DELL Technologies

Whitepaper

Data Protection, Zero Trust, and Cybersecurity

PowerProtect DD Zero Trust

Table of Contents

Data Protection is a Key Component to Zero Trust and Cybersecurity

Data protection has become one of the key attack points for cyber criminals today. It is critical to ensure your business is protected from all attack points in your organization by hardening your backup infrastructure to combat today's cyber criminals. Dell has a Zero Trust architecture that can be implemented on your existing PowerProtect DD's today to eliminate a majority of the known threat vectors. To provide further protection, the PowerProtect Cyber Recovery Vault can create an isolated, immutable, intelligent copy of your most mission critical data that is not accessible from the production network and not exposed to any advanced hacking techniques.

File Immutability

PowerProtect DD Retention Lock provides the ability to make backup files written to the PowerProtect DD immutable. Retention Lock comes in two editions (Governance and Compliance) and is set at a logical storage unit (Mtree) level. Governance Mode can be set for any Mtree on an existing system, but Compliance Mode will not be an option until it has been enabled for the entire PowerProtect DD. Enabling Compliance Mode on a system will lock the system down, require the creation of a Security Officer for dual authentication, harden the system clock against tampering, remove many of the destructive commands, hardening the iDRAC interface, and requires a reboot to implement. There is no way to override, even with the help of Dell support, the Retention Lock period for a file with Compliance Mode enabled.

When enabling Retention Lock on an Mtree, you have the option to set it use to Manual mode, which will give control to the backup application to set the Retention Lock period, or Automatic mode, which will set the Retention Lock period after a cool down period has expired. Guard Rails are placed on each Mtree to set a minimum and maximum Retention Lock period, if a request is outside of those parameters, the lock request is failed.

As Retention Locks are set at an Mtree level, it is possible for different data sets in different Mtrees to:

- Have no locking
- Governance Mode locking
- Compliance Mode locking

all on the same system.

Proprietary Transport Protocol (DDBOOST)

While PowerProtect DD will continue to support the CIFS and NFS protocols, many of the leading backup applications have integrated with the PowerProtect DD Bandwidth Optimized Open Storage (DDBOOST) API. This proprietary secure protocol prevents access to the backup data in the underlying filesystem and makes it undiscoverable to a crypto virus. This protocol also enables client-side deduplication and compression for better backup and restore performance, and encryption in flight from the client to the PowerProtect DD.

Encryption

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

Encryption at Rest is a feature of the PowerProtect DD and can be enabled with either AES128 or AES256 (CBC or GCM). Encryption can be enabled at any time, with the option of encrypting any data that was previously written. The encryption keys can be managed by the PowerProtect DD or an external Key Manager.

Multi-Factor Authentication

Multifactor authentication adds an extra layer of security on the protection system by requiring the security officer and system administrator to enter an RSA SecurID passcode before certain destructive commands or configuration changes are allowed.

Dual Role Authorization

To provide an additional layer of protection for administering sensitive operations, such as changes to DD Encryption, DD Retention Lock Compliance, and archiving now require a second layer, out of band “security officer” approval.

In a typical scenario, an admin role user issues a command and, if security officer approval is required, the system displays a prompt for approval. To proceed with the original task, the security officer must enter his or her username and password on the same console at which the command was run. If the system recognizes the security officer credentials, the procedure is authorized. If not, a security alert is generated.

The creation of a Security Officer is required when Compliance Mode is enabled on the system, and optional when using Governance Mode.

Secure AD/LDAP Authentication

PowerProtect DD can use secure LDAP by enabling SSL. For LDAP for Active Directory, configure secure LDAP with SSL/TLS options.

Role-based Access

Role-based access control (RBAC) is an authentication policy that controls which DD System Manager controls and CLI commands a user can access on a system.

For example, users who are assigned the admin role can configure and monitor an entire system, while users who are assigned the user role are limited to monitoring a system. When logged into DD System Manager, users see only the program features that they are permitted to use based on the role assigned to the user.

SIEM/SOAR Integration

PowerProtect DD can be configured to send system log events to a remote server. Remote logging with syslog utilizes the Linux Syslog Daemon, syslogd, to send system messages to a syslog server using UDP port 514.

The PowerProtect DD Syslog configuration requirements are: IP address of the Syslog server Use of the PowerProtect DD log commands to enable the feature, add the syslog server, and verify configurations.

Integrated Lights Out Management Hardening

The PowerProtect DD supports the Integrated Dell Remote Access Controller (iDRAC) with Lifecycle Controller to remotely power the system off or on. This is a Dell proprietary access method for Dell specific hardware.

iDRAC provides functionality that helps IT administrators deploy, update, monitor, and maintain PowerProtect DD systems. iDRAC functions regardless of the operating system or the presence of a hypervisor.

When Retention Lock Compliance is enabled, the iDRAC admin users are disabled and the PowerProtect DD Security Officer oversight is required to allow iDRAC admin to be enabled for specific duration.

Secure System Clock

Retention Lock Compliance Edition enables advanced controls of the system time to prevent more sophisticated NTP or time-based attacks. When enabled, PowerProtect DD implements an internal security clock that is monitored against the system clock. When the variation between these two clocks reaches a designated value, the file system automatically shuts down to protect the data residing on the system. Only the security officer can resume the file system once it has shut down.

Additionally, the system can prevent NTP Clock Tampering by enforcing a maximum allowed amount to advance the system time and date, and a minimum amount of time in between changes. Alerts will be generated when the clock skew exceeds half of the date change limit.

Proprietary Operating System (DDOS)

The PowerProtect DD Operating System (DDOS) is built upon a hardened and custom version of Linux. Access is highly restricted to the underlying operating system and requires the PowerProtect DD Administrator, with Security Officer oversight, to generate a key from the system to send to Dell support to generate a response. Access is only granted for a short period of time to allow support to make very specific, low level configuration changes that require support oversight.

When Retention Lock Compliance Mode is enabled, the Security Officer is required to make any higher-level system changes or to reboot the system.

Proprietary File System (DDFS)

The PowerProtect DD File System (DDFS) was written to be the storage of last resort, knowing that even the smallest amount of corruption could potentially impact a large percentage of the backup files written to the PowerProtect DD. One of the methods utilized to protect that data in the file system was to implement an append only file system to ensure no containers would be partially overwritten and corrupt the existing data in the container.

While not its direct intent, it offers protection from a mass encryption or deletion event. When a file is deleted from the file system space used by that file is not immediately available for re-use. The reason for this is because the PowerProtect DD does not immediately know whether data which was referenced by the deleted file is also being de-duplicated against by other files and therefore whether it is safe to remove that data or not. When a file is modified or encrypted, the new data is written to a new container and the previous data is left in place to be analyzed during the Garbage Collection process.

Until the Garbage Collection process has run, any data that was deleted or encrypted can be recovered by Dell Support.

Data Invulnerability Architecture

The DDOS Data Invulnerability Architecture™ protects against data integrity issues from hardware and software failures. When writing to disk, the DDOS creates and stores checksums and self-describing metadata for all data received. After writing the data to disk, the DDOS then recomputes and verifies the checksums and metadata. After a backup completes, a validation process examines what was written to disk and verifies that all file segments are logically correct within the file system and that the data is identical before and after writing to disk.

In the background, the online verification operation continuously checks that data on the disks is correct and unchanged since the earlier validation process.

Storage in most systems is set up in a double-parity RAID 6 configuration (two parity drives). Also, most configurations include a hot spare in each enclosure, except in certain low-end series systems, which have eight or fewer disks. Each parity stripe has block checksums to ensure that data is correct. Checksums are constantly used during the online verification operation and while data is read from the system. With double parity, the system can fix simultaneous errors on as many as two disks.

To keep data synchronized during a hardware or power failure, the system uses NVRAM (nonvolatile RAM) to track outstanding I/O operations. An NVRAM card with fully charged batteries (the typical state) can retain data for hours, which is determined by the hardware in use.

When reading data back on a restore operation, the DDOS uses multiple layers of consistency checks to verify that restored data is correct.

Secure Remote Support Services

Secure Remote Support Services is a two-way remote connection between Dell Customer Service and Dell products. This connection enables remote monitoring, diagnosis, and repair. Secure Remote Services assures availability and optimization of the Dell EMC infrastructure and is a key component of Dell EMC industry-leading Customer Service. The connection is secure, high speed, and operates 24x7.

Secure Remote Services is the remote service solution application that is installed on one or more customer-supplied dedicated servers. For devices associated with a particular service, Secure Remote Services is the single point of entry and exit for all IP-based remote service activities.

Secure Remote Services functions as a communication broker between the managed devices, the Policy Manager, and the Dell enterprise. Secure Remote Services sets permissions for devices using the Policy Manager. Secure Remote Services is an HTTPS handler. All messages are encoded using standard XML and Simple Object Access Protocol (SOAP) application protocols. Secure Remote Services message types include:

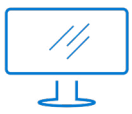
- Device state heartbeat polling
- Connect homes
- Remote access session initiation
- User authentication requests
- Device management synchronization

Isolated Data Vaulting

In addition to all the above capabilities, which are part of every PowerProtect DD, organizations can choose to create an additional level of protection using PowerProtect Cyber Recovery (PPCR). PPCR uses the three principles of isolation, immutability, and intelligence to create a protected third tier of data designed to enable an efficient recovery if portions or all of the production and/or DR environments are compromised in a ransomware or destructive attack. More information on PPCR is available at http://www.dell.com/cyberrecovery.

Conclusion

PowerProtect DD provides a number of embedded capabilities that help ensure your business is safe from a malicious attack. Cyber criminals are getting smarter by the day, and Dell Technologies continues to build our solutions with security in mind to give you peace of mind.



Learn more about PowerProtect DD

Contact a Dell Technologies Expert

View more Security resources

Join the conversation with #ZeroTrust