Don't rely on cybersecurity analytics software that looks only at the tip of your data iceberg

By Andrew Glinka | November 2022

When it comes to scanning, detecting, and isolating ransomware code or anomalous activity in your production backups, you need an AI/ML-based analysis tool that looks thoroughly *beneath* the surface and not merely at the tip of the iceberg. After all, 90% of an iceberg is hidden beneath the surface. That's also where malware and ransomware code can lurk undetected from mere 'surface' or partial scans as bad actors increasingly get more sophisticated with their cyberattacks.

Dell's PowerProtect Cyber Recovery isolates your mission-critical backup copies in a network-isolated cyber vault. With full integration of CyberSense, intelligent analytics software scans your entire data copy contents stored in the vault to detect unusual patterns and anomalous data changes, as well as other suspicious activity. The two solution components offer powerful cyber resilience and a fast recovery combination for restoring clean backup copies.

What is CyberSense

CyberSense is a *post-attack* product that is focused on data resiliency. It doesn't replace the ransomware prevention measures of PowerProtect Cyber Recovery's isolated cyber vault but complements it with an intelligent and powerful last line of defense – one that helps identify corrupted data and clean backup copies suitable for rapid recovery if/when an attack has infiltrated your production data or backups.

CyberSense goes beyond the competition because of its:

- Breadth *and* depth of its data, file, and database scanning by analyzing your backup copies' full contents – not just with superficial or basic scans
- New and innovative methodology that enables the above thorough inspection of file and database contents by using over 200 analytic algorithms
- Powerful machine learning models that are trained using thousands of ransomware variants to help detect the latest attacks

The above 3 key design features of CyberSense are critical not only to help detecting malware, ransomware, and disruption by bad actors (or accidental mishandling) in gaging the integrity of data post-attack, but also for quarantining contaminated data and identifying virus-free 'clean copies' for safe and fast recovery back in your production environment.

Afterall, the last thing you want to do is to introduce or re-introduce contaminated copies and/or ransomware back into your production environment.

Typical Malware and Ransomware Scanning Tools

There are many storage and backup vendors offering cyber resilience and recovery solutions. Many –state to offer intelligent AI analysis capabilities. But how 'intelligent' are they in analyzing, detecting, isolating, and identifying clean copies? And how do they deliver effective protection in pre- and post-attack cyberattack scenarios involving *new* variants coming from increasingly clever and sophisticated attackers?

Typical approaches employed by backup vendors are:

1. Adding signature-based scanning tools to their production backups to find *known* malware
2. Performing scans and searches based on meta-data or data threshold analysis (i.e., data or activity changes)

Let's take a closer look at the #1 and #2 approaches, specific to backing up and storing data copies.

Signature-based scanning

Scanning for known malware and ransomware signatures is typically done on production systems for attack prevention (i.e., pre-attack phase), but recently signature-based scanning security tools that rely on production-based public catalogs or watchlists have been added by backup software vendors.

The obvious weakness of relying on signature-based scanning for pre-attack *or* post-attack cyber resilience is this: your backup's security and data integrity depends on – and is only as good as -- the *production* watchlist's currency *and* what known malicious code has been reported and cataloged. Are you ready to bet your business on that?

New, previously undetected, and under-reported malware code such as BianLian, which is designed to defeat signature-based scanning by constantly changing encryption algorithms, is a prime example. It's worth noting that according to a recent security report from WatchGuard, 57.8% of malware codes avoid signature detection.

Metadata Analysis and Threshold Detection

There's value in signature-based scanning, particularly during the recovery of backups and detecting *known* security threats. But watchlists and catalogs must be continually updated and kept fresh. Vendors who rely solely on signature detection alone may not offer the level of protection your business needs. BianLian is only one example of how sophisticated bad actors have become in designing malware and overcoming pre- and post-attack detection tools.

Metadata and threshold analysis are also common tools being used by backup software vendors these days. Like signature-based scanning, metadata and threshold analysis tools are not hard to create and incorporate. They also provide some level of detection capability and data integrity. But like signature-based scanning for known malware code, metadata and data threshold analysis tools can be defeated by new, sophisticated bad actors.

How? Metadata analysis scans can be fooled when scanning for file extensions of corrupted data (ex., by appending new, unknown file extensions not recognized by the scanning tool). Like signature-based scanning, metadata analysis tools must be continually updated with the latest known variants. Metadata analysis is also based on limited metadata fields and can also return false positives from such things as deliberate/authorized file extension changes.

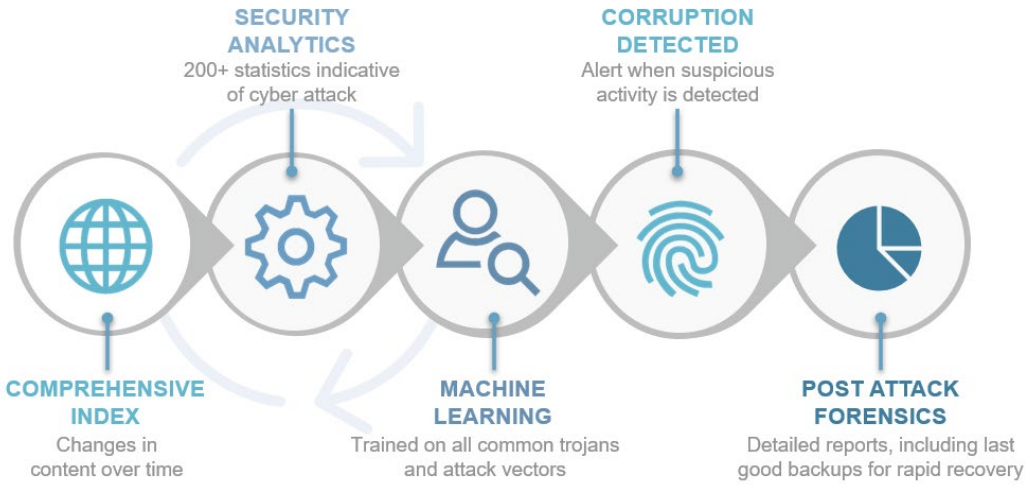
Threshold analysis? It's designed to observe patterns of activity (POA) in data, and alerts when pre-determined threshold values have been exceeded. Things like data changes, unusual access or behavioral activity, an unusual number of file creations or deletions, etc. Threshold analysis-based detection is not sophisticated. It's only as good as the types of thresholds being monitored and set changes and POA values to alert on. Sophisticated attackers know how to 'duck under' threshold-based detection tools.

There are other approaches to post-attack forensics such as file entropy analysis or *pre-attack* detection of infrastructure resource threshold spikes, changes or unusual patterns, and real-time activity. Those are typically performed on the production platform where backups are run from.

CyberSense's Approach – Adaptive Learning

CyberSense is an AI/ML analysis tool that searches for unusual patterns of behavior based on file and database full-content scans. Like other vendors' approaches, CyberSense *does* scan a limited set of metadata properties. But unlike other vendors, CyberSense *goes much deeper* beneath the metadata and threshold surface and searches through hundreds of content statistics across the complete set of files and databases contained in each backup.

Moreover, CyberSense continually learns from ongoing training and recognition of anomalous activity patterns. This adaptive ML training is based not only on all the known common approaches of real-world, contemporary attack profiles and approaches but also on actual examples of malicious attacks from customer feedback reporting.



Dell's PowerProtect Cyber Recovery solution with full integration of CyberSense adds an intelligent layer of protection, coupled with a network-isolated vault, to help protect your backup copies and quickly identify virus-free ones using sophisticated post-attack analysis and learning.

CyberSense is unique in how it analyzes full content data stats well beyond traditional code signatures, threshold triggers, and superficial and/or partial metadata scans.

Trust Dell…Trust CyberSense's Intelligent Analysis

CyberSense is trained with:

- data derived from volumes of advanced metadata and content analytics
- Continual updated 'lessons' on known common and newly reported attack approaches
- Sophisticated AI pattern recognition algorithms to perform post-attack forensics and identification of virus or malicious code-free 'clean copies' for quick recovery

Because CyberSense adaptive learning keeps it 'smart', it is able to detect new and advanced ransomware variants like BianLian that partially or intermittently encrypts data files --typically beneath other vendors' detection radars -- before they can update their analysis software.

In closing, CyberSense allows you to leverage the power of machine learning to help detect new, harmful viruses and other malicious code variants that can escape detection by other vendors' approaches and post-attack analysis methods. The result is a very high confidence level that your backup data copies are 'clean' and can be recovered quickly, with a corresponding very low percentage of false negatives and false positives. Full content analysis of files and databases combined with advanced AI/ML capabilities delivers confidence that your data is better protected from even the most sophisticated cyber threats and attacks. Confidence that you can trust.

Click here for more detailed information on PowerProtect Cyber Recovery and CyberSense, and Dell's Trusted Infrastructure, and listen to our recent podcast and LinkedIn Live webinar. Don't hesitate to contact a Dell Technologies Sales Rep or partner for more information on our full range of IT infrastructure products, software solutions, and services, too.

#TrustDell

About the author: Andrew Glinka is Vice President, Competitive Intelligence at Dell Technologies. Andrew is an 11-year Dell Technologies veteran and brings over 23 years of experience in technology sales, management, and operations. Before assuming his current role, Andrew served as Global Director of Sales Strategy for the Data Protection Solutions Division. He has also managed the Global Software Sales team as well as other sales teams in the Data Protection Solutions Division. Prior to joining Dell through the EMC acquisition, Andrew owned and operated an IT Managed Services business in Virginia for over 8 years before successfully selling the company.