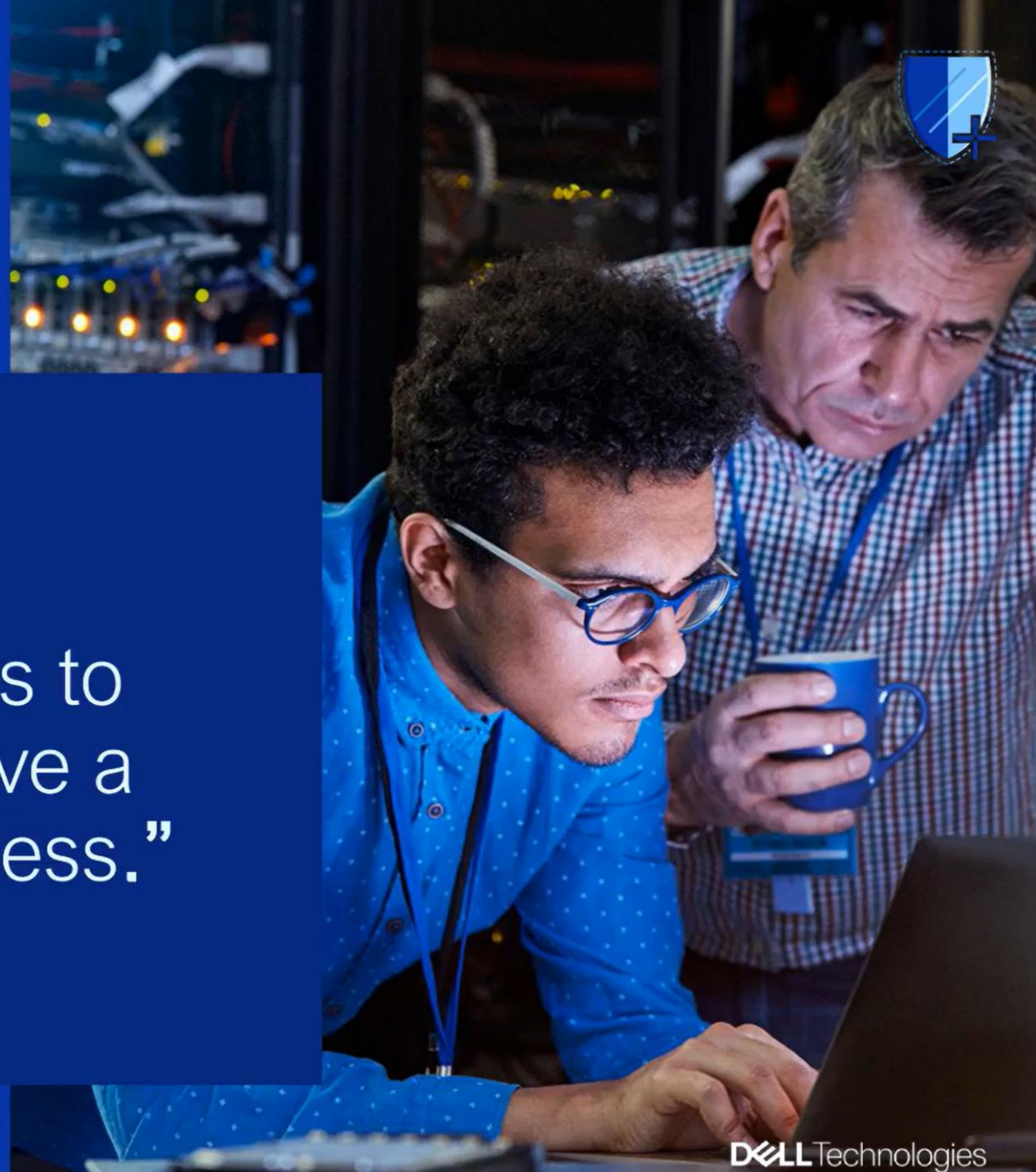
SECURITY DAY '26

2026 11 10 I LITEXPO

Prepare for the Worst-Case Scenario

“If a focused entity really wants to get into your system, they have a really high probability of success.”

Adm. Michael Rogers, former director of NSA and commander of U.S. Cyber Command



DELL Technologies

AI changes the cyber threat landscape

Weapon

Attackers leverage AI to harm
Protect against AI-enabled attacks that accelerate vulnerability discovery & exploitation

Target

New risks created by your use of AI
Protect the integrity of models and training data and define security controls for the use of AI in your products and offers

Tool

Improve services and cybersecurity using AI
Help identify risks faster and how controls can help decrease those risks

89% Increase in attacks by AI-enabled adversaries*

* CrowdStrike 2026 Global Threat Report

Copyright © Dell Inc. All Rights Reserved.

AI, accelerating vulnerability exploitation to hours, not weeks

The impact is already real

Frontier AI models compress attack velocity

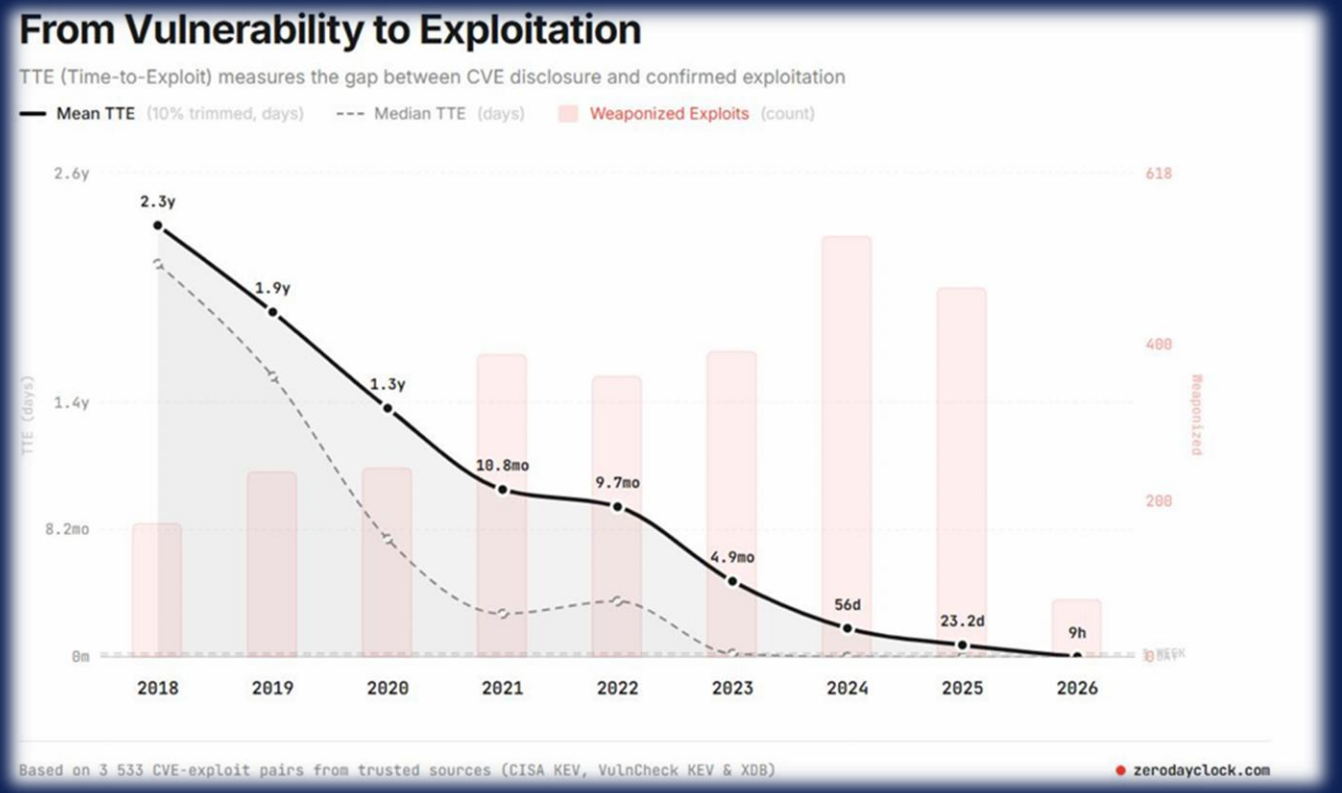
Models such as Anthropic's Mythos shrink the gap between vulnerability discovery and exploitation from weeks or months into hours.

Adversaries are more convincing and at scale

AI-enabled attackers increase the speed, scale and sophistication of attacks — including AI-assisted voice social engineering.

Non-human identities are the new target

Attackers increasingly pursue tokens, service accounts and other non-human identities that can unlock broad administrative access.



Resilience is not an option, it's **Existential** to your business

* Zerodayclock.com

Copyright © Dell Inc. All Rights Reserved.

Is your business resilient or at risk?

24 days

Average downtime after a Ransomware attack[1]

79%

Attacks did not deploy malware - relying instead on “hands-on-keyboard” techniques[3]

$1.84M

Average cost to recovery from ransomware attack in 2025 (excluding payment)[2]

94%

Of ransomware attacks included attempts to compromise the backup (57% success rate)[4]

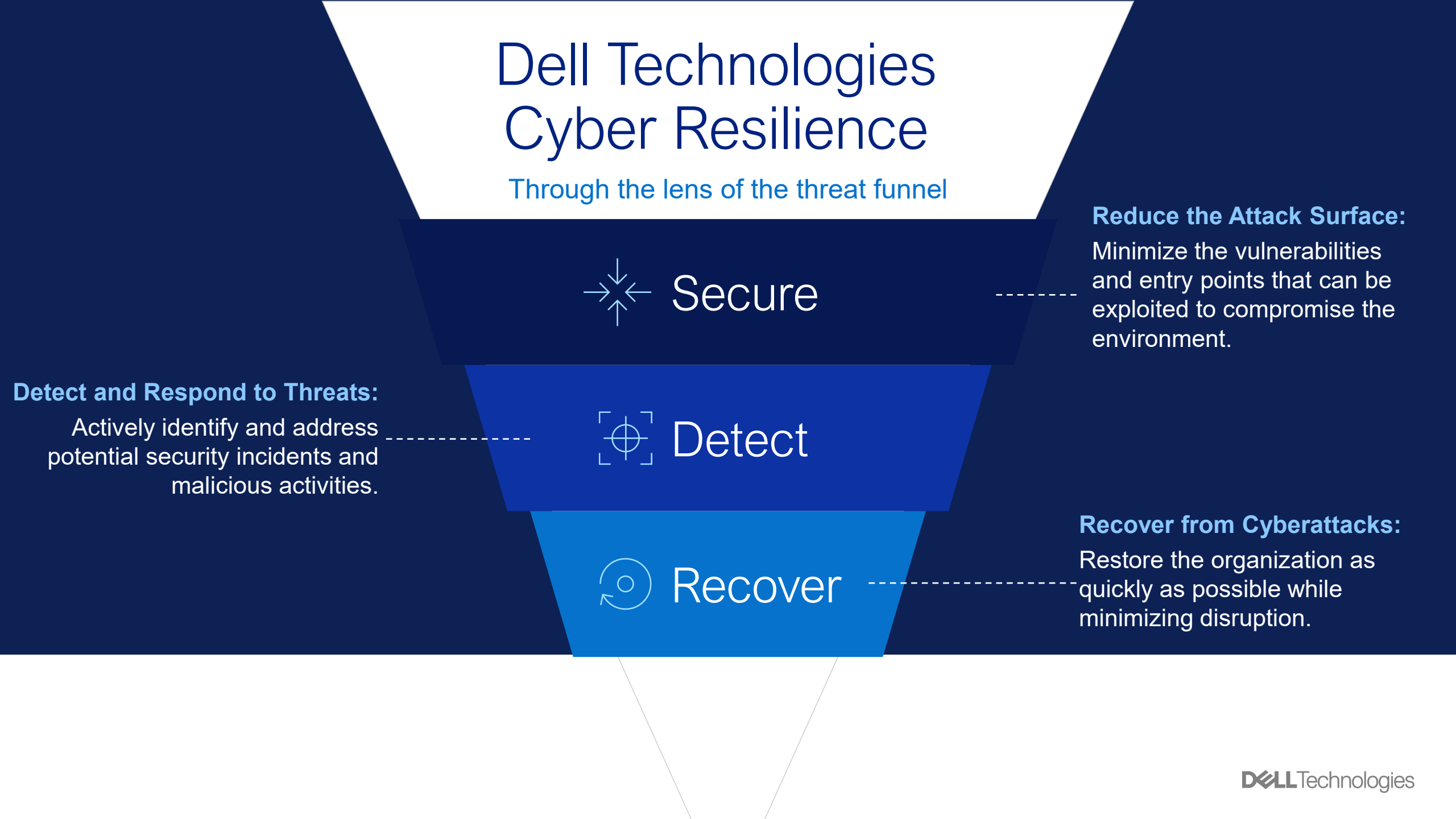
Without a clean state to recover to, an IT incident becomes a business crisis

DELL Technologies

Copyright © Dell Inc. All Rights Reserved.

Dell Technologies Cyber Resilience

Through the lens of the threat funnel



Reduce the Attack Surface:
Minimize the vulnerabilities and entry points that can be exploited to compromise the environment.

Detect and Respond to Threats:
Actively identify and address potential security incidents and malicious activities.

Recover from Cyberattacks:
Restore the organization as quickly as possible while minimizing disruption.

Dell Customer Communication - Confidential

The 5 ingredients for recovery

Recovery has no easy button — successful recovery depends on five ingredients, in sequence.

1 **Prioritize Critical Services**

Know what must come back — and in what order.

> 2 **Viable Recovery Source**

Find data you can prove is safe to restore.

> 3 **Viable Recovery Target**

Rebuild somewhere the attacker can't reach.

> 4 **Verify Clean Recovery**

Validate that what you restore is truly clean.

> 5 **Return To Service**

Bring workloads back with confidence.

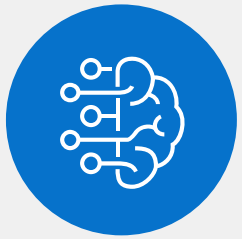


Only Dell covers all five ingredients end-to-end

DELL Technologies

How to ensure your data is clean for recovery

AI-Driven Detection



Highly trained AI helps protect against evolving threats, detecting corruption with up to 99.99% accuracy.

Rapid Identification & Restoration



Quickly detect compromised snapshots and recover from clean primary storage copies

Assured Recovery



Air gapped vault provides trusted copies for assured recovery (CyberSense)

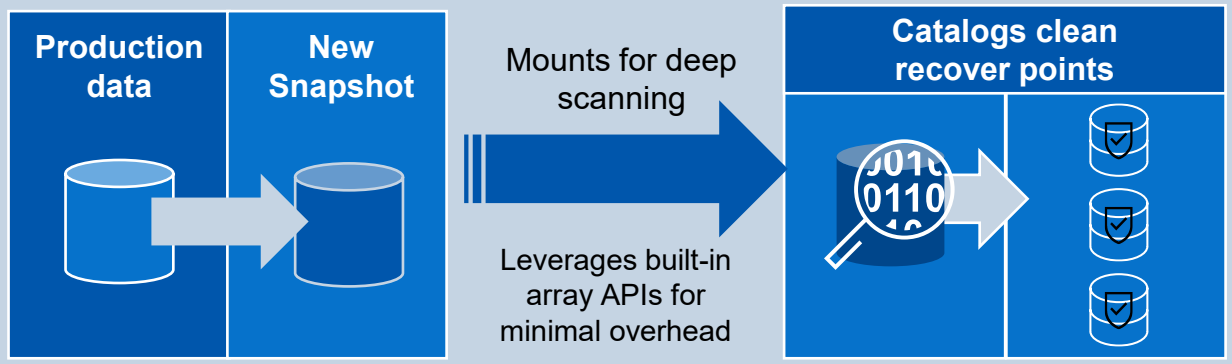
Rapidly detect corruption and confidently recover from ransomware

Copyright © Dell Inc. All Rights Reserved.

Dell Cyber Detect for Storage

Recover mission-critical data faster from clean snapshots directly on Dell Storage appliances

Create and identify clean snapshots ***directly on the array***





PowerStore



PowerMax[1]



Cyber Detect
(VM[2] or bare metal)

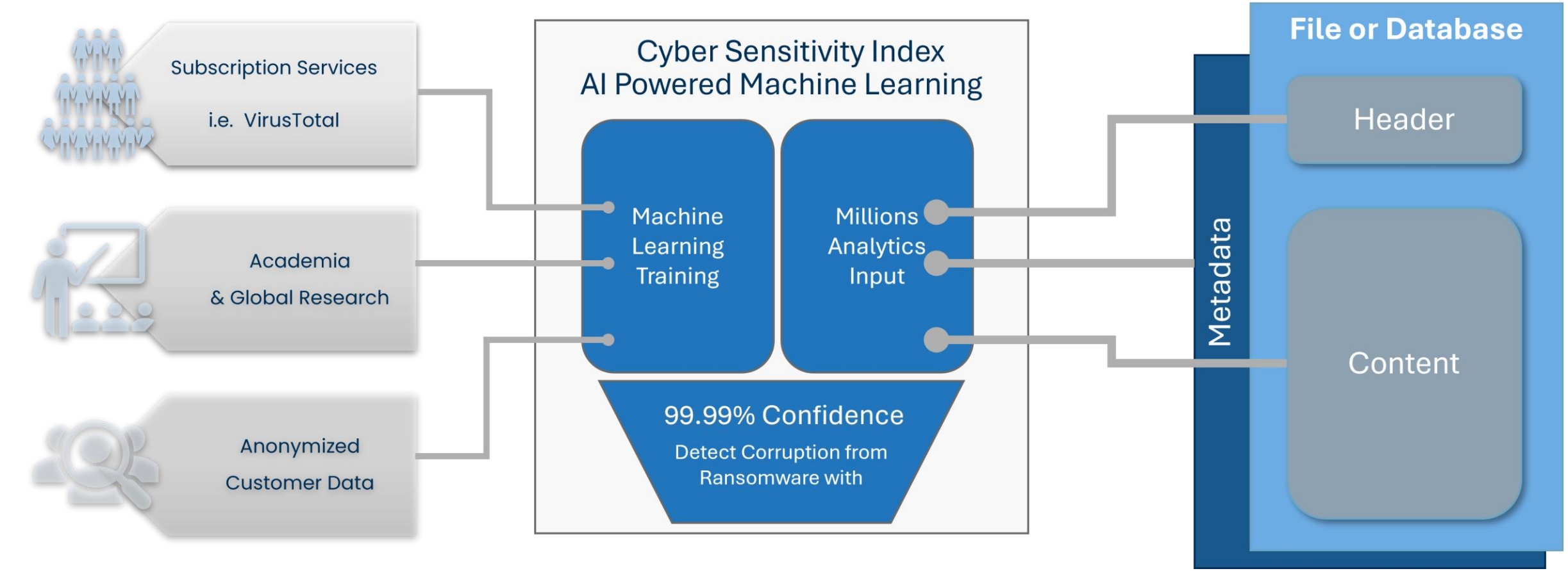
- Create a schedule for regular restore checkpoints
- Supports a broad range of mission-critical applications
  - Oracle, SAP, SQL, and more…
- Make informed recovery decisions to eliminate reinfection and minimize downtime and data loss
- Deep forensics provides type of attack, blast radius, affected files, and more
- Ready to integrate with SIEM/SOAR systems

1 PowerMax Cyber Detect availability planned for 2H, FY2026
2 Support for VM deployment planned for future release.

Copyright © Dell Inc. All Rights Reserved.

AI-based Machine Learning Analytics in Cyber Vault

The intelligence to verify data integrity



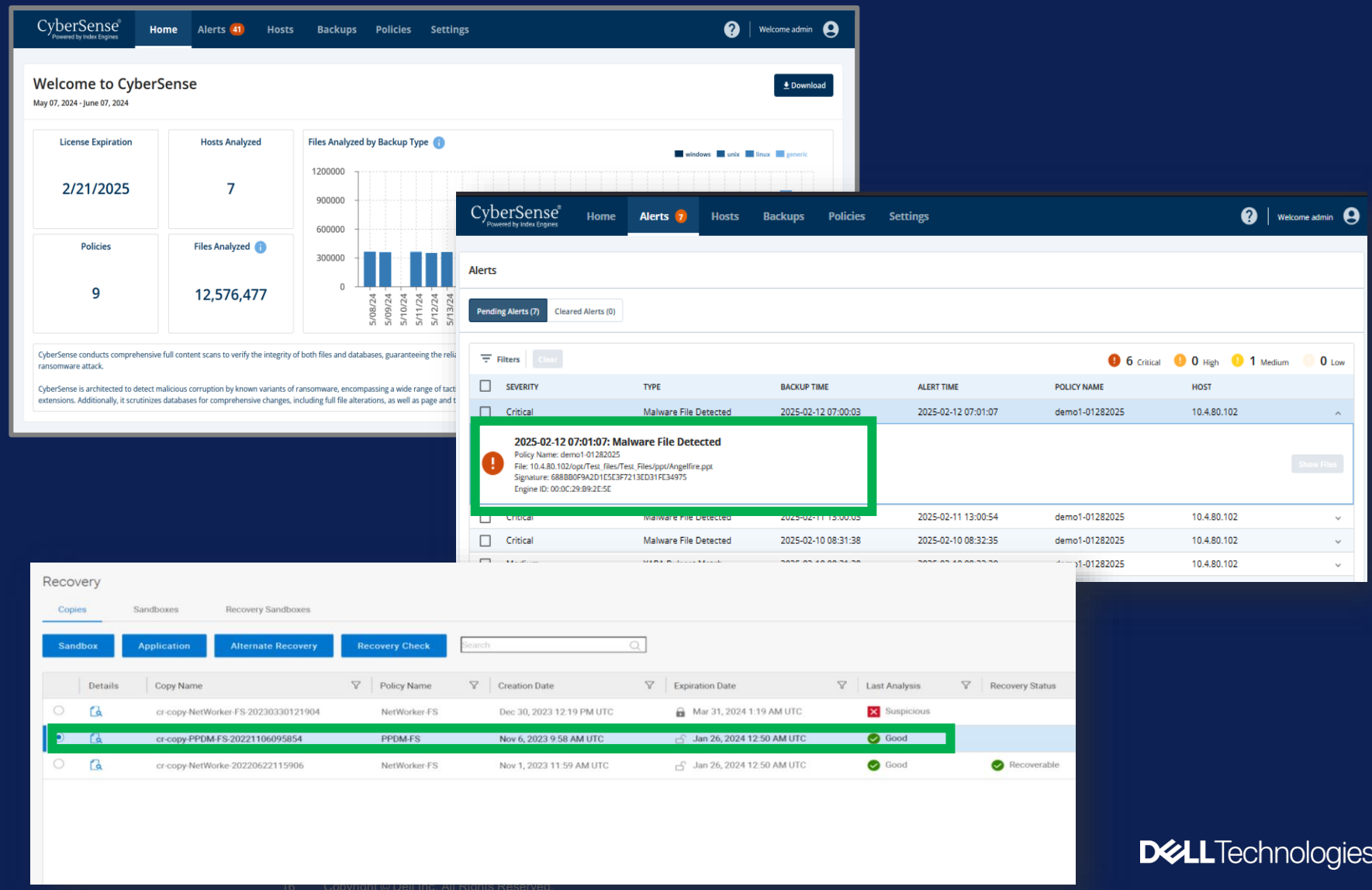
Copyright © Dell Inc. All Rights Reserved.

Recover Smarter with Cyber Detect

Simplified Dashboard for Analytics and Reporting

Dashboard View

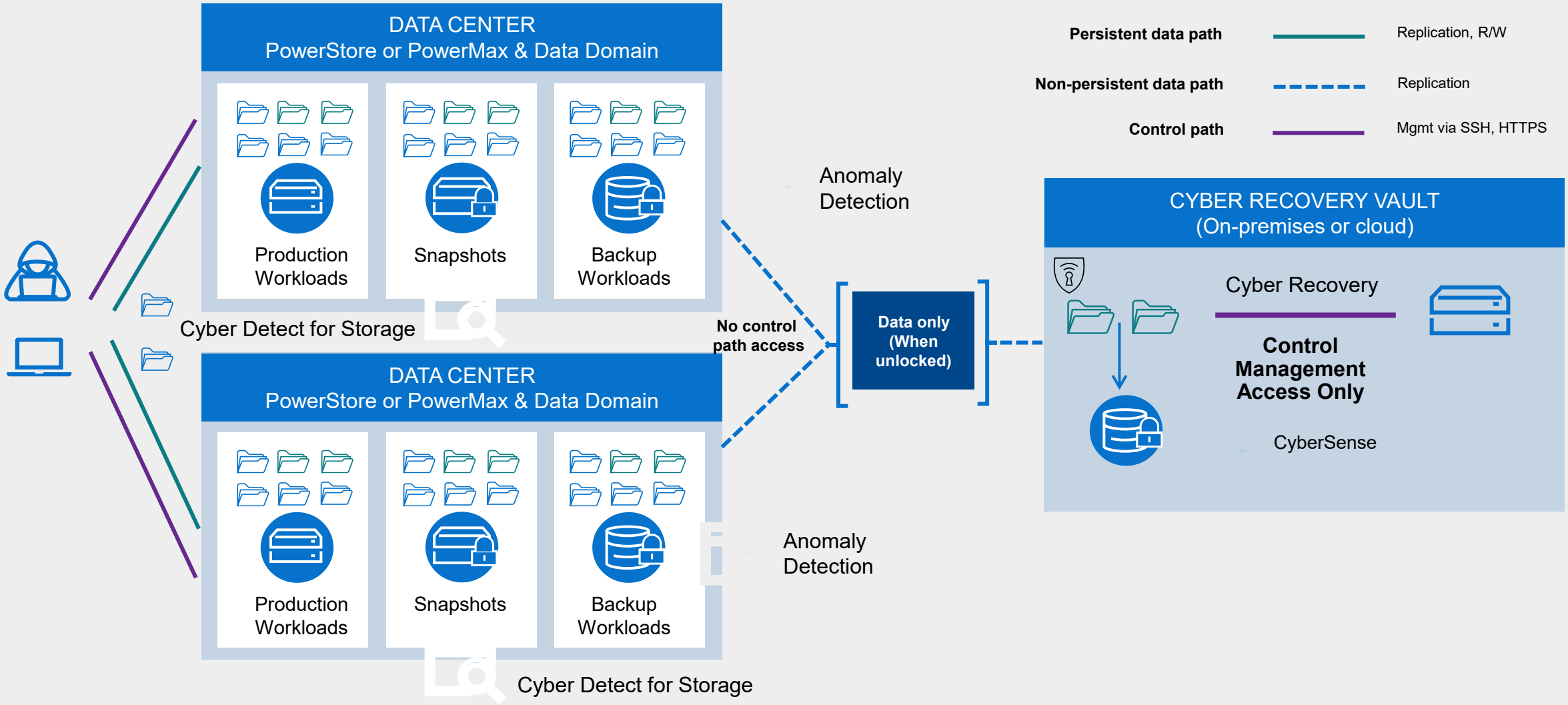
- Simple Health view of analytics environment
- Detect corruption within a backup cycle
- Investigate the Who, What, Where and When of the attack
- Quickly identify last Clean backup for recovery



Copyright © Dell Inc. All Rights Reserved.

End-to-end Cyber Resilience

A layered approach for early detection and fast, assured recovery



Copyright © Dell Inc. All Rights Reserved.

Cyber Recovery Essentials

A standardized, quickly deployable cyber recovery vault that isolates critical data, delivers predictable recovery timelines, scales modularly and maintains transparent costs and simple operations through a validated architecture.



- Protect Critical Data & Services
- Continuous Threat Detection
- Predictable Recovery Time Objective & Cost of Recovery
- Minimize Business Impact & Downtime
- Satisfy Regulation & Governing Boards

Copyright © Dell Inc. All Rights Reserved.

Dell Customer Communication - Confidential

PROVEN CYBER RECOVERY LEADERSHIP

Dell brings a decade-plus track record customers can trust

2,800+

Cyber Recovery customers worldwide trust Dell.

15+ years

A proven track record protecting and recovering customer data.

Independently accredited

Sheltered Harbor and DoD Target Level Zero Trust

When it matters most, Dell responds fast:

500+
Real businesses recovered

2 hr
response to engage

24 hr
onsite support mobilized

Decades of experience, proven at scale — customers recover with confidence.

DELL Technologies

Comprehensive Cyber Resilience Services

Swift detection, resilient response and prevail against threats.

ADVISORY, DESIGN & MANAGED SERVICES



Tailored, strategic solutions to enhance cyber resilience and safeguard your data

MANAGED DETECTION AND RESPONSE



24X7 threat detection and response to secure your cyber resilience environments

INCIDENT RESPONSE & RECOVERY SERVICES



Industry-certified security professionals to recover after a cyberattack

Additional Services capabilities

- Security & Resilience Strategic advisory
- Framework alignment assessments
- Attack Surface Reduction
- Cyber Recovery vault solutions
- Business Continuity and Disaster Recovery

Copyright © Dell Inc. All Rights Reserved.

Thank You

DELL Technologies