DELL Technologies

Solution Brief

CyberSense for PowerProtect Cyber Recovery

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

WHY CYBERSENSE?

CyberSense integrated with Dell EMC Cyber Recovery provides a secure and powerful solution to combat ransomware and other cyber attacks.

When an attack gets past real-time defenses and corrupts files or databases, you have confidence that clean data is isolated in the Cyber Recovery vault and has been analyzed by CyberSense.

CyberSense checks the data's integrity and determines if any corruption exists. This enables business operations to continue without interruption and cyberattacks to be thwarted painlessly and quickly rather than within many weeks or months.

CyberSense delivers a unique approach, auditing data content to determine if it has been compromised. Key advantages include:

- Direct scanning of all common backup software images, including NetWorker and Avamar
- More than 100 statistics generated to look inside the data for unusual behavior
- Machine learning to generate a Yes/No indicator that an attack has occurred
- Forensic tools to find corrupt files and diagnose the attack vector
- Ability to quickly find and restore last good file to minimize business interruption

Real-time cybersecurity solutions are designed to protect from an attack. However, these solutions are not 100% effective and corporate data is still corrupted daily. CyberSense adds a layer of protection to these real-time solutions, finding corruption that occurs when an attack has successfully penetrated the data center. CyberSense also enables quick recovery so you can avoid business interruption.

CyberSense takes a unique approach in uncovering cyberattacks, observing how data changes over time and using analytics to detect signs of corruption due to ransomware. Its innovative approach uses machine learning to analyze over 100 content-based statistics and finds corruption with up to 99.5% confidence, helping you protect your business-critical infrastructure and content.

CyberSense detects mass deletions, encryption, and other types of changes in files and databases that result from common attacks. If CyberSense detects signs of corruption, an alert is generated, with the attack vector and listing of files affected.

CyberSense provides forensic reports to further diagnose the cyberattack. With CyberSense, organizations can proactively audit their files and databases to determine when an attack begins and quickly recover with the last good version of the data before there is any interruption to the business.

Automated Data Integrity Audits

CyberSense adds a layer of protection that examines inside of files and databases to understand how they change over time.

CyberSense monitors the integrity of the data and sends alerts when changes occur that are indicative of a cyberattack. This added layer of security is designed to compensate for when attacks circumvent existing security defenses.

CyberSense with Cyber Recovery Workflow

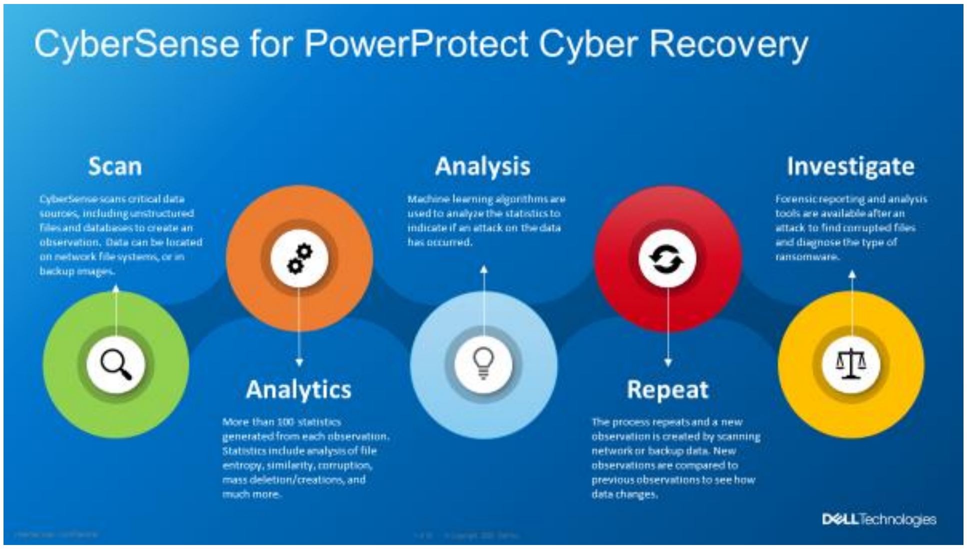
CyberSense is fully integrated with Dell EMC Cyber Recovery and monitors files and databases to determine if an attack has occurred based on data corruption. Once data is replicated to the Cyber Recovery vault and retention lock is applied, CyberSense scans the backup data, creating point-in-time observations of files and databases.

This scan occurs directly on the data within the backup image without the need for the original backup software. Analytics are generated, including file type mismatch, corruption, known ransomware extensions, deletions, entropy, similarity and more.

The analytics are then used by machine learning algorithms to make a deterministic decision on data corruption that is indicative of a cyberattack. The machine learning algorithms have been trained by all the latest trojans and ransomware and can be updated as new attack vectors are discovered. Observations of the data allow CyberSense to track how contents of files change over time. If an attack does occur a critical alert is displayed in the Cyber Recovery dashboard and CyberSense post-attack forensic reports are available to quickly diagnose and recover from the ransomware attack.

Full Content Analytics

CyberSense delivers full-content based analytics. 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 cyber criminals are using today.



CyberSense for PowerProtect Cyber Recovery

Scan

CyberSense scans critical data sources, including unstructured files and databases to create an observation. Data can be located on network file systems, or in backup images.

Analytics

More than 100 statistics generated from each observation. Statistics include analysis of file entropy, similarity, corruption, mass deletion/creations, and much more.

Analysis

Machine learning algorithms are used to analyze the statistics to indicate if an attack on the data has occurred.

Repeat

The process repeats and a new observation is created by scanning network or backup data. New observations are compared to previous observations to see how data changes.

Investigate

Forensic reporting and analysis tools are available after an attack to find corrupted files and diagnose the type of ransomware.

CyberSense goes beyond metadata-only solutions because it is based on full-content analytics that provide 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 do not scan inside the file to compare how it is changing 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 and agreements; intellectual property and databases such as Oracle, DB2, SQL, Epic Caché and others.

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