carahsoft

Securing the Modern Enterprise

Slide Deck

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies GSA, ITES-SW, MHEC and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Dell Technologies, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/DellResources

Join Events & Webinars:
carah.io/DellEvents

Discover Technology Solutions:
carah.io/Dell

Learn About Procurement:
carah.io/DellContracts

Connect With Our Team:
DellTechnologies@carahsoft.com
888-622-2724

Securing the Modern Datacenter

Recovery Denial, Not Just Data Theft

DELL Technologies

Copyright © Dell Inc. All Rights Reserved.

The Anatomy of an Attack

Finance & Banking
Top 20 Global Bank

2024 · Global Banking Operations Disrupted

Who Was Affected

- Top 20 Global Bank — Operating across 9 core markets in Europe and the Americas through five global businesses
- Annual revenue (2025): $85 billion
- Asset holdings around $2.11 trillion as of Dec. 2025

Attack Vector

Third-party contractor laptop compromised — attacker compromised the edge device and gained access the network as the device was connected to the bank over a VPN connection. This connection allowed them to gain an initial foothold and establish persistence.

What Was Targeted

- Active Directory compromised and Domain Admin level control established
- ~1,400 VM and database workloads representing ~1.5PB of data were encrypted in 37 minutes
- Backup infrastructure was compromised and catalogue destroyed

Operational Impact

- Lack of planning and preparation resulted in two days lost while deciding what to recover first
- Complete rebuild of infrastructure required
- 21 days to get minimally viable business (MVB) services back online

Recovery & Cost

- Incident was not disclosed publicly
- Total business and financial impact not reported

DELL Technologies

Copyright © Dell Inc. All Rights Reserved.

01

The Evolving Threat Landscape

How the attack playbook has changed — from ransomware to recovery denial, and how AI is compressing the timelines for everyone.

Copyright © Dell Inc. All Rights Reserved.

From "Encrypt & Extort" to Recovery Denial

Mandiant M-Trends 2026: attackers now deliberately destroy your ability to recover, not just encrypt your data.

Backup Infrastructure

- Primary target — not afterthought
- Corrupted or destroyed pre-encryption
- 2-in-3 incidents: backups compromised

Identity Services

- Domain admin access obtained first
- Removes recovery options
- Enables persistence across wipes

Virtualization Planes

- ESXi & AHV targeted directly
- Entire virtual clusters encrypted
- Not just guest OSes — the hypervisor

Edge Device Entry

- VPNs & firewalls: #1 vector (6th year)
- Email phishing dropped to ~6%
- Unpatched edge = open front door

Speed of Escalation

- Hours from entry to backup targeting
- Dwell time compressing — less time to detect
- Recovery infrastructure hit before defenders respond

Source: Mandiant M-Trends 2026 · CISA · Verizon DBIR 2025

DELL Technologies

Copyright © Dell Inc. All Rights Reserved.

Claude Mythos: A New Category of Threat

The AI Inflection Point · April 2026

73%

success rate on expert-level cybersecurity tasks — tasks no AI could complete before 2025

1ST

First AI to complete a 32-step full corporate network takeover — autonomously

Superhuman Autonomous Hacking

Finds weaknesses, chains them, and helps generate working exploits with minimal expert guidance — agent-like workflows, not simple Q&A.

Thousands of Zero-Days Discovered

Found thousands of previously unknown high-severity vulnerabilities in major operating systems and browsers — including bugs over two decades old that survived prior automated scanning.

Gated Behind Project Glasswing

Not released publicly. Gated behind Project Glasswing — shared with 40+ vetted critical-infrastructure and security partners to fix vulnerabilities before attackers exploit the same capabilities.

AI-Orchestrated Attacks Are Now Expected

Analysts and governments now expect AI systems to plan and coordinate intrusions — not just assist human operators. Espionage and sabotage campaigns targeting identity and control planes are the anticipated next step.

Sources: Anthropic Project Glasswing · UK AI Security Institute (AISI) Evaluation · Council on Foreign Relations · Bain & Company · April 2026

Copyright © Dell Inc. All Rights Reserved.

02

Lessons Learned

What the evidence tells us about where conventional defenses fall short — and why isolation is no longer optional.

Copyright © Dell Inc. All Rights Reserved.

Key Lessons Learned from Cyber Attacks

Why Recovery Takes Longer Than It Should

Lack of IR Plan

No playbook forces panicked decisions when stakes are highest.

Recovery Untested

Assumed-clean backups fail on their first real test mid-crisis.

Containment Failures

Unclear perimeter makes it hard to know where to cut access.

Missing Runbooks

Teams rebuild from memory; missing dependencies surface mid-restoration.

Comms Breakdown

No resilient comms plan; poor communication slows response.

Paths Abandoned

Ransom paid while a viable recovery path sits unvalidated.

No IR Partners

No retainers or SLAs; partners are scrambled mid-crisis.

Lack of Clean Infrastructure

Building a recovery target mid-crisis adds days to recovery.

Lapsed Support Agreements

Lapsed contracts mean no vendor priority when it counts.

EOL Infrastructure

Legacy systems need specialists; no vendor recovery path exists.

Planning gaps hit first and hardest

No IR plan and untested recovery dominate time-to-containment.

Operational gaps compound the timeline

Abandoned paths and siloed comms add weeks even with good backups.

Infrastructure gaps can't be solved mid-incident

Clean environments, contracts and partners must exist before the attack.

DELL Technologies

Copyright © Dell Inc. All Rights Reserved.

The Five Ingredients for Recovery

Recovery has no EASY BUTTON. Every organization that has survived a major cyber attack has navigated these five steps — in sequence, under pressure. There are no shortcuts.

01

Prioritize Critical Services

Minimum Viable Company

Map your most critical business services to their applications, infrastructure dependencies, and client access paths. You cannot recover everything at once.

02

Viable Recovery Source

Confirm a Clean Copy Exists

Identify at least one recovery source confirmed to be free from compromise. More sources give options — but each must be validated before use.

03

Viable Recovery Target

Build a Safe Target Environment

Provision clean infrastructure to restore into. This step demands multiple teams working in parallel — network, identity, compute, and storage.

04

Verify Clean Recovery

Confirm No Residual Threat

Validate recovered items are free from compromise, attack replay, or mechanisms of persistence.

05

Return To Service

Reconnect Users to Services

Business recovery is not achieved until services are live and connected to their users. Functional testing and staged re-entry complete the cycle.

These five steps cannot be skipped or reordered. Every day of delay in completing them is another day your business is not operating at full capacity.

DELL Technologies

Copyright © Dell Inc. All Rights Reserved.

03

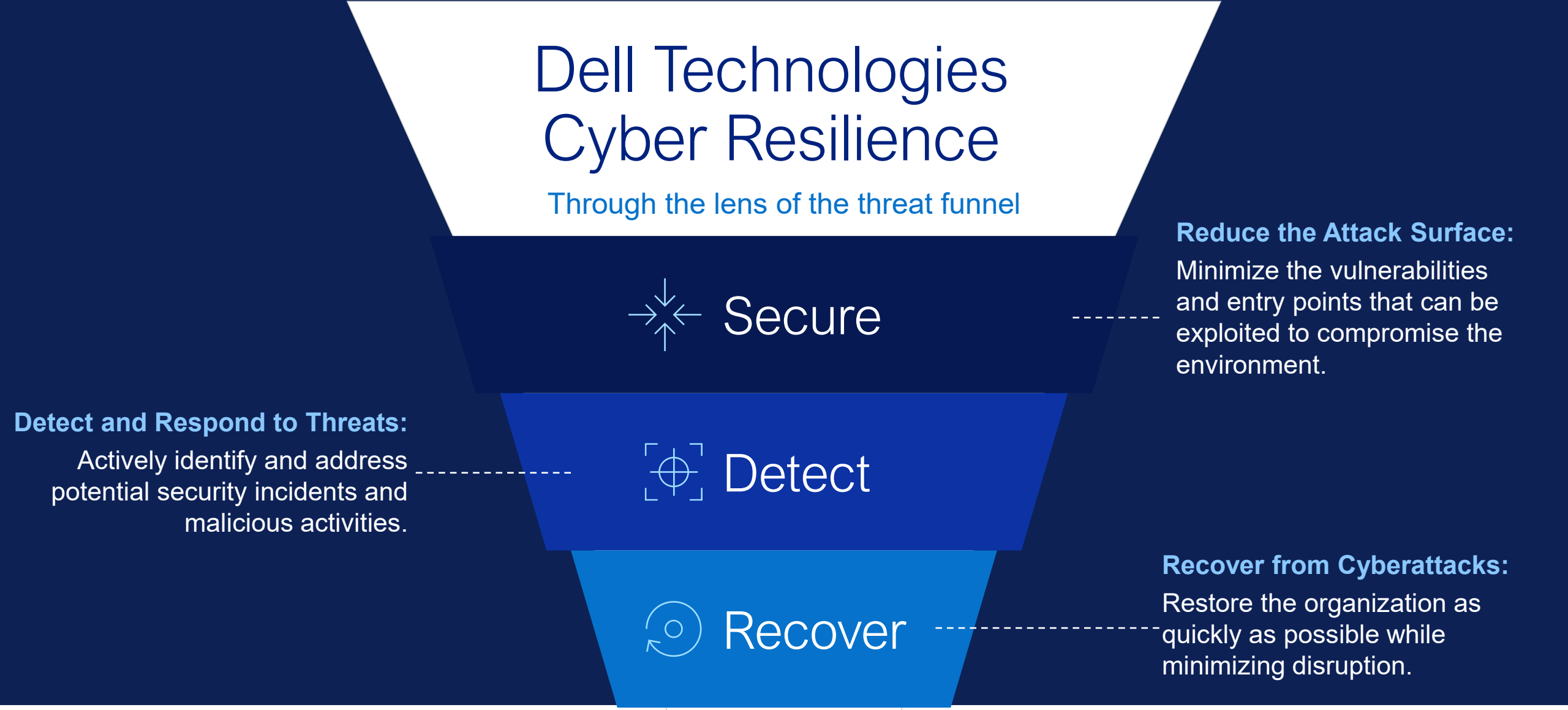
Building Resilience

Practical steps, a layered technical framework, and a maturity journey — grounded in how leading organizations are responding.

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.

Secure

Reduce the Attack Surface

Minimize the vulnerabilities and entry points that can be exploited to compromise the environment

- SECURE SUPPLY CHAIN
- ZERO TRUST MATURITY
- IMMUTABILITY
- OBSERVABILITY

"The right technology is critical because our reputation is on the line. Customer data is our key asset. The Dell PowerProtect portfolio ensures it's protected."

— RHB Banking Group

RHB

DELL Technologies

Copyright © Dell Inc. All Rights Reserved.

Detect

Detect and Respond to Threats

Actively identify and address potential security incidents and malicious activities

- THREAT MANAGEMENT
- ANOMALY DETECTION
- PROACTIVE MONITORING

We knew we needed to improve our security posture. Dell Managed Detection and Response gets the job done without additional headcount.

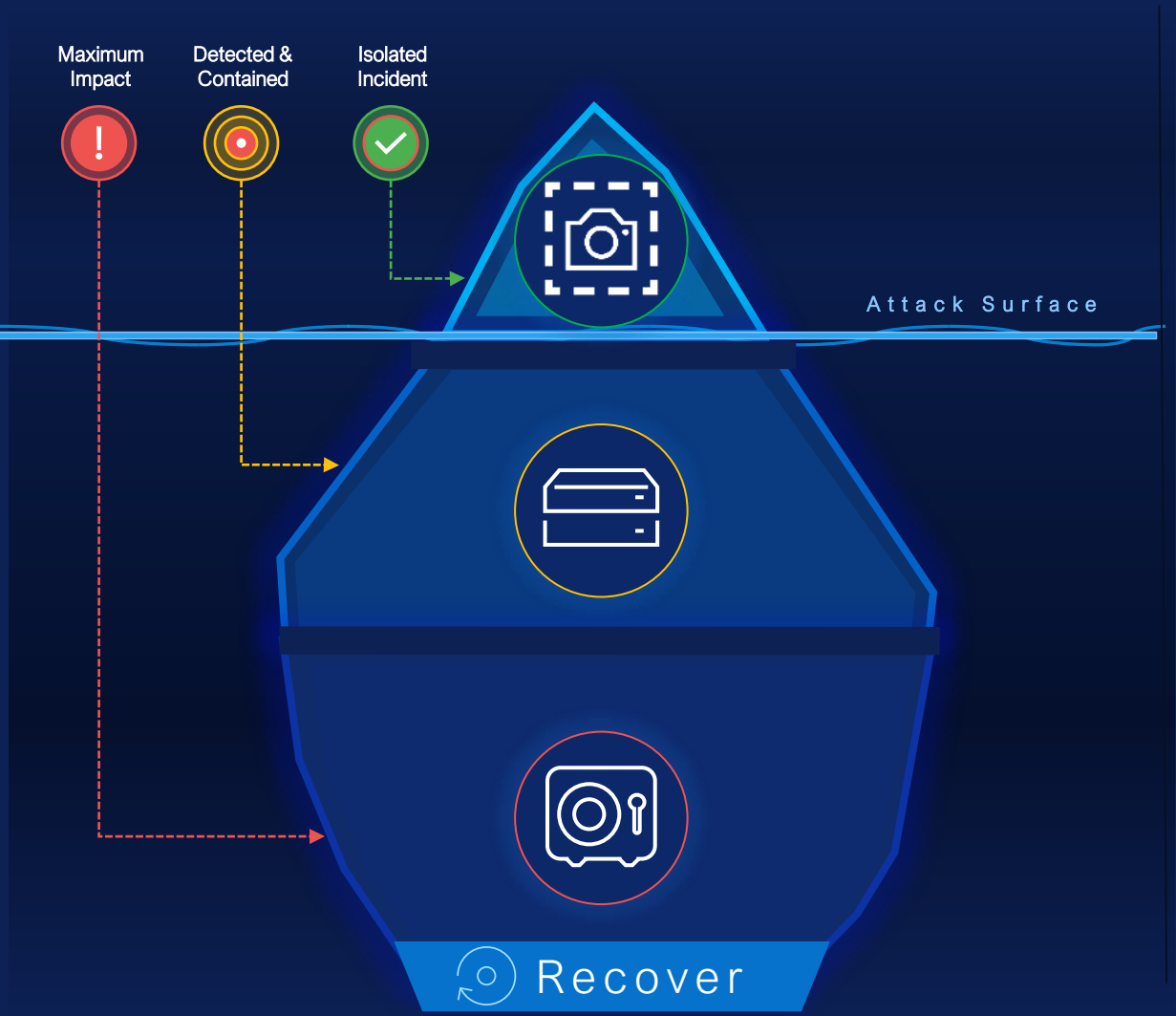
— Director of Information Systems, Large Southwestern U.S. County

DELL Technologies

Copyright © Dell Inc. All Rights Reserved.

Recover – A Layered Approach to Cyber Resilience

A layered recovery strategy gives you flexible options to balance recovery speed and assurance, so you can reliably restore from cyber attacks of any scale.



Layer 1 – Primary Storage Layer

Secure Snapshots

Restore Speed	Recovery Confidence
Fast	Lower

- On-array, immutable snapshots
- Fastest path back to production
- Validate snapshot integrity before restore

Layer 2 – Backup Resilience Layer

Protected Backups

Restore Speed	Recovery Confidence
Moderate	Medium

- Immutable, encrypted backups off primary array
- Hardened platform: access controls, MFA, threat monitoring
- Post-containment restores with higher confidence

Layer 3 – Cyber Vault Layer

Isolated Recovery Area

Restore Speed	Recovery Confidence
Deliberate	Highest

- Isolated network, identity and operations
- Cyber analytics pre-validated recovery points
- Fast, highest-assurance recovery for worst-case attacks

Copyright © Dell Inc. All Rights Reserved.

Why Dell Technologies for Your Cyber Resilience Journey

Comprehensive Cyber Resilience

Beyond point backup — complete coverage across supply chain, endpoints, core, edge, cloud, mainframe, and OT/ICS.

Proven Experience & Outcomes

Thousands of cyber recovery engagements. Dedicated teams. NIST, ISO, and sector-aligned reference architectures.

A Trusted Resilience Partner

We deliver outcomes, not just products. Strategy workshops, runbook design, recovery testing, managed services and ongoing governance.

Flexible Consumption

Own it, subscribe, or let us run it. Dell Managed Services operates your entire resilience program as a service.

Supply Chain Confidence

When recovery speed matters, Dell delivers. Hardware in days, not months — when the industry faces backlogs, we ship.

DELL Technologies

Copyright © Dell Inc. All Rights Reserved.

Dell PowerProtect Updates

Copyright © Dell Inc. All Rights Reserved.

Introducing…

PowerProtect One

Delivers both open ecosystem support and integrated management

Protect every workload, across vendors, under one resilience framework

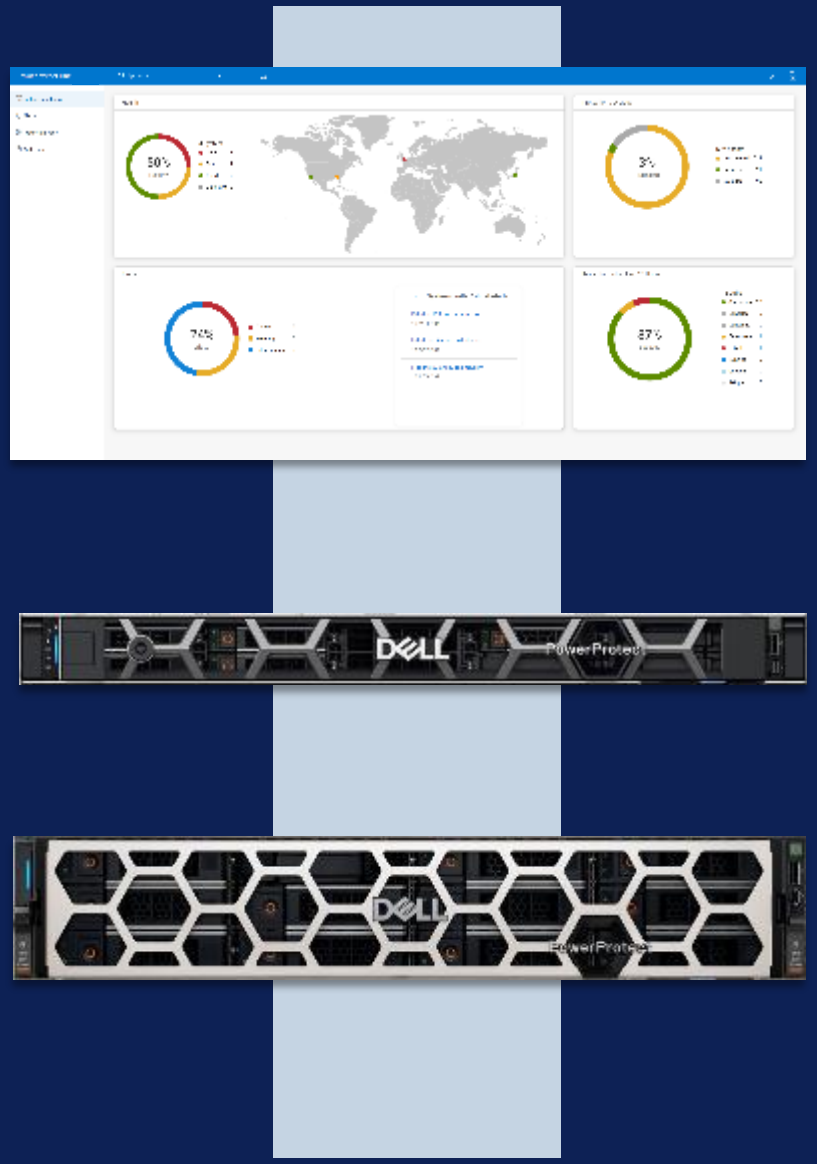
Orchestrate protection and recovery across your environment

Secure, efficient, high-performance storage that stands between your data and cyber threats

Copyright © Dell Inc. All Rights Reserved.

PowerProtect One

Open and Integrated architecture



Unified experience

Single management console and orchestrated operations for the entire protection stack

Modern protection

Intelligent protection for modern workloads on optimized hardware

Resilient storage

Highly efficient, secure storage, scalable up to 256TB today, support for all DD models this year

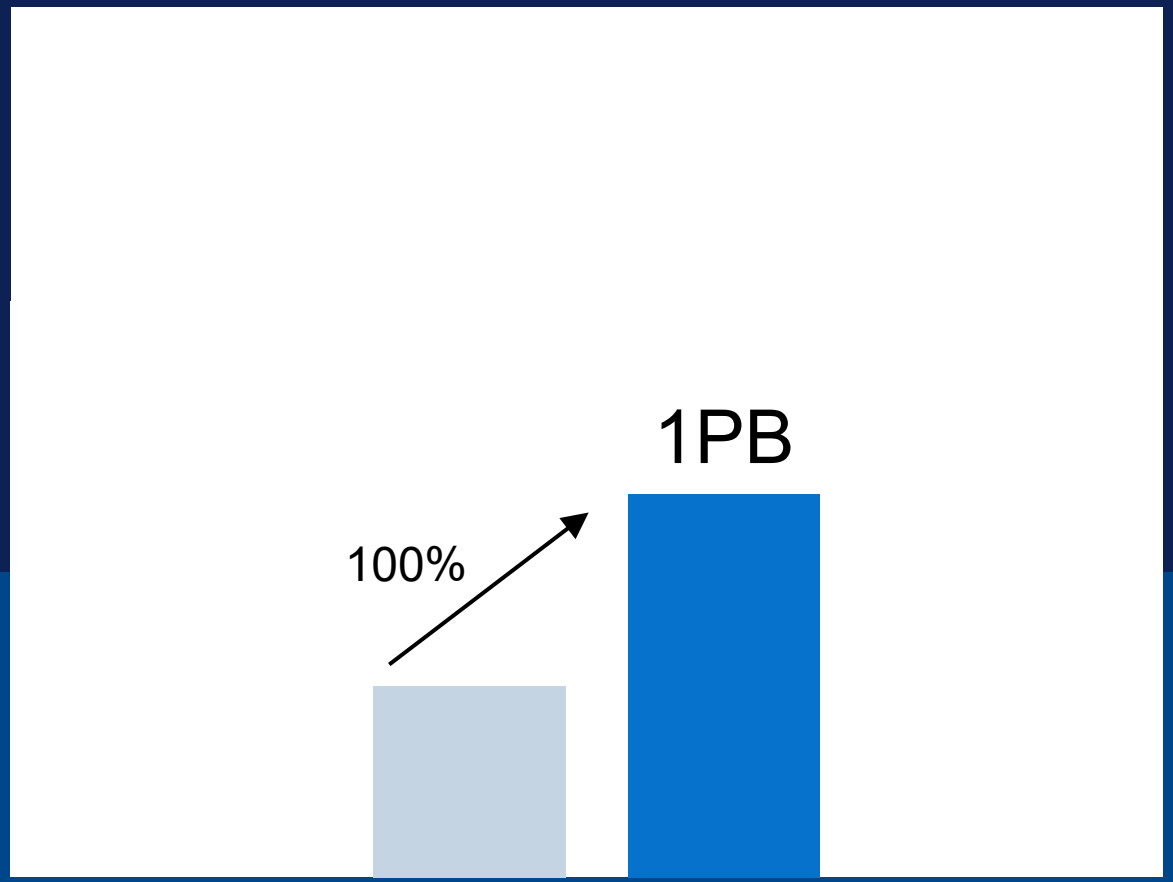
One solution to deploy, operate, upgrade and support

COMMVAULT VEEAM HYCU

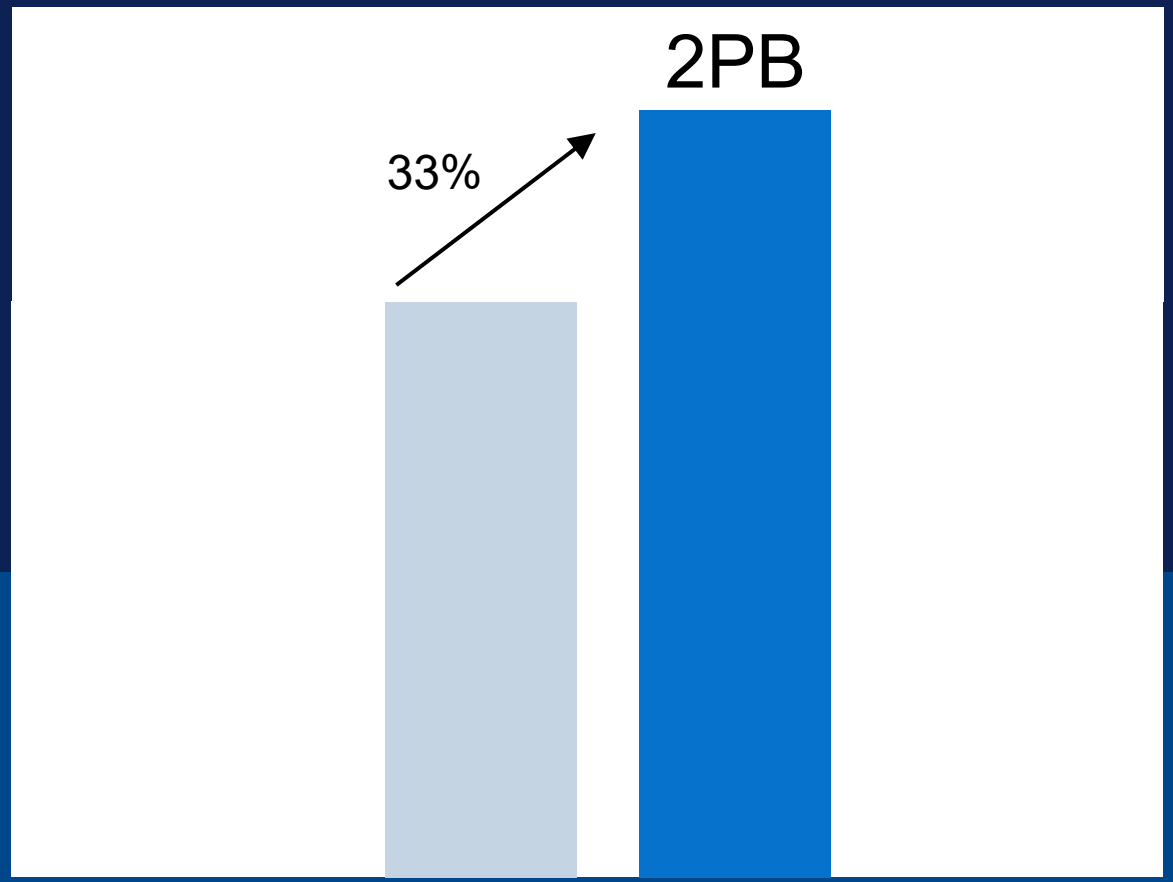
DELL Technologies

Copyright © Dell Inc. All Rights Reserved.

PowerProtect DD: Improved Enterprise Scalability



DD9910F
(All-Flash)



DD9910

Copyright © Dell Inc. All Rights Reserved.

AI-Powered Threat Detection

Continuously trained AI engine identifies corruption patterns with unmatched accuracy

Coverage Across Infrastructure

Trained on Real Ransomware

Line-Speed Data Scanning

Rigorous Validation

Full Content-Based Analytics

AI-Powered Engine

Dell Cyber Detect

*Validates data integrity & identify clean recovery points with **99.99%** SLA*

Confidence in Data Integrity

✓ **End-to-End Data Validation**

Detects ransomware behaviors across files, databases, and raw disk while distinguishing malicious activity from normal operations.

✓ **Advanced Encryption Detection**

Detects corruption from shadow encryption, slow encryption, polymorphic ransomware, and more.

✓ **Zero-Day Variant Detection**

Analyzes the full content of data over time to spot data corruption from even new, unknown variants.

✓ **Raw Disk Corruption Detection**

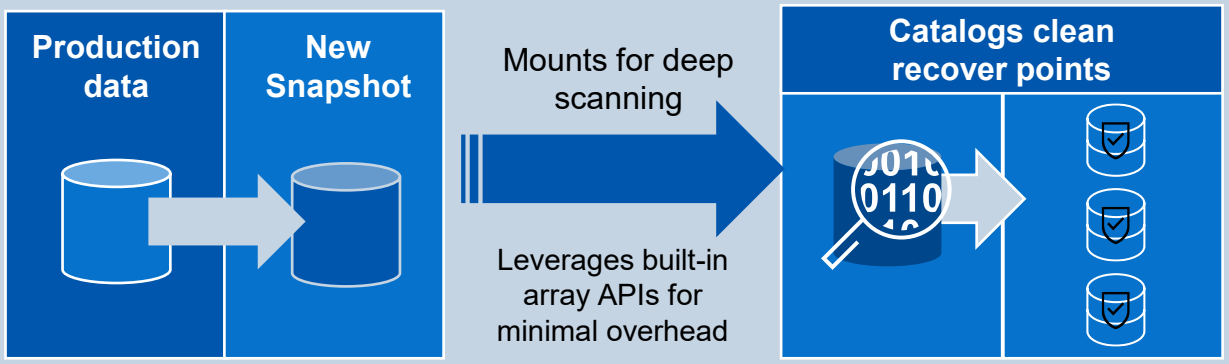
Detect raw disk attacks on virtual machines, identifying hidden ransomware that creates the appearance of empty or faulty storage.

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*

Cyber Detect
(VM 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

*PowerMax Cyber Detect availability planned for 2H, FY2026

Copyright © Dell Inc. All Rights Reserved.

DELL Technologies