

Dell Cyber Detect

AI-Powered Detection to Ensure Data Integrity and Enable Rapid Recovery

Validate and recover mission-critical data faster with Dell Cyber Detect

- **Next-Generation Resilience:** AI-powered learning and deep analytics delivers advanced protection against evolving ransomware.
- **Trusted Data Integrity:** Cyber Detect identifies corruption with 99.99% accuracy*, ensuring recovery points are clean and dependable.
- **Rapid Recovery:** When an attack strikes, clean recovery points and forensic reporting are immediately available, reducing risk of extended downtime and business impact.

Modern cybercriminals are relentless, and today's ransomware is engineered to evade traditional detection. Increasingly sophisticated techniques like shadow encryption deploy subtle, byte-level corruption of data to bypass common indicators and controls that most defenses rely upon.

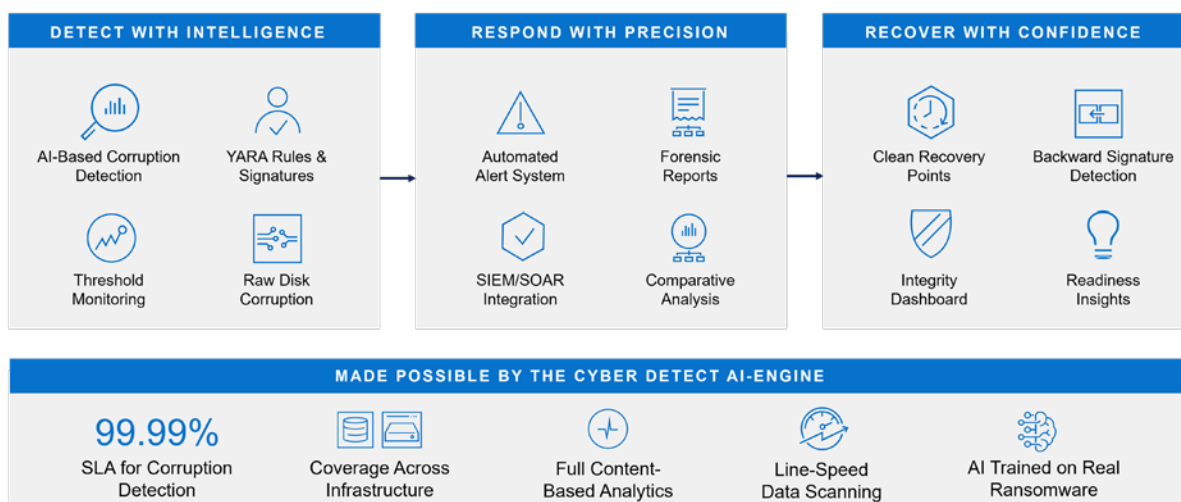
The result is a bigger downstream problem: ransomware is no longer just difficult to prevent. Once ransomware is in, it becomes extremely difficult to prove which data is clean and which is infected. That uncertainty is what turns a recovery into a high-risk, drawn-out effort.

To keep the business running, organizations need to validate the integrity of their data as close to the source as possible. In doing so, they can restore from the **most recent clean copy**, minimizing their risk of extended downtime and data loss.

Dell Cyber Detect validates the integrity of your critical data to ensure intelligent recovery from ransomware corruption. Unlike traditional tools that rely on surface-level indicators like metadata analysis, threat signatures, or file activity thresholds, Cyber Detect analyzes the actual content of files and databases to detect corruption caused by ransomware. Using AI trained through a patented process on thousands of real-world ransomware variants, it analyzes 200+ content-based statistics to deliver 99.99%¹ accuracy in validating data integrity. By creating an end-to-end detection strategy across both primary storage and backup environments, businesses can rely on Cyber Detect to spot corruption early and identify the last clean copy of data, so they can confidently recover their mission-critical workloads after an attack.

Advanced Capabilities for Trusted Data Recovery

Detect, respond, and recover faster from ransomware corruption



¹ Based on an ESG report commissioned by Index Engines, "Index Engines' CyberSense Validated 99.99% Effective in Detecting Ransomware Corruption". June 2024. Actual results may vary.

Fast Detection and Confident Recovery for Dell Storage

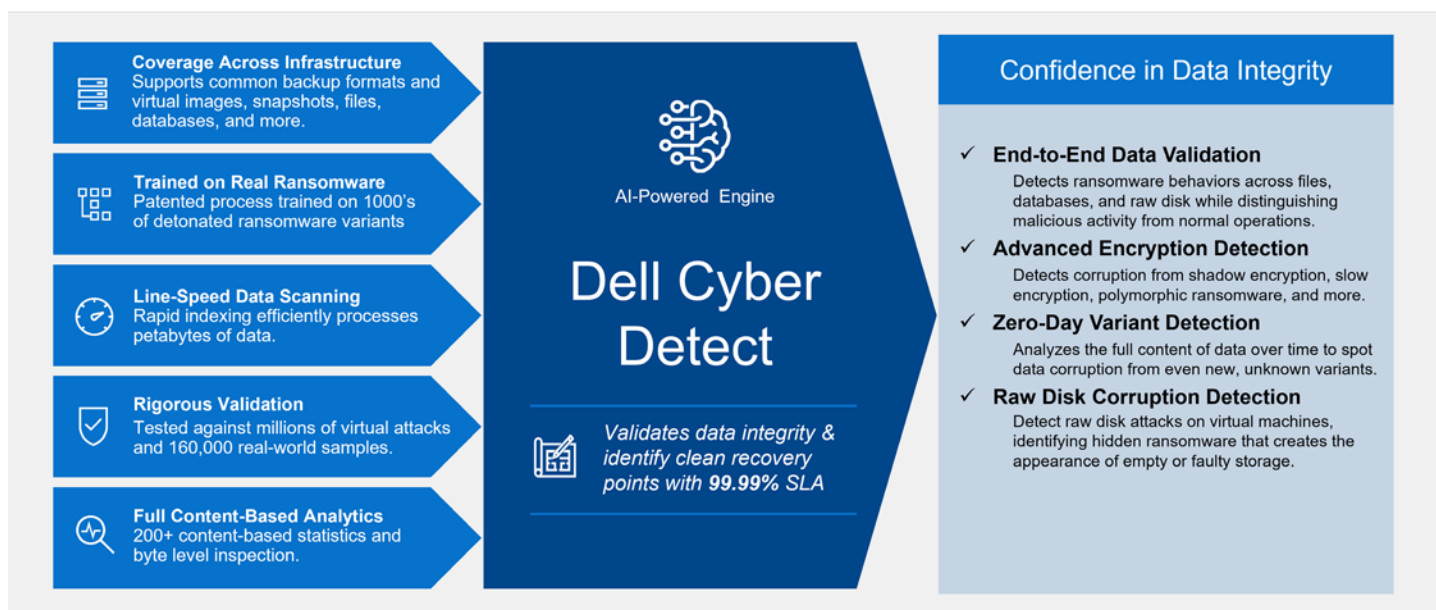
Cyber Detect for Storage is deployed on a dedicated server within the same datacenter as your PowerStore or PowerMax² systems. Once connected, administrators can easily configure snapshot schedules through the Cyber Detect management interface. The software then takes actions leveraging built-in array APIs to create snapshots which are then mounted to the Cyber Detect server and thoroughly scanned with powerful AI-driven inspection. This tightly integrated approach simplifies security operations by leveraging the advanced snapshot capabilities of Dell's primary storage arrays, all within a single, streamlined interface. This results in snapshots that are verified and clean, enabling you to confidently recover directly on your primary storage, significantly improving RTO.

Maximum control and security with layered protection for Dell PowerProtect

CyberSense for PowerProtect Cyber Recovery actively monitors files and databases. Once data is replicated to the Cyber Recovery vault and retention lock is applied, CyberSense then automatically initiates a comprehensive scan of the backup data, creating point-in-time observations of files, databases, and core infrastructure. CyberSense meticulously tracks changes in files over time, effectively uncovering data corruption by even the most sophisticated of cyber threats.

Advanced AI-Powered Machine Learning

Continuously trained AI engine identifies corruption patterns with unmatched accuracy



The Cyber Detect Advantage

Dell Cyber Detect is ideal for enterprises seeking ransomware corruption detection and rapid recovery for their Dell infrastructure. It provides the AI-powered analytics needed to detect corruption early and ensure clean, dependable recovery points for your most critical applications.

Key Capabilities:

AI-Driven Detection

Cyber Detect's AI models are trained on over 7,000 ransomware variants and millions of real-world datasets in a dedicated lab using a patented process that detonates real ransomware. This enables Cyber Detect to perform deep, detailed inspections at the byte level, analyzing how data changes over time to accurately identify ransomware corruption and detect even the most subtle signs of an attack.

- Detects mass deletions, encryption, corruption, and other suspicious changes.
- Analyzes over 200 content-based statistics per host/volume for unmatched precision.

² PowerMax Cyber Detect availability planned for 2H, FY2026

Fast, Localized Recovery for Critical Data

Cyber Detect for Storage scans data directly on the PowerStore and PowerMax arrays, ensuring recovery points are quickly accessible for the applications that drive your business. Unlike other solutions, it delivers deep, detailed inspections with advanced capabilities like page-level analysis of databases and support for virtual machines. These features enable unmatched precision in detecting corruption, making it ideal for today's complex IT environments. Core Infrastructure: Active Directory, DNS, LDAP

- Databases: Oracle, DB2, SQL, PostgreSQL, Epic Caché
- Unstructured Data: Documents, contracts, intellectual property, file repositories

Trusted Data Integrity

Cyber Detect continuously scans and analyzes data to ensure only clean, uncompromised files are used for recovery. Recovery points and reporting are readily available with every scan giving you confidence in your ability to restore critical data before an attack occurs.

- Pinpoints the last known clean backup or snapshot for fast restoration.
- Identifies specific files impacted by an attack for surgical recovery.
- Provides detailed assessments and telemetry for your SIEM/SOAR systems to help prevent future attacks.

End-to-End Cyber Resiliency

True resilience requires a unified, multi-layered defense. Cyber Detect is available to protect primary data while CyberSense for PowerProtect Cyber Recovery is available for backup data, creating a robust strategy that storage-only vendors cannot match.

- Cyber Detect for Storage: Quickly identify the last clean copy of data directly on Dell PowerStore and PowerMax arrays to minimize downtime for critical applications.
- CyberSense for PowerProtect Cyber Recovery: Create a comprehensive defense strategy by analyzing data within the PowerProtect Cyber Recovery Vault. CyberSense scans backup images from Dell and third-party solutions without needing to rehydrate the data.

Transform Your Recovery Strategy with Dell

Don't let the threat of ransomware dictate your business continuity. With Dell Cyber Detect, you can transform your recovery strategy from reactive to resilient. Empower your organization to detect, respond, and recover from cyberattacks with speed and confidence.



Contact your Connection Account Team for more information.

Business Solutions
1.800.800.0014

Enterprise Solutions
1.800.369.1047

Public Sector Solutions
1.800.800.0019

www.connection.com/dell-storage-solutions

Copyright © Dell Inc. All Rights Reserved. Dell Technologies, Dell and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.