Dell PowerProtect Cyber Recovery Vault and CyberSense analytics software deliver unique safeguards against ransomware

By Andrew Glinka, Vice President of Competitive Intelligence, Dell Technologies | Oct. 2022

There are a lot of storage and backup vendors offering cybersecurity solutions. Common messaging themes from these vendors are organized around terms such as zero trust architecture, immutable snapshots, and cloud vaults. Some vendors even claim to offer isolated data vaults and comprehensive analytics that help identify uncorrupted data copies. However, not all vendors' solutions have the same trust factor as Dell PowerProtect Cyber Recovery Vault and CyberSense software.

Sheltered Harbor, the standard-bearer for data protection and cyber-resilience in the U.S. financial sector, awarded Dell PowerProtect Cyber Recovery their very first endorsement for meeting all Sheltered Harbor cyber resilience and recovery requirements by a turnkey data vaulting solution vendor. That's a powerful validation of Dell's ability to deliver cyber-resiliency solutions you can trust.[1]

So why did Sheltered Harbor endorse Dell first, and why do customers consistently turn to PowerProtect Cyber Recovery and CyberSense analytics software? PowerProtect Cyber Recovery delivers these key, essential protections:

- Snapshot immutability reinforced by exclusive data integrity functions
- Data isolation with strict access controls
- Analytics intelligence with differentiated machine learning intelligence

Immutability Alone is Not Enough

When it comes to data protection and immutability, virtually all vendors claim their backup copies and VM snapshots are write-protected and cannot be modified or deleted by accident or by bad actors. After all, the immutability of data and file copies is the most basic form of data protection against corruption, deletion, or embedding of 'stealth' malware code. Immutability alone, however, is simply not enough protection against cyberattacks.

Snapshots alone are *not* sufficient for reliable data protection or cybersecurity and recovery. Snapshots can be deleted by unauthorized personnel and production data can be corrupted or encrypted with 'stealth malware' when snaps are taken. What good is an immutable snap if the system itself is vulnerable or if the system clock can be manipulated (I.e., fast forwarded) to cause the snap to expire and be deleted prematurely? Data and files simply cannot be sufficiently protected from cyberattacks by solely relying on immutable snaps.

Dell's PowerProtect Data Manager software and DD backup and recovery appliance support Dell's Data Invulnerability Architecture (DIA) for reliable internal data integrity checking and retention lock immutability for backup copies. PowerProtect DD appliances are used for PowerProtect Cyber Recovery isolated vaulting of backups.

Isolation is Essential!

It's an indisputable fact and something Sheltered Harbor looks for in a reliable cyber recovery solution.   The more data, files or databases are removed and isolated from production and system domains, the more resistant they will be from disruptions caused by cyberattacks, corruption, internal actions or natural disasters.

PowerProtect Cyber Recovery vaults do exactly that. Data is copied and stored in sep*arate, isolated independent vaults for on-prem deployments separate from production environments*. But not all attacks target just data. Key IT system infrastructure code is vulnerable, too. There have been high profile reports of attacks on operating systems, firmware, network/comm switches, and apps as well.

Some vendors rely solely on storing all their snapshots in the public cloud or by storing multiple replication copies in multiple geographic availability zones or on several storage platforms and media types (with or without dedicated comm port controls).

Some of these same vendors may even claim that there's little to no difference between disaster recovery (DR), long-term retention (LTR), ransomware protection and cyber recovery (CR) copies regardless of how and where these copies are separated from production environments – or how infected copies are kept from being restored back into production. Finally, some don't offer an on-prem physical vault appliance for broader cyber security protected backups and fast recovery, claiming immutable snapshots are enough protection from cyberattacks.

Dell's PowerProtect Cyber Recovery vault uses an isolated vault to help keep your mission-critical data safely backed up in a separate storage appliance with independent internal access and online network controls. For hybrid or public cloud deployment, PowerProtect Cyber Recovery also isolates data sent to the public cloud. Backing up data in both on-prem vault appliances *and* public cloud environments gives you more protection and fast recovery options from cyberattacks.

There's Intelligence, and then there's CyberSense Intelligence

The third key component of an effective and reliable cyber security and recovery solution is 'intelligence'. The sooner you detect suspicious data or activity patterns, the more you can mitigate the costly impact of malware code hiding in your data vault.

So, when it comes to artificial intelligence (AI) and dynamic adaptive machine learning (ML) software for...

- Anomalous data and activity pattern recognition
- Early detection of infected copies
- Alerting and reporting…you'll be hard-pressed to find a smarter cyber analytics solution than CyberSense.

Many vendors offer separate or bundled intelligent analytics software for the detection of data or file corruption by any cause. But do their analytics scan all storage or backup contents? Do they rely on metadata or known cyber-attack catalogued code signatures previously reported for detection criteria? CyberSense is a software option available with PowerProtect Cyber

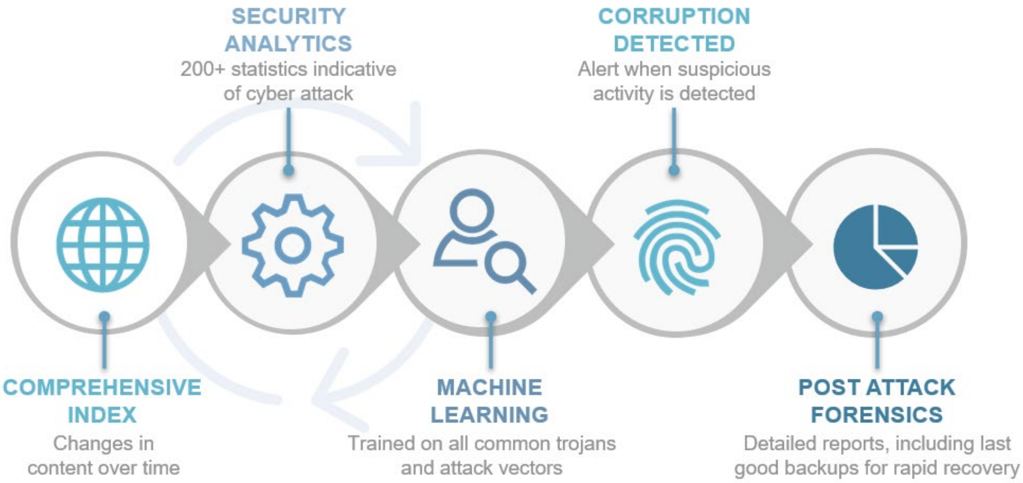
Recovery. CyberSense stands apart from the competition with its own innovative and unique AI/ML adaptive training and learning capabilities.

CyberSense applies advanced intelligent adaptive learning when performing full content analysis of data, files, and databases -- not by scanning metadata files alone. It searches for anomalous data, suspicious access and activity pattern recognition and gets smarter the more it's used and trained.

Be sure to ask other vendors how *their* cybersecurity intelligent analysis software tools work and whether they analyze full data and file content. You want smart cyber analytics with low false negative *and* false positive results when scanning your storage and backup copies. You *need* early detection for faster recovery time and effective mitigation. Knowing *early on* which dataset or file copy version is *not* infected enables you recover quicker and reduce downtime.

PowerProtect Cyber Recovery and CyberSense are a Powerful Combo

Per the infographic below, the combination of Dell's PowerProtect Cyber Recovery vault and CyberSense AI/ML analytics software is a powerful tool for detecting malicious code lurking in your backup copies. By identifying infected data via full content analysis scans, CyberSense can minimize the costly risk of copying infected copies back into your production environment during recovery.


SECURITY ANALYTICS
200+ statistics indicative of cyber attack
CORRUPTION DETECTED
Alert when suspicious activity is detected
COMPREHENSIVE INDEX
Changes in content over time
MACHINE LEARNING
Trained on all common trojans and attack vectors
POST ATTACK FORENSICS
Detailed reports, including last good backups for rapid recovery

Intelligent CyberSense works with PowerProtect Cyber Recovery vault to help protect your backup copies and quickly identify virus-free ones.

In Closing

I'll further explain in a follow-on blog why CyberSense is so unique and 'smarter' than competing solutions in analyzing data patterns, recognizing anomalous activity, and detecting malware and ransomware code.

In the meantime, do reach out to a Dell Sales Representative or Authorized Dell Partner for more information on PowerProtect Cyber Recovery and CyberSense, and why both are industry-leading cybersecurity solutions. While you're at it, ask them for more information on Dell's Trusted Infrastructure products and services and why you can trust with confidence Dell for all your IT needs.

#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. Prior to 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.