DELL Technologies

Solution Brief

CyberSense® for Dell PowerProtect Cyber Recovery

AI-Powered Analytics and Forensic Tools to Detect, Diagnose, and Recover Smarter from Cyberattacks

THE CYBERSENSE ADVANTAGE

CyberSense® is fully integrated with the Dell PowerProtect Cyber Recovery vault solution.

- Automates regular scanning of backup data to validate data integrity and alert when suspicious behavior is detected.
- Directly scan content within backup images from Dell Avamar, NetWorker, Commvault, NetBackup, and PowerProtect Data Manager without the need to rehydrate the data.
- Delivers deep full-content analysis with every scan of data to detect even the most sophisticated ransomware attacks.
- Custom alerts for YARA rules and malware signatures to detect known behavior from ransomware or internal bad actors.
- Facilitate a smarter and faster recovery with post-attack forensic reports to gain detailed insights into the depth and breadth of the attack and provides a listing of the last good backup sets before corruption.

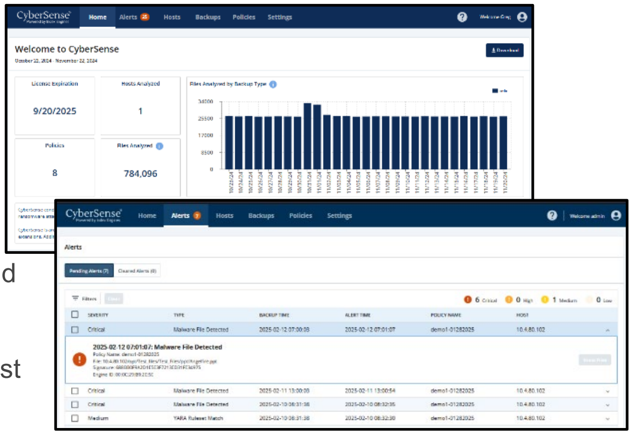
CyberSense stands apart from other data analytic approaches and provides a higher level of confidence that backup data has integrity and can be quickly recovered after an attack occurs.

As the frequency of cyberattacks continue to rise and cyber criminals become more resilient, conventional security tools fall short in safeguarding data against cyberattacks.

CyberSense® steps in to detect data corruption after an attack with 99.99% accuracy*and facilitates intelligent and rapid restoration. Serving as the first line of recovery for thousands of organizations worldwide, CyberSense ensures the integrity of data assets, including core infrastructure, databases, and critical documents, instilling confidence that the data is clean from malicious corruption.

CyberSense scans data backups in a Cyber Recovery vault to observe how data changes over time. It then utilizes machine learning and AI to detect signs of corruption indicative of a ransomware attack. Data is compared with 200+ content-based analytics to identify corruption with 99.99% confidence*, helping you protect your business-critical infrastructure and content. CyberSense detects mass deletions, encryption, and other suspicious changes in core infrastructure (including Active Directory, DNS, etc.), file repositories, file systems, and critical databases resulting from sophisticated attacks.

When suspicious behavior occurs, CyberSense provides post-attack forensic reports to diagnose the blast radius of the cyberattack. When data corruption is detected, a listing of the last known good backup data sets is available to support rapid curated recoveries that help minimize business interruption and data loss—lowering the cost of cyber recovery.



Welcome to CyberSense

October 22, 2024 - November 22, 2024

License Expiration: 9/20/2025

Hosts Analyzed: 1

Policies: 8

Files Analyzed: 784,096

Alerts

SEVERITY	TYPE	BACKUP TIME	ALERT TIME	POLICY NAME	HOST
Critical	Malware File Detected	2025-02-12 07:00:03	2025-02-12 07:01:07	demo1-01282025	10.4.80.102
Critical	Malware File Detected	2025-02-11 13:00:03	2025-02-11 13:00:54	demo1-01282025	10.4.80.102
Critical	Malware File Detected	2025-02-10 08:31:38	2025-02-10 08:32:35	demo1-01282025	10.4.80.102
Medium	YARA Ruleset Match	2025-02-10 08:31:38	2025-02-10 08:32:30	demo1-01282025	10.4.80.102

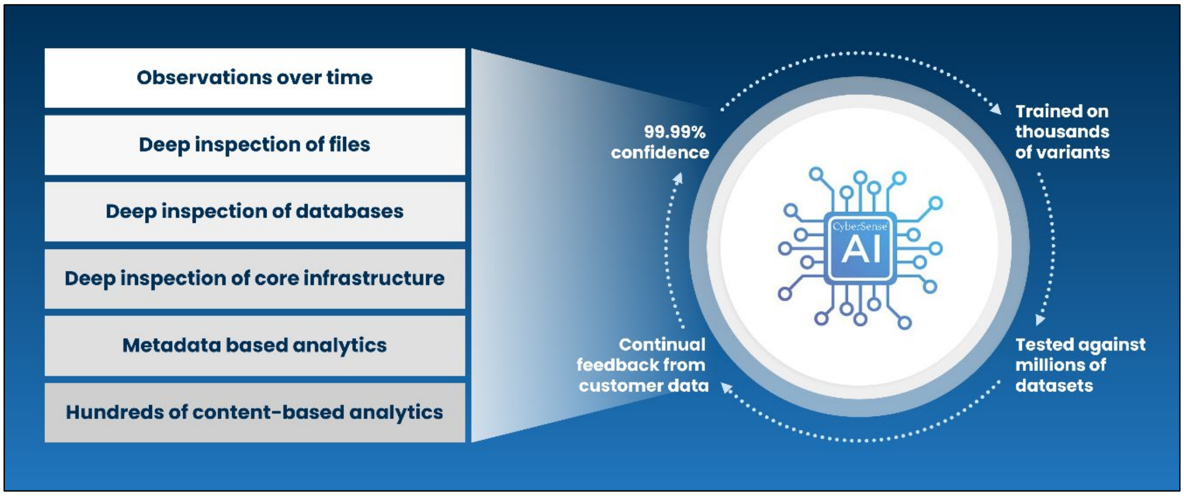
2025-02-12 07:01:07: Malware File Detected

The Cyber Recovery Workflow

CyberSense seamlessly integrates with Dell PowerProtect Cyber Recovery, actively monitoring files and databases to detect ransomware corruption by analyzing the integrity of the data. Once data is replicated to the Cyber Recovery vault and retention lock is applied, CyberSense 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.

Full Content Analytics

CyberSense is the only product on the market that delivers full-content-indexing and analysis on all protected data. CyberSense deep AI analysis runs across the entirety of data and a probabilistic decision is generated with 99.99% accuracy* as to whether the data has integrity or whether it has been corrupted by ransomware. This capability sets CyberSense apart from other solutions that take a high-level view of the data and use analytics that look for obvious signs of corruption based on metadata. Metadata-level corruption is not difficult to detect; for instance, changing a file extension to .encrypted or radically changing the file size. These types of attacks do not represent the sophisticated attacks that cybercriminals are using today.


Observations over time
Deep inspection of files
Deep inspection of databases
Deep inspection of core infrastructure
Metadata based analytics
Hundreds of content-based analytics
99.99% confidence
Trained on thousands of variants
CyberSense
AI
Tested against millions of datasets
Continual feedback from customer data

CyberSense goes beyond metadata-only solutions and detects data corruption using full-content analytics. It audits files and databases for changes indicative of an attack, including full or partial file corruption. Traditional analytics miss these threats, leading to false confidence. Custom threshold alerts can be set based on changes in files, added files, or deleted files. Custom YARA rules and malware signatures can also be implemented for both forward and backward detection of malware in backups.

Supported Data Types

CyberSense generates analytics from a comprehensive range of data types. This includes core infrastructure such as DNS, LDAP, Active Directory, unstructured files such as documents, contracts, intellectual property, and databases including Oracle, DB2, SQL, PostgreSQL, Epic Caché, etc.

Summary

Fully integrated with Dell PowerProtect Cyber Recovery, CyberSense analyzes your vault data and detects behavioral indicators of compromise and corruption. CyberSense empowers you to proactively understand the blast radius of a cyberattack in motion, facilitate the implementation of a plan to swiftly diagnose and recover, to mitigate business interruption and associated significant costs.

Learn more about Dell PowerProtect Cyber Recovery

Contact a Dell Technologies Expert

Learn more about CyberSense

Join the conversation with #PowerProtect

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