DELL Technologies

Dell PowerProtect Cyber Recovery vs. Rubrik Cyber Recovery 7.0

Immutability

Dell PowerProtect Cyber Recovery

Compliance
By configuring retention lock in compliance mode, PowerProtect Cyber Recovery is SEC 17a-4(f) compliant. Offers retention lock and WORM immutability along with security officer role and multifactor access credentials. Compliant since 2013.

NTP Protection
NTP source is optional and can be accessible from vault-only or from an external NTP source. The system accepts time changes to a specified maximum, and newer patent-pending protection provides more granular protection against NTP manipulation.

Protect System Configuration
Disaster recovery (DR) backup can be configured to preserve backup or Cyber Recovery configuration data and policies. Recovery is done by retrieving the backup data and then performing a recovery.

Rubrik Cyber Recovery 7.0

Compliance
If configured with Locked SLA Domains, Rubrik is SEC 17a-4(f) Compliant; a Request must be made to Rubrik Support for this feature. Offers immutability and administrative private-key authentication. Compliant since 2019.

NTP Protection
The customer must configure an external NTP clock; syncs NTP clock with the local clock. Customers must also configure a security attribute for NTP to encrypt keys to authenticate.

Protect System Configuration
The configuration data is not backed up externally from the cluster. Instead, a script must be used to back up and restore parts, not all, of the configuration.

Isolation

Dell PowerProtect Cyber Recovery

Air Gap
Productized "operational air gap" is stricter than other "air gap" definitions which typically claim isolation merely by storing data on a separate LAN segment or in the public cloud. PowerProtect Cyber Recovery "operational air gap" specifies a private vault network that is completely disconnected while locked; and only enables a data update/replication path when unlocked, never exposing access to the control plane. This tracks to the Sheltered Harbor data vaulting standard and NIST 800-209 Isolation. The process for ingestion of data and management is fully automated and controlled from the secure/vault side.

Security
Cyber Recovery also includes encryption, role-based access, and other security measures. But adds another layer of protection through isolation - air gapping the vault from the rest of the environment. This architecture prevents access to the vault outside of authorized, automated data syncs or recovery scenarios. The backup system does not operate the network connection. When the data transfer is complete, the connection is closed and the interface is disabled, thus reestablishing complete vault isolation.

Replication
When the air gap vault is briefly unlocked, only the replication destination is accessible to accept data. Vault components, including existing data and management controls to the system, are not accessible from the unsecure/low side.

Rubrik Cyber Recovery 7.0

Air Gap
Rubrik's solution focuses on the immutability of the backups, and the security of the platform. There is not a productized version that includes strict isolation as we define it. Rubrik touts Cloud Vault which is a cloud archive with a Rubrik software instance offered as a service. Rubrik claims the DR copy as a "logical" air gap simply by disabling ports and configuring firewall rules. Requires manual management.

Security
Rubrik claims a logical air gap through encryption, role-based access, and other security measures. They assert that you can achieve the same security outcomes of a physical air gap even though the environment is on the network. Rubrik's definition of a vault is an off-site cloud archive of the data offered as a SaaS solution in Azure. Recovering from a cloud archive back to a production environment will be slow or even impossible if external connections have been brought down to secure and isolate the compromised environment.

Replication
Replication is not controlled from an isolated vault and leverages existing replication or archive capabilities, accessible from production or public Internet, to provide a restorable copy. Firewall rules between Primary and DR copy are left up to the customer and are difficult to both validate as secure and manage at scale.

Intelligence

Dell PowerProtect Cyber Recovery

Integrity
Data Invulnerability Architecture (DIA) provides end-to-end verification; it confirms all file system data and metadata is correct and recoverable from every level of the system.

Data Types
CyberSense generates analytics from a comprehensive range of data types that includes core infrastructure such as DNS, LDAP, Active Directory, files such as documents, contracts, and intellectual property; VMware, SharePoint, and databases such as Oracle, DB2, SQL, SAP HANA, Epic Cachè, Exchange, etc. CyberSense also supports a variety of enterprise backup software.

Statistics
Analytics can take over 200 observations per file, including measurements requiring full content access such as entropy and similarity, along with metadata signals. These observations generate input to machine learning algorithms trained on millions of samples of clean and corrupted data, representing over 5500 ransomware variants with about 80 added each month. CyberSense finds corruption with up to 99.5% confidence and can diagnose the class and attack vector of the malware.[1]

Rubrik Cyber Recovery 7.0

Integrity
API is used to perform a backup verification job for an individual or batch of snapshot IDs; this validation supports VMware, AHV, and filesets only. The process is CPU intensive.

Data Types
Radar supports VMware, NAS, Linux, and Windows. Databases are not supported.

Statistics
Polaris Radar analyzes metadata to detect and report anomalies. It does not determine the attack vector or type of ransomware. Investigation of anomilies is performed in the cloud to compare current backup metadata to past backups to identify changes. If no anomolies are found in this comparison, false negatives may occur. Polaris performs checks including path, size, ACL details, UIDs, GIDS, Attributes, adding and moving files, and a sharp increase in encryption.

Sheltered Harbor

Dell PowerProtect Cyber Recovery is the first solution to receive endorsement for meeting all of the data vaulting requirements of the Sheltered Harbor standard, protecting U.S. financial institutions from cyber threats like ransomware.

[1] Based on Dell analysis of publicly available data, June 2022. Actual results may vary.