DELL Technologies

Dell PowerProtect Cyber Recovery vs. Other Industry Approaches

Immunability

Dell PowerProtect Cyber Recovery

Compliance
Immutability helps protect data by making it very difficult to change or delete during a "locked" period. Dell PowerProtect Cyber Recovery immutability is based on a compliance mode retention lock – a built-in capability for Dell PowerProtect DD since 2012 and attested by a third party to comply with the 17a-4(f)(2) "WORM" archiving standard.

Attack Surface
Advanced NTP clock hardening capabilities extend immutability protection against even sophisticated clock-based attacks to both production and vaulted copies.

What's in Scope?
Dell PowerProtect Cyber Recovery is designed to capture all the data needed to perform recoveries, including backup catalogs, metadata records, and other various ancillary data.

Defense in Depth
When immutability such as PowerProtect DD's Retention Lock is combined with isolation, as described below, both controls are stronger and provide defense in depth.

Other Industry Approaches

Compliance
There is no cybersecurity standard for storage immutability, so many vendors will claim immutability without specifying the details of how the data is being protected. This can leave your data exposed to deletion if you don't fully understand their definition of immutability.

Attack Surface
Common attacks on immutability include clock tampering, physical access, secure vendor access, and platform crashes; meanwhile, immutability in a software-defined infrastructure can be defeated by anyone with hypervisor access.

What's in Scope?
Storage immutability normally does not protect other components required for recovery such as backup catalogs, media servers, dedupe databases, and other backup infrastructure; without additional manual configuration. Your ability to recover may be compromised even if the data is not deleted.

Defense in Depth
Strong immutability is a good control as part of "defense in depth." On its own, without other protections such as isolation, it is subject to attack and may not be sufficient to protect your most critical assets.

Isolation

Logical Air Gap
Dell PowerProtect Cyber Recovery uses a "logical air gap", which is connected on-demand so that data within the vault environment can be updated. This means that when "locked" there is no connectivity into the secure vault. Then, when the operational air gap is temporarily unlocked to update data, the vault remains secure because only data replication is permitted. The management plane is never exposed to the production side, so an outsider has no ability to delete or modify data, configurations, or policies.

Secure Vault Operation
Data is "pulled" into the vault, not pushed from production – meaning the vault is opened and closed, from the secure vault side, on an automated basis according to pre-configured policies.

On-Prem & Cloud
Dell PowerProtect Cyber Recovery is an isolated environment and is fully automated. When on-prem, additional security can be provided through physical isolation. The vault components can be in a locked cage or room, providing further isolation and protection from even insider activity.

Logical Air Gap
The terms "air gap" and "isolation" are used differently by different vendors, so it's important to understand the details of any isolation claim. If isolation simply means another copy of data on a different network, that data may remain subject to direct attack – it's just a connection and a password away. If a switch or firewall is used to create isolation and is accessible from the production environment, or controlled by the backup software, it can be vulnerable to compromise.

Secure Vault Operation
Other vendors can use encrypted tunnels to the cloud or other sites or use a firewall as an in-between for controlling access, but those need to be controlled from a production environment, potentially leaving those controls accessible to bad actors.

Cloud-Only
Public Cloud operates on shared virtual resources, which present different challenges when it comes to isolating data. Cloud data tends to be accessible through a browser-based control panel, which is not isolated - therefore additional considerations need to be taken with this scenario.

Intelligence

Next-Generation Analytics
CyberSense is built on AI/ML, leveraging a supervised machine learning model that is trained on millions of samples across thousands of malware strains to recognize data corrupted by malware. Since the model is trained to recognize corruption and anomalous behavior, and not look for constantly changing malware, it can identify data corrupted by new and unique attacks. In addition, because it analyses the data itself, it does not need frequent updates as required by systems using malware signatures/definitions.

What's Being Observed
A CyberSense scan generates 200 observations per file, analyzing full content and not just metadata, for a more thorough understanding of even advanced attacks that leave metadata unchanged. This approach also helps reduce false positives/negatives.

Purpose
CyberSense helps to quickly identify last-known good copies of data. Post-attack capabilities also provide more efficient and safer recovery processes.

Next-Generation Analytics
Some other vendors use a "known issue" approach and scan for known signatures or vulnerabilities. These can be informative but often duplicate what is used by the cybersecurity team in production. They cannot recognize new updates or unique attacks and have limited value in identifying "last known good" data for the recovery process. Many other vendor's solutions run in production or in the cloud, where they are vulnerable to compromise. A bad actor with admin-level backup infrastructure or cloud account access can hide their activity.

What's Being Observed
Metadata-only analytics can be fast but deliver a limited view because they evaluate fewer criteria and bad actors can hide changes by leaving metadata alone. Frequently metadata scanners deliver a high level of false positives and negatives.

Purpose
In some cases, other vendors' analytics serve purposes other than helping to ensure a faster and more effective recovery. Ultimately, such scans do not help to improve the recovery process.