Solution Brief

# CyberSense® for PowerProtect Cyber Recovery

AI-based Machine Learning, Analytics, and Forensic Tools to Detect, Diagnose, and Recover from Cyberattacks

## THE CYBERSENSE ADVANTAGE

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

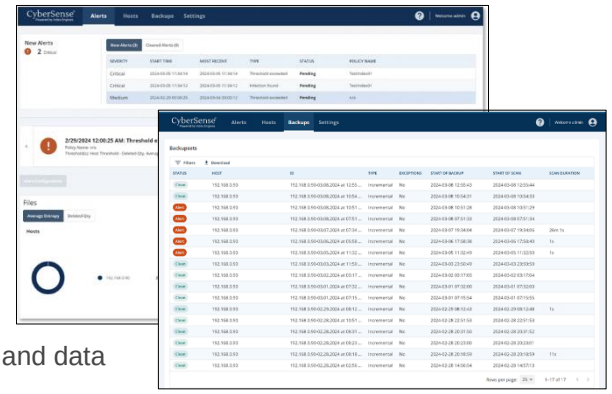
- This integration allows for an automated approach towards regular scanning of backup data to validate the data's integrity and alert when suspicious behavior is detected.
- CyberSense's ability to directly scan inside backup images, including Dell NetWorker, Avamar, PowerProtect Data Manager, and more, allows for content to be analyzed without the need to rehydrate the data.
- Only CyberSense delivers full-content analytics with every scan of the data to detect even the most sophisticated ransomware attacks that can easily go undetected by lightweight scanning tools that only inspect metadata.
- When an attack occurs, CyberSense provides post-attack forensic reports to understand the depth and breadth of the attack and provides a listing of the last good backup sets before corruption to facilitate the recovery process.

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

When conventional security tools fall short in safeguarding data against cyberattacks, **CyberSense®** steps in to detect data corruption after an attack with 99.5% accuracy and facilitates intelligent and rapid restoration. Serving as the last line of defense and first line of recovery for thousands of organizations worldwide, CyberSense ensure the integrity of their data assets, including core infrastructure, production databases, and critical documents, instilling confidence that the data is clean from malicious corruption.

CyberSense leverages data backups to observe how data changes over time and then utilizes AI-based machine learning to detect signs of corruption indicative of a ransomware attack. Machine learning then examines these 200+ content-based analytics to find corruption with 99.5% 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.), user files, and critical production databases resulting from sophisticated attacks. If CyberSense detects signs of corruption, an alert is generated in the dashboard with additional information that details the scale and impact of the attack.

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 a rapid curated recovery that helps to minimize business interruption and data loss.



### The Cyber Recovery Workflow

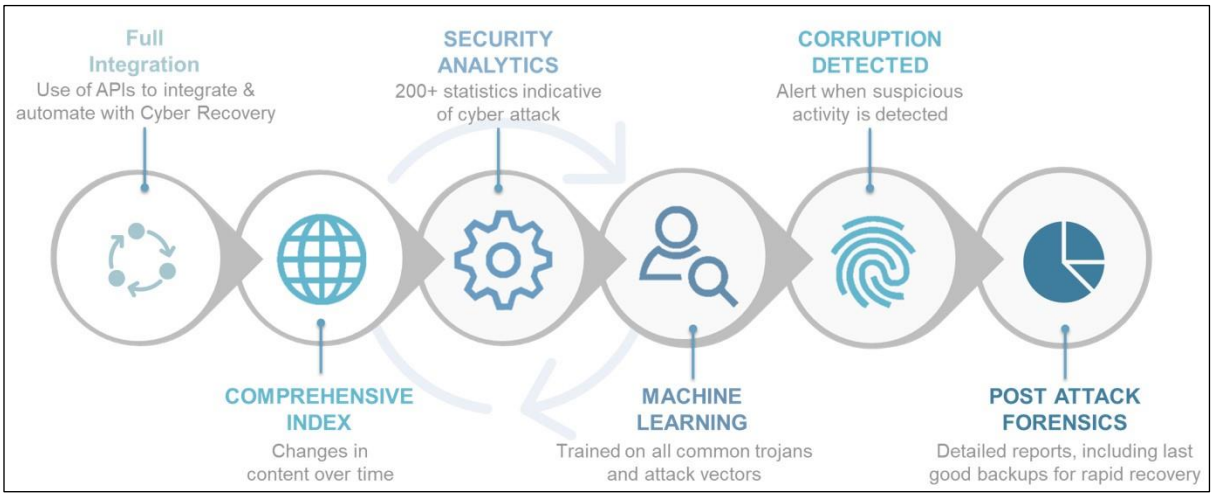
CyberSense seamlessly integrates with Dell PowerProtect Cyber Recovery, actively monitoring files and databases to detect ransomware corruption by analyzing the integrity of the data. Once data is replicated to the Cyber Recovery vault and retention lock is applied, CyberSense automatically initiates a comprehensive scan of the backup data, creating point-in-time observations of files, databases, and core infrastructure. These observations empower CyberSense to meticulously track changes in files over time, effectively uncovering data corruption by even the most sophisticated cyber threats.

The CyberSense scan operates directly on data within the backup image, eliminating the need for the original backup software and rehydration of the data. Through advanced analytics, CyberSense identifies encryption/corruption of files or database pages, recognizes known malware extensions, detects mass deletions/creations of files, and more.

Utilizing AI-based machine learning algorithms trained with the latest trojans and ransomware, CyberSense makes deterministic decisions on data corruption indicative of a cyberattack. In the event of an attack, a critical alert is promptly displayed in the Cyber Recovery dashboard. Additionally, CyberSense offers post-attack forensic reports, facilitating swift diagnosis and recovery from ransomware attacks to minimize data loss.

**Full Content Analytics**

CyberSense is the only product on the market that delivers full-content-based analytics on all of the protected data. 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.




CyberSense goes beyond metadata-only solutions because it is based on full-content analytics in detecting data corruption. It audits files and databases for attacks that include content-only based corruption of the file structure or partial encryption inside a document or page of a database. These attacks cannot be found using analytics that do not scan inside the file to compare how it changes over time. Without full-content-based analytics, the number of false negatives will be significant, providing a false sense of confidence in your data integrity and security. In addition, custom threshold alerts can be created based on the quantity or percentage of changed files or file type, added or deleted files and entropy across a host.

**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 audits your data and detects indicators of compromise and corruption. CyberSense empowers you to proactively understand the blast radius of a cyberattack in motion, facilitating the implementation of a plan to swiftly diagnose and recover, thus mitigating business interruption and its associated significant expenses.

| | | | |
|---|---|---|---|
| Learn more about Dell PowerProtect Cyber Recovery | Contact a Dell Technologies Expert | Learn more about CyberSense | Join the conversation with #PowerProtect |



DELL Technologies