Dell PowerProtect DD appliances take backup security to a higher level

By David Noy | April 2023

Cyber-criminals know that if they want to be successful at destroying data or getting paid a ransom, they have to make sure that the companies they've targeted can't turn to backups to recover their data. This places backup data squarely in cyber-criminals' crosshairs. As a result, any good backup solution today must address cyber-security.

Backup providers have done a lot to help companies secure their data from attackers, and they are actively marketing their capabilities. When you survey the competitive landscape, you find a common wordlist of cyber-security features, such as immutability, encryption, role-based access controls (RBAC), multi-factor authentication (MFA), air-gap, etc.

8 ways Dell PowerProtect DD appliances can help you take backup security to a higher level

1. Data immutability with greater flexibility and more stringent protections
2. Client access with client-side deduplication and compression
3. Anytime encryption, so it's easier and less costly to bring PowerProtect DD appliances into existing infrastructure
4. A more security-hardened administrative environment
5. Extra security measures to help prevent clock tampering
6. More rigorous validation of data integrity
7. A more secure data isolation approach with cyber vaults
8. Sheltered Harbor standards, proving that PowerProtect DD appliances measure up to some of the most rigorous standards for protecting mission-critical data

On the surface, the features appear to offer similar capabilities across competitors' offerings, but when you take a more detailed look at Dell's PowerProtect DD appliances, you will find that they have some unique capabilities to harden the backup environment against cyber-attacks more rigorously than typical backup offerings. You will also find a high level of operational flexibility with PowerProtect DD appliances, which can enable greater management excellence across the entire backup estate.

Notably, the advanced cyber recovery vault functions available with PowerProtect DD appliances helped Dell to be the world's first turnkey cyber-vault solution endorsed to meet Sheltered Harbor's data vaulting standards. Sheltered Harbor is the standard-bearer for data protection and cyber-resilience in

the U.S. financial sector where you find some of the most rigorous standards for protecting mission-critical data.

Immutability with greater flexibility and more stringent protections

At the most basic level, the ability to lock backup data so that it can't be changed is common across the competitive landscape. On Dell PowerProtect DD appliances, immutability is a built-in hardware function that adds significant value beyond typical immutability functions. With the PowerProtect implementation, companies can enable immutability across a broader set of applications—those supported by backup software, as well as those that backup directly to storage.

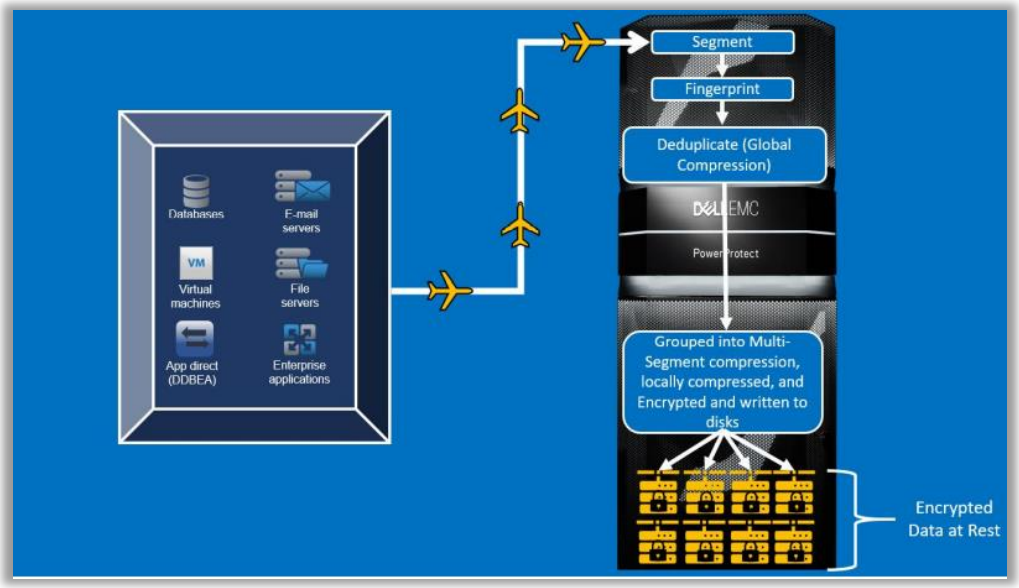
Immutability isn't the same across all backup offerings. Dell PowerProtect DD appliances enable more rigorous tamper protection with compliance-level implementations by hardening not just the data, but also the security around underlying system functions.

Immutability in PowerProtect DD appliances also offers greater flexibility than conventional solutions. While software policies usually apply one security level wholesale across all data sets—for example, either governance level or compliance level, but not both—Data Domain Retention Lock in PowerProtect DD appliances allow governance and compliance immutability levels to be selectively applied to individual data sets so companies can consolidate diverse backups within a system.

Immutability functions in PowerProtect DD appliances can also help enable more rigorous tamper protection with compliance-level implementations than other solutions by tamper-proofing the underlying system hardware and software along with the data. Examples of underlying system clock functions tamper-proofed by PowerProtect compliance-level immutability include the system clock, the filesystem, and the remote system management ports. PowerProtect compliance-level immutability also blocks overriding retention lock periods.

Client access with client-side deduplication and compression

Using proprietary protocols for communicating with clients helps harden backup filesystems against access by crypto malware. PowerProtect DD appliances support CIFS and NFS protocols, but they also have a proprietary API, DD Boost. In fact, many leading backup applications integrate with DD Boost. This API enables encryption on data in flight to and from



Dell PowerProtect DD appliances offer the only data-in-flight encryption with global compression.

the PowerProtect DD appliances, so the underlying filesystem is undiscoverable by malware. In addition to helping secure data in fight, DD Boost also enables client-side deduplication and compression for better backup and restore performance. Some other conventional backup offerings don't provide this advantage.

Anytime encryption

With basic backup solutions, encryption is typically a monolithic function that must be turned on up front. Any unencrypted backup data can't be encrypted without outages and heavy-handed services—unwelcomed challenges and cost for any company bringing these solutions into established infrastructure.

Encryption can be enabled at any time with Dell PowerProtect DD appliances, so it's easy and less costly to bring them into existing infrastructure.

Dell's PowerProtect DD appliances have broad support for encryption on data in flight, as well as data at rest. Importantly, encryption can be enabled at any time, with the option of encrypting any data that was previously written. This makes it easier and less costly to bring PowerProtect DD appliances into existing infrastructure.

Encryption in flight is supported through the DD Boost protocol utilizing either AES128-SHA1 (medium) or AES256-SHA1 (high). When enabled, both backup and restore traffic will be encrypted to and from PowerProtect DD appliances. Replication traffic can also be encrypted to protect data traveling over the WAN.

Encryption at rest can be enabled in PowerProtect DD appliances with either AES128 or AES256 (CBC or GCM). Encryption keys can be managed by PowerProtect DD appliances or an external key manager.

More security-hardened administrative environment

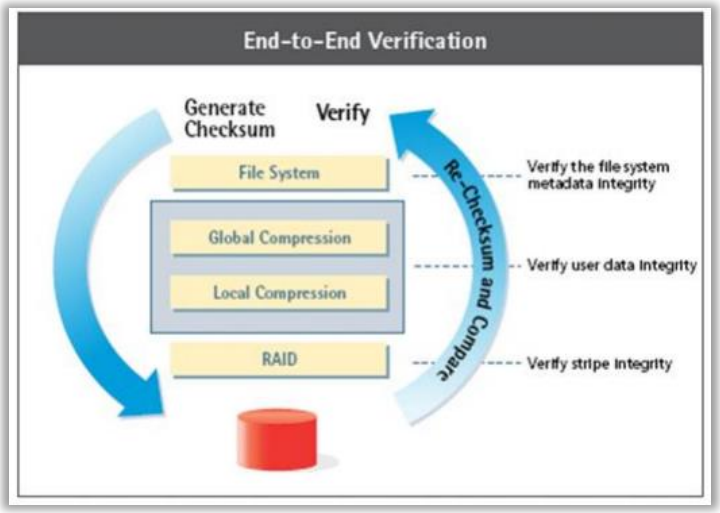
PowerProtect DD appliances come with built-in dual-authorization control for a broader set of administrative functions than basic backup solutions, which can require service engagements for expanding administrative security.

Dual-role authorization with "security officer" oversight on command functions for administering sensitive operations is yet another area where PowerProtect DD appliances excel. Some of the basic backup solutions provide dual-role authorization for fundamental data immutability functions in compliance-mode deployments and compensate for the limited scope of their built-in controls by requiring onsite support engagement for other administrative functions. PowerProtect DD appliances have expanded built-in dual-authorization controls that cover immutability functions in addition to other administrative functions such as encryption, retention lock compliance, and archival. Companies get expansive hardening of the administrative environment in compliance-mode deployments without the cost and inconvenience of services engagements.

Extra security measures to help prevent clock tampering

The system clock is vital to data immutability, which helps prevent cyber-criminals from corrupting or destroying data. As a result, clock functions can be a target for cyber-criminals. Most of the basic backup offerings rely solely on secure network time protocol and the system clock to harden their data immutability functions, but PowerProtect DD appliances implement an internal security clock that is monitored against the secured system clock. When the variation between the PowerProtect clock and the secured system clock reaches a designated value, the file system automatically shuts down to thwart an attack. Only a security officer can reactivate the file system once it has been shut down.

Additionally, PowerProtect DD appliances go above and beyond typical solutions to harden the system clock by enforcing a maximum allowed amount to advance the system time and date and a minimum amount of time between changes. Alerts will be generated when the clock skew exceeds half of the date change limit.

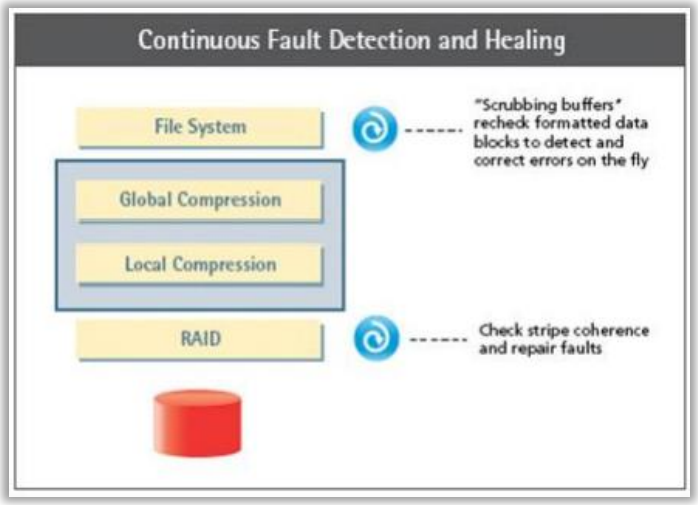


Since every component of a storage system can introduce errors, an end-to-end test is the simplest path to help ensure data integrity. End-to-end verification in Dell PowerProtect DD appliances means reading data after it is written and comparing it to what was sent to disk, proving that data has not been corrupted.

More rigorous validation of data integrity

Any security strategy starts at the most fundamental level—protecting backup data from system anomalies that can silently cause corruption during both backup and restore operations. PowerProtect DD appliances have a unique Data Invulnerability Architecture that automatically validates data integrity with more layers of consistency checks than other backup offerings on the market.

PowerProtect DD appliances compute checksums and self-describing metadata automatically in real-time for all data that comes into the system to help ensure that data is validated before it goes to disk. Once data is on disk, the appliance recomputes and verifies the checksums and metadata a second time. After a backup completes, the appliance ultimately verifies that all file segments are logically correct within the file system and that the data is identical before and after it is written to disk.



No matter the software safeguards in place, it is the nature of computing hardware to have occasional faults. Storage media can fail, and other more localized or transient faults may also occur. Continuous fault detection and healing in Dell PowerProtect DD appliances help protect against storage system faults.

PowerProtect DD appliances also continuously do background data scanning to validate that data on the disks remains correct and unchanged since the earlier validation process. Some basic backup solutions make this step an occasional, manual operation, and one that scans only a fraction of the data on disk. Ultimately with PowerProtect DD appliances, when reading data back on a restore operation, the system again uses multiple layers of consistency checks to verify that restored data is correct. These multiple layers of data integrity checks in PowerProtect DD appliances can give administrators greater confidence than competitors' solutions that restored data will be valid.

A more secure data isolation approach with cyber vaults

Ransomware, wiper malware, and similar attacks can commonly spread through the network to infect any connected devices, including backup servers and storage devices in datacenters and in the cloud, so simply having a second copy of data isn't enough. Isolation vaults accommodate a secure off-the-network backup of last resort that is a must-have for mission-critical and government-regulated data.

> While some competitors support only logical separation of the recovery vault, Dell PowerProtect DD appliances benefit from an operational air gap that is both physically and logically isolated, either on-premises or in the cloud.

Despite the importance of this element in the backup infrastructure, some of the basic backup solutions underdeliver on isolation. They typically claim isolation merely by storing data on a separate LAN segment or in the public cloud.

Dell offers an isolation vault for PowerProtect DD appliances that is more security-hardened. The PowerProtect Cyber Recovery vault—whether residing on-premises or in the cloud—enables a private network that is completely disconnected from any network while locked and never exposes the control plane to public network access. The private network can be unlocked for data replication only from the vault side, and only when deemed safe, so there is no remote access to the vault or the data within.

To harden the PowerProtect Cyber Recovery vault even further, Dell offers the CyberSense analytics engine, which can take more than 200 observations looking at actual file data to help detect potential anomalies with up to 99.5% accuracy based on model performance objectives. Analytics in competitive solutions are much less rigorous, usually looking only for metadata anomalies in the filesystem index.

> CyberSense software, available for PowerProtect DD appliances, gives Dell a more rigorous analytics capability than typical backup solutions to help thwart attacks and prevent damage to the data environment.

Take your backup security to a higher level

As cyber-attacks intensify around the world and criminal tactics become more sophisticated, companies need to amplify security in their backup environment, which is a prime target for cyber-criminals. As you look across the competitive landscape for technology that can help you protect your company's valuable data assets from increasing threats, trust Dell PowerProtect DD appliances to deliver more layers of protection and high-level operational flexibility than typical backup offerings. Dell PowerProtect DD appliances help you take backup security to a higher level with:

- More rigorous validation of data integrity
- A more secure data isolation approach
- Data immutability with greater flexibility and more stringent protections
- Client access with client-side deduplication and compression

- Anytime encryption so it’s it easier and less costly to bring PowerProtect DD appliances into existing infrastructure
- A more security-hardened administrative environment
- Extra measures to help prevent clock tampering
- The assurance of Sheltered Harbor standards, validating that PowerProtect DD appliances meet the most stringent standards for protecting mission-critical data

#TrustDell

About the author: David Noy brings over 25 years of experience in the storage and data management industry. He spent nearly a decade leading engineering and product management teams for numerous companies, including Dell Technologies, NetApp, Veritas, and Cohesity. Today, David leads product management at two industry-leading divisions at Dell Technologies—Unstructured Data Storage and Data Protection—where he is helping to embolden innovation around data management and hybrid cloud and driving advancement of holistic solutions to help heighten business success for customers worldwide.