DELL Technologies

Solution Brief

CyberSense® for PowerProtect Cyber Recovery

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

THE CYBERSENSE ADVANTAGE

CyberSense is fully integrated with the Dell EMC 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 EMC 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.

Cyber threats are increasingly becoming more sophisticated in how they penetrate the data center. Even with the most advanced security products deployed, organizations are still at risk of having data attacked and corrupted by bad actors. CyberSense adds a last line of defense to your existing security solutions, finding corruption that occurs when an attack has successfully breached the data center.

CyberSense leverages data backups to observe how data changes over time and then utilizes analytics to detect signs of corruption indicative of a ransomware attack. Machine learning then examines these 100+ content-based analytics to find corruption with up to 99.5% confidence, helping you protect your business-critical infrastructure and content. CyberSense detects mass deletions, encryption, and other suspicious changes in core infrastructure (such as Active Directory, DNS, etc.), user files, and critical production databases resulting from common attacks. If CyberSense detects signs of corruption, an alert is generated, 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 cyberattack further. With CyberSense, when data corruption is detected, a listing of the last known good backup data sets is available to support rapid recovery and minimize business interruption.

The Cyber Recovery Workflow

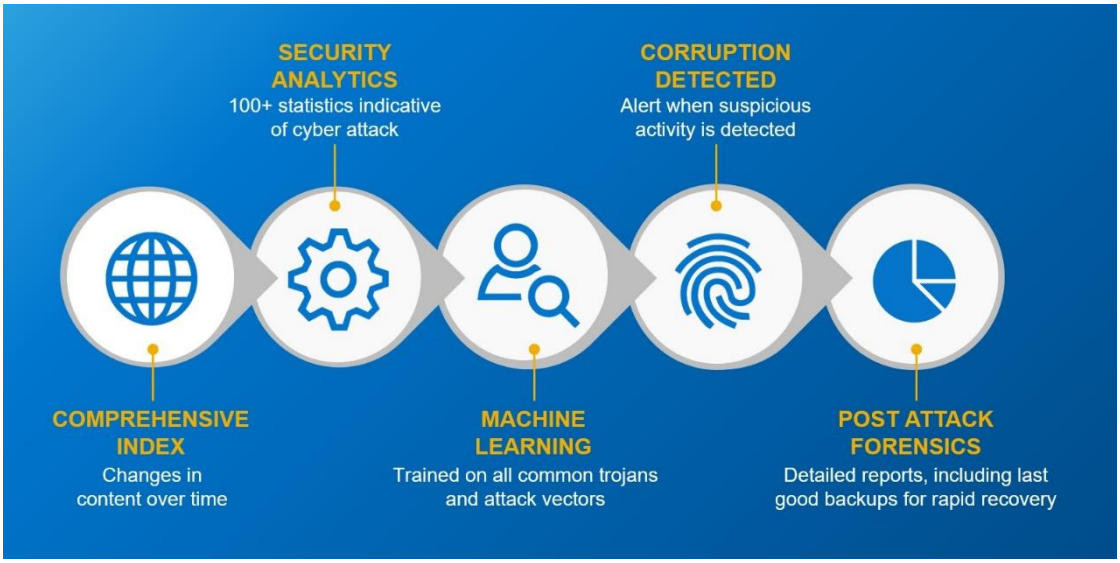
CyberSense is fully integrated with PowerProtect Cyber Recovery and monitors files and databases to determine if an attack has occurred by analyzing the data's integrity. Once data is replicated to the Cyber Recovery vault and retention lock is applied, CyberSense automatically scans the backup data, creating point-in-time observations of files, databases, and core infrastructure. These observations enable CyberSense to track how files change over time and uncover even the most advanced type of attack.

This scan occurs directly on the data within the backup image without the need for the original backup software. Analytics are generated that detect encryption/corruption of files or database pages, known malware extensions, mass deletions/creations of files, and more.

Machine learning algorithms then use analytics to make a deterministic decision on data corruption that is indicative of a cyberattack. The machine learning algorithms have been trained with the latest trojans and ransomware to detect suspicious behavior. If an attack occurs, a critical alert is displayed in the Cyber Recovery dashboard. CyberSense post-attack forensic reports are available to diagnose and recover from the ransomware attack quickly.

Full Content Analytics

CyberSense is the only product on the market that delivers full-content-based analytics on all 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 that provides up to 99.5% confidence 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 does 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.

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 such as Oracle, DB2, SQL, Epic Caché, etc.

Summary

Fully integrated with Dell EMC PowerProtect Cyber Recovery, CyberSense audits your data and detects indicators of compromise and attacks so that you can proactively understand when an attack is in motion with over 99% accuracy and put a plan in place to diagnose, recover quickly and avoid business interruption and the significant expense it can cause.

Learn More about CyberSense

Contact a Dell EMC Expert

Reference Number: H18214