A Principled Technologies report: In-depth research. Real-world value.

Bolster your data protection plan with a fast-acting, more robust cyber recovery solution

Based on our research, Dell Technologies PowerProtect Cyber Recovery can offer physical isolation for backup vaults and deeper scanning for ransomware

Physical air gap isolation for backup vaults

Create a physical barrier that data cannot traverse

Deeper scanning for ransomware

CyberSense looks at file contents and databases, not just metadata

Scan 2X more anomaly workloads

Search for malware in more places with a single tool

The average cost of a ransomware attack increased almost 20 percent over two years to USD $5.23 million.[1] Efficient cyber recovery solutions can help reduce or even avoid these potential costs by enabling organizations to recover from incidents promptly, reduce data loss, minimize downtime, and, in the process, preserve their brand integrity. Solutions should pinpoint and restore known good data post-attack, ensuring the organization can salvage critical data and systems while helping to minimize business risk and downtime.

Dell PowerProtect Cyber Recovery (Cyber Recovery) is such a solution. It helps organizations protect their data and applications against ransomware, destructive cyberattacks, and unexpected events. This report uses publicly available data to contrast fundamental data protection features and functionality of Cyber Recovery and a competing solution, Rubrik Security Cloud (RSC). We specifically looked at features and functionality that cyber recovery solution customers might find important, including the recovery vault, immutability, workload support, scanning technology, recoverability, and isolation.

Unlike RSC, Cyber Recovery uses a multi-copy approach, meaning that after creating backups, it copies those backups (or normally, a selected subset) to isolated storage for safeguarding and analysis. Cyber Recovery comprises several components, including one or more storage vaults, located either on-premises in a PowerProtect Data Domain appliance or in the cloud via software-defined Dell APEX Protection Storage for Public Cloud. In comparison, RSC does not offer local vault options. Cyber Recovery also includes CyberSense, a fully automated and integrated intelligent security analytics engine that scans data, files, databases, and images in the vault for signs of corruption from a ransomware attack. The CyberSense solution can scan two times more anomaly workloads than the Rubrik solution, which could allow the CyberSense scanning ML (machine learning) to detect the impact of malware or other threat actor activity in more data. We'll dissect how PowerProtect Cyber Recovery works differently and could be more advantageous for your organization.

Product overview

Dell PowerProtect Cyber Recovery overview

Dell PowerProtect Cyber Recovery comprises a storage appliance that houses production data and a target storage appliance in the vault for replication. It also comprises Cyber Recovery software, which coordinates synchronization, manages multiple data copies on the PowerProtect Data Domain (PPDD) system in the Cyber Recovery vault, oversees the recovery process, and oversees the analytics process with CyberSense.

The solution transfers unique data from the production PPDD MTree to the vault counterpart via MTree replication and enables data immutability* for a set duration. The vault features a server that contains the Cyber Recovery software and a component where the solution restores backup applications and data. Each Cyber Recovery vault typically houses many such components. The vault also contains an analytics/indexing host equipped with data analysis software, providing direct integration between the Cyber Recovery software and CyberSense.

*Dell's products are designed to support customers' efforts to secure their critical data. As with any electronic product, data protection, storage, and other infrastructure products can experience security vulnerabilities. It is important that customers install security updates as soon as they are made available by Dell.

Figure 1 provides an overview of the Dell Cyber Recovery solution.

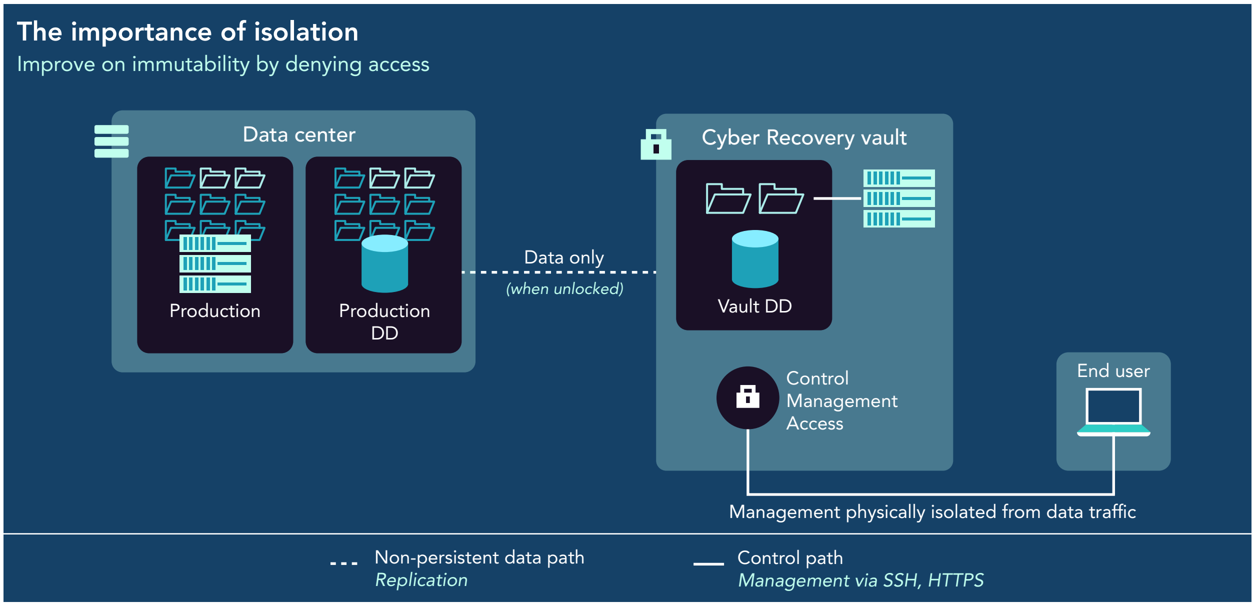
The importance of isolation
Improve on immutability by denying access
Data center
Production
Production DD
Data only
(when unlocked)
Cyber Recovery vault
Vault DD
Control Management Access
End user
Management physically isolated from data traffic
Non-persistent data path
Replication
Control path
Management via SSH, HTTPS

Figure 1: High-level data and control path architecture of the Cyber Recovery vault. Source: Principled Technologies.

To learn more about the key components of the Dell PowerProtect Cyber Recovery solution, read the Dell PowerProtect Cyber Recovery Solution Guide.

Rubrik Security Cloud overview

Rubrik describes Rubrik Security Cloud as a software-as-a-service (SaaS) platform that enables customers to "keep [their] data secure, monitor data risk, and quickly recover [their] data, wherever it lives—across the enterprise, in the cloud, and in SaaS applications."[4] Rubrik states that it built the solution on a "secure microservices architecture using high-availability services and infrastructure running in Google Cloud Platform (GCP)."[5] Figure 2 shows the general structure of Rubrik Security Cloud.

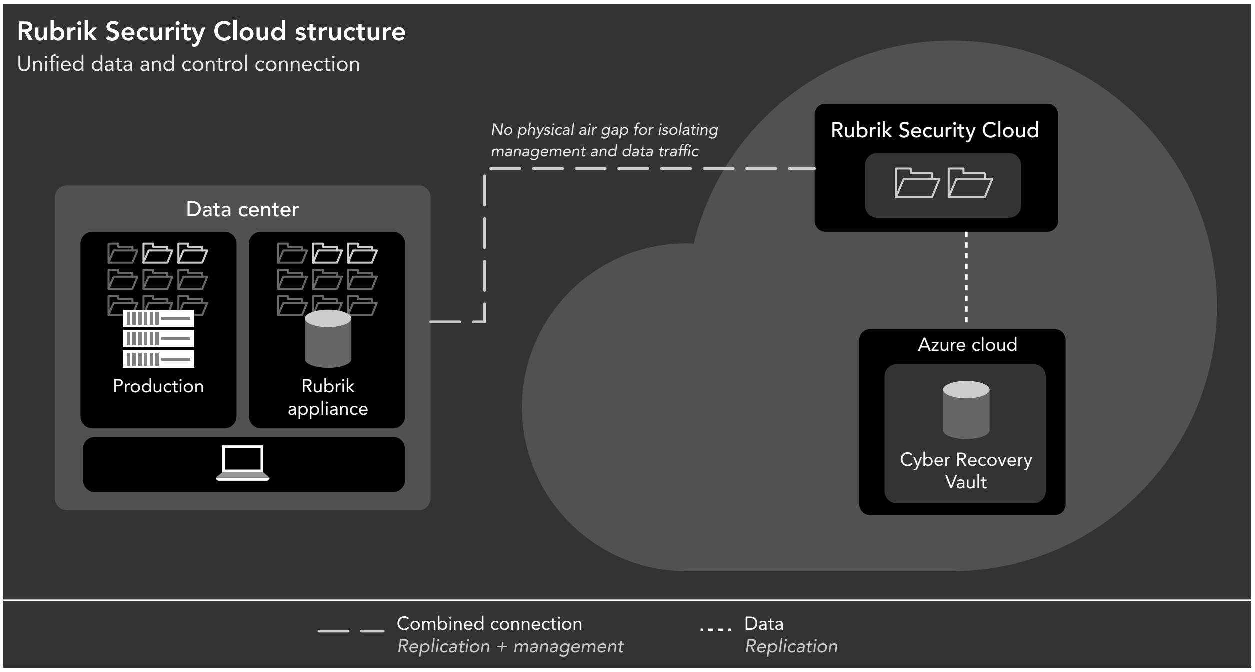

Figure 2: The general structure of Rubrik Security Cloud. Source: Principled Technologies.

Feature support

Recovery vault

Vaults are the dedicated storage that house encrypted copies of backups the solution takes within your production environment. The vaults are not part of the production backup solutions; instead, each serves as an isolated "backup to the backup" location from which customers can recover validated backups.

Dell offers several vault options, including on premises, at a remote colocation site, or within a public cloud. The on-premises vault leverages an operational air-gapped PPDD that resides in your data center, potentially even within the same rack as your backup solution. An air-gapped solution is normally physically isolated from the production environment. An off-site co-located vault requires dedicated network connections to a physical vault, like an on-premises version, but the vault is geographically separate in a remote data center. Dell also provides vaults within the public cloud, partnering with cloud service providers Amazon Web Services (AWS), Microsoft Azure, and Google Cloud. Public cloud vaults could provide configuration flexibility to meet customer needs.[6, 7, 8]

Rubrik Cyber Recovery is a component of the Rubrik Security Cloud. Provided through a software-as-a-service model, the recovery vault uses storage on Microsoft Azure only. Many of the publicly available documents we found in our research tie the Rubrik Cyber Recovery vault to the Rubrik Cloud Vault, the backup tier, which offers immutability.[9, 10] This vault requires no additional hardware and can be used by any version of the Rubrik Cloud Data Management (CDM) platform from version 6.02 onward.

Immutability

Immutability refers to the condition of being unchangeable or permanent. Immutable backups and backup copies allow administrators to create permanency for files that users or systems cannot modify or delete until an allotted timeframe has passed. Then the files "roll off"—the solution automatically removes them. Solutions typically perform this process through policies, or definitions that govern how the system treats files.[11]

Dell PowerProtect Cyber Recovery immutability relies on retention locks, via the Retention Lock feature, to prevent deletion or modification (for a period of time) or forced early expiration of backup copies. (The PPDD is an append-only file system, regardless of whether the organization has enabled Retention Lock or not.[12]) Dell customers manage backups using PPDD MTrees, which are user-defined logical partitions with independent retention settings that they assign as backup application destinations.[13] Customers can choose from two types of retention locks: governance and compliance. Compliance locks are the stricter and more secure of the two. Customers enable retention locks on a per-MTree basis, meaning all files within a given MTree will adhere to the retention lock definition for that MTree, and set the length of time for retention on a per-file level. Once customers define a compliance retention lock, no user or system can remove it. An administrator can revert a governance retention lock, the less strict option.[14]

The Rubrik solution's immutability also relies on retention locks to prevent deletion or forced early expiration of backup copies. Like PowerProtect Cyber Recovery, the Rubrik solution appends new data to the file system rather than overwriting existing data. The solution fingerprints incoming data and stores it with the data. **The Rubrik solution does not enable retention locks by default**, and customers must either open a ticket to Rubrik Support or enable a two-person rule to permit retention locks. (Prior to Rubrik Cloud Data Management version 7.0.1, customers needed to contact Rubrik support to enable retention locks; Rubrik documentation does not make clear whether customers may still contact support for this to work or not.) Once customers have enabled them, retention locks prevent users or systems from deleting data outside the defined parameters. Rubrik retention locks require an external Network Time Protocol (NTP) server for time synchronization, which may present an opportunity for bad actors to manipulate the reference NTP source and thereby expire retention locks prematurely.[15]

> *"The Rubrik solution does not enable retention locks by default, and customers must either open a ticket to Rubrik Support or enable a two-person rule to permit retention locks."*

Licensing and subscriptions

Dell PowerProtect Cyber Recovery is a licensed solution. During installation, Dell installs a 90-day evaluation license by default. After 90 days, customers must purchase a new license to continue using the product. Dell offers both standard (permanent) licensing and subscription-based licensing.

Rubrik integrates Rubrik Cyber Recovery into Rubrik Security Cloud (RSC). Customers must have a subscription to Rubrik Enterprise Edition to use Rubrik Cyber Recovery. Subscription terms are for three years.[16, 17] In the event of RSC failure, SAP HANA and Db2 workloads require third-party tools to recover data, which could incur additional subscription costs.[18]

Management access

Management of the Dell PowerProtect Cyber Recovery system is local to whichever topology customers choose for deployment. Because the solution initiates recovery from the vault, administrators log into the management UI from wherever their vault resides. On-premises vaults offer administrators local access without the need for internet access, which cyberattacks can severely impair, due to either denial of service attacks or from securing the data by severing the connection to the internet, as recommended by the National Institute of Standards and Technology (NIST). Co-located vaults allow for physical access to the appliance from a remote site and use connections outside the public internet. Cloud-based vaults would require internet access for recovery, which could delay on-site recovery until the cyberattack ended and normal network connectivity resumed.

Managing Rubrik Cyber Recovery requires access to Rubrik Security Cloud, which requires internet access. As we have noted, this kind of connectivity could delay on-site recovery until network functionality returns to normal following a cyberattack.

Because customers must have access to RSC to use Rubrik Cyber Recovery features, RSC becomes a single point of failure. If that service became unavailable, it would hinder recovery from the vault for the affected customer. Rubrik can recover 10 workloads during an RSC service disruption, but two database workloads require third-party tools and help from Rubrik Support to recover them.[19, 20] Additionally, compromised administrator accounts, or bad actors with access to the RSC platform, would gain access to the entire estate, rather than a single vault.

Get additional help with Managed Detection and Response from Dell

Some organizations may not feel comfortable with a "go it alone" approach to cyber security. Dell offers these customers Managed Detection and Response (MDR), a fully managed service that monitors and detects threats and risks and works with customers to mitigate those risks. According to Dell, the service offers the following:[21]

- Trusted support, including expert advice for deploying and configuring the extended detection and response (XDR) security analytics platforms that Dell supports
- Threat response and security configuration, including up to 40 hours of service-related security configuration included per quarter
- 24/7 detection and investigation, including proactive threat hunting specific to each customer's environment to discover new threats or variations of known threats that evade security systems
- Cyber incident response initiation, including 40 hours of annual remote incident response assistance that enables investigative activities to commence quickly

When coupled with APEX Cyber Recovery Services, MDR allows customers to choose from many options to monitor, detect, and mitigate threats and risks. The availability of options could mean expanded coverage or a hybrid approach that suits your organization's needs.

For more information on MDR, visit **https://www.dell.com/en-us/dt/services/managed-services/managed-workplace-services/managed-detection-response.htm**.

Seamlessness

Setup

Dell PowerProtect Cyber Recovery setup consists of software installation on a Linux system or creation of a VMware® vSphere® appliance from an Open Virtualization Format (OVF) template. Software installation requires 14 steps,[22] while the alternative vSphere appliance deployment requires 8 steps and takes 5 minutes.[23] After installation, administrators can access the solution via web browsers from within the isolated environment.

Customers need to separately deploy CyberSense, a fully automated and integrated intelligent security analytics engine.[24] The instructions for installing CyberSense in Dell PowerProtect Cyber Recovery are not publicly available.[25]

Dell has multiple metrics users can tune, including destruction detection objective (DDO), destruction assessment objective (DAO), Cyber Recovery point (CRP), Cyber Recovery time (CRT), Cyber Recovery synchronization interval, and Cyber Recovery data copy count. Dell also recommends characterizing data that needs protection. This data may be mission critical, business critical, dependent on core infrastructure services or other applications, or general, such as application binaries, boot images, and backup catalogs. The range of options gives customers full control over their backup environment and the ability to customize the classification of their data. Dell consulting services can also provide further assistance and suggestions.[26]

The Rubrik setup also consists of multiple steps. Before creating a cluster, Rubrik support services must install and configure Rubrik CDM. Then an administrator downloads and installs the most recent or desired version of CDM (15 steps).[27] Next, the administrator can set up a Rubrik cluster using the UI or the CLI. You can set up the cluster with the UI or CLI, with both approaches taking 24 steps.[28, 29] Then the administrator can register the Rubrik clusters using an online method (12 steps)[30] or offline method (18 steps).[31] Next, the administrator enables multi-factor authentication (MFA), which takes 13 steps.[32] Finally, the administrator adds the initial account (6 steps) and any other accounts.[33] Figure 3 shows the maximum number of possible steps to set up each cyber recovery solution.

Rubrik customers cannot tune other metrics, which could reduce flexibility to meet their needs. One reviewer claimed, "Most of the User Interface is quite straightforward and easy, but some areas are a bit lacking in a description of what the option is used for, or the option is missing. While making the user experience easy, many tunables aren't present and require a Support Tunnel to be open for a Support person to make a change in the customer's environment."[34]

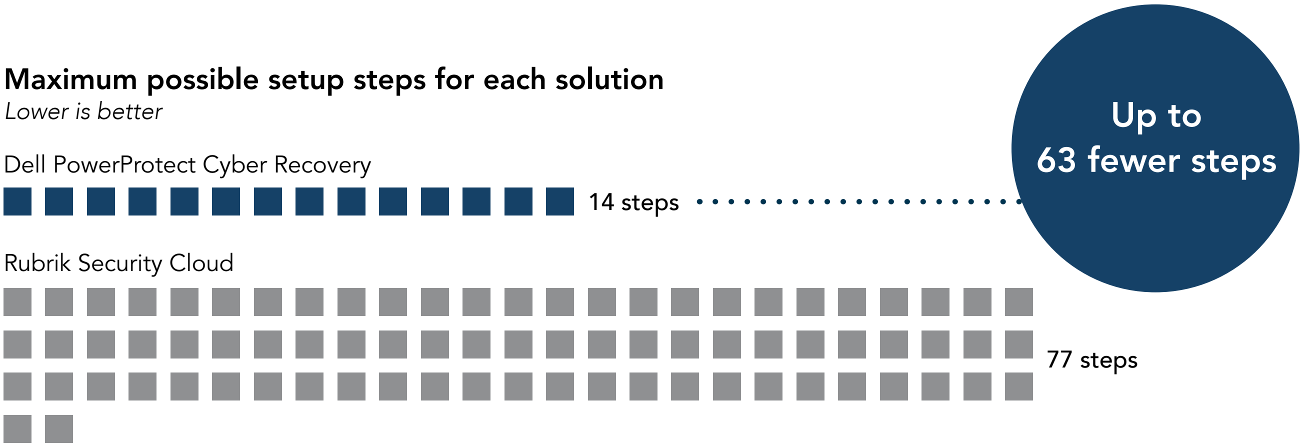

Figure 3: The maximum number of possible steps to set up Dell PowerProtect Cyber Recovery and Rubrik Security Cloud. Lower is better. Source: Principled Technologies.

Maintenance

We observed that after setup, the Dell and Rubrik UIs for performing daily maintenance operations are similar. After configuration, customers can configure Dell PowerProtect Cyber Recovery to do the following:[35, 36]

- Automatically generate Cyber Recovery jobs reports according to a schedule and in response to a manual user request
  - A user or schedule creates jobs when they initiate a policy, recovery operation, system backup, or cleaning operation
- Automatically monitor the vault status, storage capacity, Cyber Recovery operations, alerts when copy/sync fails or if the Cyber Recovery vault is down, and Cyber Recovery jobs
- Automatically and continuously scan for attacks and then display CyberSense alerts after them, in order of severity, giving the number of files, hosts, policies affected, specific threat detected, the point in time of the attack so you can find a clean backup, and a list of corrupted files to use in attack analysis

Similarly, customers can configure Rubrik to do the following:[37]

- Automatically use Rubrik Security Cloud to track, monitor, and display all events of all connected Rubrik clusters. It provides three event types:[38]
  - Critical - Events that require attention, such as failed backup, archive, or replication
  - Warning - A backup, archive, or recovery was finished
  - Informational - Information only
- Automatically and continuously scan snapshots for new and existing indicators of compromise using Threat Monitor, which gives the time the solution last took a snapshot, the event timeline, the detection time, the number of changed files, the number of suspicious files, the cluster name, and the object type and name

Anomaly workload support

Both Rubrik Security Cloud Data Threat Analytics and CyberSense scan multiple workload types, but according to the sources we found, CyberSense supports two times more anomaly detection workloads. This includes scanning the following types of workloads:

- VMs
- Core infrastructure
- User files that might contain documents, contracts, and intellectual property
- Databases
- Backups made by other clients

> *“If we count the number of supported workloads that we found in publicly available data, we find that CyberSense supports 21 anomaly detection workloads while Rubrik supports 7.”*

If we count the number of supported workloads that we found in publicly available data, we find that CyberSense supports 21 anomaly detection workloads while Rubrik supports 7. Therefore, according to publicly available data shared by each, CyberSense supports two times more workloads than Rubrik Security Cloud Data Threat Analytics. The more data that a cyber recovery solution can scan, the better chance it has to find sneaky malware or other corruption.

VM workload support

VM workloads refer to the applications, services, or tasks that VMs run on a physical host server or cloud environment. Because these workloads can vary in function and many other ways that could increase their exposure to malware, scanning VMs is essential. Rubrik Security Cloud Data Threat Analytics, which "comprises Anomaly Detection, Threat Monitoring, Threat Hunting, and data recovery services on protected resource,"[39] supports scanning of the following VM workloads:[40]

- VMware
- Nutanix® AHV
- Microsoft Hyper-V
- Microsoft Azure

CyberSense supports scanning of the following VM workloads:[41, 42, 43]

- VMware
- Amazon Web Services (AWS)
- Hyper-V, with Dell Avamar or Dell NetWorker backups

VMware claims that "as much as 80 percent of virtualized workloads run on VMware technology."[44] In the first quarter of 2024, the most popular vendor in the cloud infrastructure services market, Amazon Web Services (AWS), controlled 31 percent of the entire market. Microsoft Azure takes second place with 25 percent market share.[45]

Core infrastructure

Core infrastructure is the foundational components and services that enable the operation of a technology environment. Detecting malware at this level can help reduce the severity of an attack because core infrastructure functionality can affect many systems and users. Rubrik Security Cloud documentation does not mention support for scanning any core infrastructure.[46]

In contrast, CyberSense supports scanning of the following core infrastructure:[47]

- Active Directory
- DNS
- LDAP

User files that might contain documents, contracts, and intellectual property

Rubrik Security Cloud Data Threat Analytics supports scanning the following user files:[48]

- NAS file sets and datasets
- Windows volume groups
- Linux and Windows

CyberSense can scan Linux and Windows user files.[49]

Scanning databases

CyberSense 7 vs.
RSC Data Threat Analytics 0

Databases

Applications can use different types of databases for many reasons, so being able to detect the presence of malware in various databases could be pivotal to a rapid response. Rubrik Security Cloud Data Threat Analytics can back up databases, but we did not find public documentation where they can scan those database backups.

CyberSense supports scanning the following databases with page-level scans:[50]

- SQL
- Oracle®
- SAP HANA
- Db2
- PostgreSQL
- Epic® Caché
- MariaDB/MySQL

Backups made by other clients

Some organizations might have data backups from multiple vendors to provide redundancy, to comply with regulations, or some other significant reason. Rubrik Security Cloud documentation does not mention support for scanning backups made by other backup clients.[51]

With a clear advantage in this category, CyberSense supports scanning backups made by the following backup clients:[52, 53, 54]

- DNAS
- Exchange
- SQL
- Avamar
- NetWorker
- Commvault
- Veritas NetBackup

Scanning technology

Rubrik Security Cloud includes many tools for scanning and to help with scanning in Data Threat Analytics:

- Rubrik Anomaly Detection shows suspicious files, snapshot changes,[55] and anomaly details as anomaly incidents for customers to study and use in snapshot investigation.[56] The software also provides recovery options.[57]
- Rubrik VM Encryption Detection detects attacks on VMware vSphere virtual disk files.[58]
- Rubrik Threat Monitoring shows information about threats and matches detected.[59]
- Rubrik Threat Hunt is a user-initiated scan for indicators of compromise.[60]
- Rubrik Quarantine isolates objects that show up in a threat hunt.[61]

Rubrik RSC also has Rubrik Backup Service Connectors for each Rubrik cluster.

Rubrik customers must select the correct tool for their task, may have to initiate scans manually, or use multiple tools to accomplish their task. In contrast, Dell has a single CyberSense scanning option, which customers might find easier to manage and administer.

CyberSense scanning goes deeper than the "surface only" scanning from Rubrik RSC Data Threat Analytics. CyberSense performs full content scans of files and page-level scans of databases and can detect partial encryption of files.[62] The tool uses a machine learning (ML) database trained by Index Engines on thousands of data threats and contains over 200 analytics points to detect data corruption.[63] Unlike Rubrik Threat Monitoring and Threat Hunt, CyberSense doesn't rely on outside threat intelligence agencies to provide malware signatures. Instead, it discovers new threats.[64] **CyberSense also doesn't rely on arbitrary thresholds of acceptable file changes or entropy levels between snapshots that can lead to false negatives**, nor does it train its ML to a baseline of previous customer behavior.[65, 66, 67]

> *"CyberSense also doesn't rely on arbitrary thresholds of acceptable file changes or entropy levels between snapshots that can lead to false negatives…."*

The Rubrik anomaly detection software relies solely on metadata to determine if a snapshot is corrupt before doing any content analysis. In comparison to the CyberSense ongoing ML, Rubrik software discovers corruption after obtaining signatures. Rubrik anomaly detection needs to build a behavioral model to define a customer's normal baseline. This can take several backups to establish. The Rubrik behavioral model requires at least two backups to create a baseline of typical changes to a file system when there are no attacks. However, a single set of change statistics might not be enough to establish what is typical. Business events could trigger more or less activity or more suspicious types of activity that did not occur between the first and second Rubrik snapshot. The more backups that the Rubrik solution analyzes, the more accurately it can train its behavioral model to a baseline.[68, 69]

CyberSense contains all its analytics in the vault. In the filesystem behavior analysis pipeline, Rubrik sends metadata about customer file system changes up to the cloud-based Polaris platform to do the behavior analysis, opening an attack surface.[70]

Customers can use Rubrik Threat Monitoring and Threat Hunt only as part of the Rubrik Enterprise edition.[71] Customers must perform Threat Hunt scans with role-based access control (RBAC) privileges, and the users must indicate which specific indicators of compromise (IOC) they want to hunt.[72] This is not industry best practice.[73] Like CyberSense, Threat Hunt supports VMware, AHV, Hyper-V, NAS file sets, and Linux and Windows servers.[74]

The following sections offer more detail on how the Rubrik solution offers threat detection.

Metadata and file system statistics

The Rubrik Anomaly Detection ML behavioral model logs the changes to the file system since the last snapshot—such as number of files added, deleted, or moved—as metadata.[75] Then, an ML model trains on these changes to build a behavioral model "baseline" for the file system. Rubrik flags a snapshot as anomalous if it detects too many changes. After behavior analysis has flagged a snapshot, the solution begins a file content analysis.[76] Monitoring metadata may add a layer of security, but it might not offer the necessary protection that helps prevent or reduce downtime from an event.

> *"CyberSense does not need a baseline; it monitors and analyzes file and database content changes from the first backup copies."*

Conversely, **CyberSense does not need a baseline; it monitors and analyzes file and database content changes from the first backup copies.** The CyberSense approach offers more granularity, as the software analyzes even pieces of a file or individual pages of a database. Similar to the Rubrik solution, CyberSense scans include metadata properties and feed results into the ML engine. In contrast to the Rubrik solution, CyberSense is not limited to metadata scanning, and Index Engines trained its ML engine on attacks documented by Index Engines, not signatures or prior customer behavior.[77, 78]

Thresholds

During behavior analysis, Rubrik ML determines how likely it is that an anomaly occurred on a file system. If the Rubrik solution finds it likely, it performs content analysis. This could be a behavioral model-determined threshold for "anomalous behavior." For example, the Rubrik solution could flag anomalous behavior when it sees many new or modified files, or an increased randomness or encryption indicators.[79] During content analysis, Rubrik Anomaly Detection displays changes in file content and computes the probability of encryption by computing the entropy of the file system. The entropy of a file system helps show the likelihood that a ransomware attack has encrypted files. If the entropy exceeds an anomaly threshold, the solution alerts the user.[80, 81] The efficacy in detecting data corruption depends on threshold stringency. Too much allowance could cause false negatives and thus a false sense of security.[82] Customers must set thresholds appropriately.

By contrast, CyberSense checks for partial encryption of a file by scanning file content to provide a 99.99 percent confidence (according to Dell and Index Engines) in data corruption detection.[83]

Signatures and file extensions

Rubrik Threat Monitoring and Threat Hunts scan snapshots for IOCs. When one of the multiple threat intelligence sources that Rubrik monitors discovers a new IOC, Threat Monitoring pushes the threat feed containing Yet Another Ridiculous Acronym (YARA) rules for identification of the new malware, otherwise known as the malware signature, to all Rubrik clusters. The clusters then begin scanning.[84] A recent WatchGuard report suggests that 57.8 percent of malware avoids signature detection. Advanced malware, such as BianLian, can employ methods to evade signature recognition, and new malware variants can have slightly different signatures than the original. As such, it could be harder for threat intelligence to stay up to date.[85]

In comparison, CyberSense uses over 200 analytics and provides an ML model trained on thousands of ransomware variants. Index Engines has proven that the CyberSense method can detect previously unseen, sophisticated variants without downloading signatures,[86] which is another advantage of not relying on the internet during an event.

Mass encryption events

The Rubrik solution monitors for mass encryption events by computing the entropy of the entire file system.[87] CyberSense is much more granular. It doesn't just scan the file system in general, or even each individual file, but instead scans pieces of the internal contents of files. According to Index Engines, calculating entropy on only a whole file rather than pieces of it will "only detect extreme encryption of the entire file," or mass encryption events.[88]

Recoverability

Based on documentation, we consider recovery with Dell PowerProtect Cyber Recovery to be a simpler, more streamlined process than recovery with Rubrik. This section of the report, including its subsections, contrast recovery features of the two solutions and how the solutions implement those features.

Rubrik documentation notes which of their recovery features work for which VM types. This may seem to offer a useful level of granularity, but the many stipulations and variations make recovery complex. For example, when Rubrik customers need to recover data, files, and systems, they must select which snapshot objects they want to include in their recovery plan. After creating one or more recovery plans, Rubrik offers many recoverability options, including the following:[89, 90, 91, 92, 93]

- Recover files via download or overwrite and recover to a separate folder, export to a different host, or export to a clustered service
- Recover files for VMs via download or overwrite and recover to a separate folder or export into another virtual machine
- Full snapshot recovery of a VM or disk snapshot via the following:
  - Live Mount, which creates a new VM from the snapshot
  - Mount virtual disks, which creates new virtual disks from the snapshot
  - Instant Recovery, which replaces the current VM with a new VM created by the snapshot
  - Export, which creates a new VM from the snapshot in a selected datastore
  - Batch recovery of VMs
- Bulk Cyber Recovery for Recovery Plans via Live Mount and Export
- Rubrik Security Cloud Orchestrated Application recovery for VM disaster recovery to an isolated sandbox, remote site, or in place

Rubrik batch recovery further demonstrates complexity. Table 1 shows the batch recovery features Rubrik provides depending on the hypervisor.[94]

Table 1: Batch recovery features Rubrik provides for different hypervisors. Source: Rubrik.

VM creation options				
	Live Mount	**Live Mount with optional migration**	**Export**	**Instant recovery**
vSphere VMs	Available, uses the Rubrik cluster as its datastore	Not available	Available, uses the datastore of the recovered hypervisor	Available, uses the Rubrik cluster as its datastore
AHV VMs	Available, uses the Rubrik cluster as its datastore	Available, uses the Rubrik cluster as its datastore and uses the Nutanix container for all subsequent writes	Available, uses the Nutanix container as its datastore	Not available
Hyper-V virtual machines	Available, uses the Rubrik cluster as its datastore	Not available	Available, uses the datastore of the recovered hypervisor	Available, replaces current VM with a new one from the snapshot. Uses the Rubrik cluster as its datastore.

For the Rubrik solution, the recovered data store is typically on the Rubrik cluster and not in the production environment, which can create problems. We present these problems in the next section, "Rubrik limitations". In contrast, PowerProtect can place recovered data on recovery or production environments to help provide a faster, smoother recovery that could minimize downtime.

Table 2 shows additional information from Rubrik about recovery of vSphere VMs.[95] As the table shows, most vSphere recovery datastores are on the Rubrik cluster.

Table 2: Recovery features Rubrik provides for vSphere VMs. Source: Rubrik.

Recovery features Rubrik provides for vSphere				
Action	**Datastore**	**Power state**	**Network**	**Source VM**
Recover files	Not applicable	Not applicable	Not applicable	No impact
Live mount	Local Rubrik cluster	On or off	Disconnected	No impact
Mount virtual disks	Local Rubrik cluster	On	Disconnected	No impact
Instant recovery	Local Rubrik cluster	On	Connected (optional)	Powered off and renamed
Export	Datastore of hypervisor	Off	Disconnected	No impact
In-place recovery	Datastore of hypervisor	On	Same as the source VM	In-place recovery overwrites the virtual disk files of the source VM with the virtual disk data from the snapshot, without changing the properties of the VM

The Rubrik solution does not broadly implement bulk recovery, and the bulk recovery options are limited and complex. As the "Dell PowerProtect Data Manager offers the equivalent of Rubrik "mass restore"" section of this report further explains, Dell PowerProtect is streamlined and simpler.

Debunking mass restore

Rubrik advertises mass recovery, which it defines as restoring business operations quickly by recovering apps, files, or users at scale.[96] They offer many bulk recovery options. However, the Rubrik solution usually stores the recovered data on the Rubrik cluster and not in the production environment.[97] Workloads depend on the availability of the Rubrik system until the solution completes their migration. The local Rubrik cluster is tier 3 storage, so customers would have to do an additional migration into their production environment to return to planned performance levels. With this single point of failure and reduced performance while the system completes migration, we cannot consider recovery complete until the Rubrik solution restores the workloads to the production environment.

Dell PowerProtect also offers bulk recovery by enabling users to select multiple VMs for recovery in its recovery UI.

Dell PowerProtect Data Manager offers the equivalent of Rubrik "mass restore"

In comparison to the Rubrik solution, the Dell solution also offers multiple equivalent recovery options for vSphere VMs. Dell PowerProtect can place VM data on recovery or production environments. Most Rubrik options place data on the Rubrik cluster only. Table 3 shows the Dell recovery options.[98, 99, 100, 101]

Table 3: Dell recovery options. Source: Principled Technologies.

Dell recovery options	
Type	**About the feature**
File level restore	Restores only infected files in place, or by rollback
Live VM	Restores a VM to the cluster with later migration to production
Restore to new	Restores to the original environment or new environment (e.g., a clean room or recovery infrastructure), and during which users may select multiple VMs at once for a bulk restore or at scale restore
Access/Live VM	Creates an isolated copy of production data
Recovery Orchestration	Enables admins to schedule recovery or make it available on demand; prioritizes automatic recovery of VMs to production or recovery environment

Rubrik limitations

The Rubrik solution quarantines snapshots infected with malware for future analysis. However, the Rubrik solution does not quarantine snapshots by default. Customers can then download and perform forensic analysis on the quarantined files themselves manually or with third-party tools, potentially opening themselves up to malware.[102, 103]

> *CyberSense conducts its analysis without requiring the user to perform their own forensics, and the software automates the creation of restore points.*

CyberSense analyzes files and databases by default. Users do not need to quarantine snapshots manually. **CyberSense conducts its analysis without requiring the user to perform their own forensics, and the software automates the creation of restore points.**[104]

Rubrik RSC in RSC-only management mode is a single point of failure for many features. Most concerning, an attack could cause an RSC service disruption that affects user internet connectivity or connectivity between the user site and the RSC. After such attacks, the solution provides a limited set of features to users, available through the Rubrik CDM UI or API based automation, but only if the users created an RSC service account prior to the attack.[105, 106] An organization can recover the following workloads and data without the RSC: MongoDB, Microsoft Exchange, files, Hyper-V snapshots, Live Mount from managed volumes, NAS host files, Oracle, SQL Server, VCD, and VMware.[107] Recovering SAP HANA without the RSC requires third-party tools, such as Studio and Cockpit Cross, and Rubrik support via the Support tunnel. Recovering IBM Db2 without the RSC requires IBM third-party tools and Rubrik support via the Support tunnel as well.[108]

Air gap/isolation

NIST defines an air gap as "an interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control)."[109]

Air gaps can help control the flow of data from a source to a target and can be an important component of any ransomware protection and cyber recovery strategy. If an attack or event compromises your production backup systems, the ability to prevent traffic from your production systems to protected backups in your cyber recovery vaults could offer a failsafe.

Physical isolation

You may have seen an example of a physically isolated solution in the movie Mission Impossible, where the main character had to bypass all other facility security features to access sensitive data on a computer system that was not connected to any external network. Physical isolation may also use normally disconnected segments of dedicated physical networking to transport backup copies from your production systems to the vault. When disconnected, these operational air gaps create a physical barrier that data cannot cross automically, making access harder for bad actors to gain.

Organizations can physically isolate Dell PowerProtect Cyber Recovery to help enable an operational air gap strategy. The solution uses a dedicated physical connection and performs data replication as a pull operation from the vault rather than a push operation from the backup solution. During copy/replication, the solution activates the connection, encrypts data, and migrates it across the dedicated line.[110] After completing replication, the solution disables the connection again from the vault side. The solution makes vault copies immutable with locked retention policies, so that even if a user or system obtains access, they cannot modify or delete the vault copies. No management traffic traverses the replication pathway, so **even if bad actors gain control of your on-prem backup solution, the vault initiates and disconnects the replication path and uses one-way, data-only pulls from the data source, thereby limiting direct access to the vault.**[111]

Logical isolation

Logical isolation, on the other hand, use systems that may reside on the same physical network, but create logical network separation and control to ensure that systems cannot send data among each other. The solution uses additional security implementations, such as encryption and hashing along with RBAC and multi-factor authentication, to ensure an unauthorized system or user cannot read the data residing within another system.

Rubrik describes its cyber recovery feature as leveraging a logical air gap strategy.[112, 113] Many of the available Rubrik public statements cast doubt on the necessity of air gaps. A Rubrik presentation entitled "Rubrik Security – Air Gap and Immutability" claims that their native solution is air gapped because there's no way to access or edit the backups once the solution takes them, even though the Rubrik appliance remains on the physical network.[114] However, an authenticated bad actor could still gain access to the appliance GUI, which could have ramifications for recovery. To mitigate this, Rubrik has retention locks that prevent the expiration of backups, which makes them immutable. Once enabled, retention locks also prevent a Rubrik cluster from being factory reset and wiped. According to the Rubrik CDM Security Guide, the solution globally disables retention locks on the cluster by default and requires customers to contact Rubrik Support to enable them.[115] Publicly available sources do not clarify if Rubrik Support can also disable retention locks, which raises the specter of an authorized bad actor still being able to bypass the layers of security.

> *No management traffic traverses the replication pathway, so even if bad actors gain control of your on-prem backup solution, the vault initiates and disconnects the replication path and uses one-way, data-only pulls from the data source, thereby limiting direct access to the vault.*

Conclusion

Organizations must actively consider numerous attack vectors on their data centers. A good data protection plan seeks to safeguard all data, particularly the critical data essential to operations. We looked at publicly available information for Dell PowerProtect Cyber Recovery and Rubrik Secure Cloud to see how both solutions approach data management, protection, and recovery.

PowerProtect Cyber Recovery physically isolates backup copies of critical data in a vault and ensures its recoverability in the event of a cyberattack. The solution employs an operational air gap strategy with physical isolation, something Rubrik Secure Cloud cannot claim—the solution relies on logical isolation.

Cyber Recovery uses ML-based analytics in CyberSense to assess the integrity of data in the vault and identify clean backup data for recovery. Rubrik Secure Cloud, in contrast, offers an ML-trained analytics tool that looks for anomalies as opposed to performing deep scans on files.

Moreover, the Cyber Recovery solution offers multiple recovery options, leveraging uncompromised data from the vault to facilitate an efficient and seamless return to operations. In many cases, the PowerProtect Cyber Recovery could offer features and advantages that Rubrik Secure Cloud lacks, thus offering a potentially more secure solution capable of deeper analysis to minimize downtime and speed recovery.

[1] Anastasia Dergacheva and Jesse R. Taylor, "Study Finds Average Cost of Data Breaches Continued to Rise in 2023," accessed July 25, 2024, https://www.morganlewis.com/blogs/sourcingatmorganlewis/2024/03/study-finds-average-cost-of-data-breaches-continued-to-rise-in-2023.

[2] Dell, "Dell PowerProtect Cyber Recovery Solution Guide," accessed April 18, 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.

[3] Dell, "Dell PowerProtect Cyber Recovery Solution Guide."

[4] Rubrik, "Rubrik Security Cloud Architecture and Security Implementation," accessed April 18, 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf.

[5] Rubrik, "Rubrik Security Cloud Architecture and Security Implementation," accessed April 18, 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf.

[6] Rob Emsley, "Public Cloud Vault to Secure, Isolate and Recover Data," accessed March 20, 2024, https://www.dell.com/en-us/blog/public-cloud-vault-to-secure-isolate-and-recover-data/.

7. Brian White, “Dell’s PowerProtect Cyber Recovery Expands to Microsoft Azure,” accessed March 20, 2024, https://www.dell.com/en-us/blog/dells-powerprotect-cyber-recovery-expands-to-microsoft-azure/.
8. Dell, “Cyber Recovery on Google Cloud Platform,” accessed March 20, 2024, https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-cyber-recovery-reference-architecture/cyber-recovery-on-google-cloud-platform/.
9. Chris Mellor, “Up to $5m compensation if Rubrik Cloud Vault recovery busted,” accessed March 20, 2024, https://blocksandfiles.com/2022/02/24/up-to-5m-compensation-if-rubrik-cloud-vault-recovery-busted/.
10. Kristina Avrionova, “Frequently Asked Questions about Rubrik Cloud Vault,” accessed March 20, 2024, https://www.rubrik.com/blog/company/22/3/faq-about-rubrik-cloud-vault.
11. Chris Wahl, “Recovering Fast from Ransomware Attacks: The Magic of an Immutable Backup Architecture,” accessed March 22, 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf.
12. Dell, “Data Domain Invulnerability Architecture: Enhancing Data Integrity and Recoverability,” accessed June 7, 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/h7219-data-domain-data-invul-arch-wp.pdf.
13. Dell, “Consolidate Governance and Compliance Archive Data,” accessed April 4, 2024, https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-data-domain-retention-lock/consolidate-governance-and-compliance-archive-data/.
14. Dell, “Dell PowerProtect Cyber Recovery Solution Guide,” accessed March 24, 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
15. Rubrik, “Retention-locked SLA Domain attributes,” accessed April 2, 2024, https://docs.rubrik.com/en-us/8.0/ug/cdm/attributes_of_retention_locked_sla_domains.html.
16. Rubrik, “Rubrik Cyber Recovery,” accessed March 20, 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/brf-rubrik-cyber-recovery.pdf.
17. Rubrik, “Rubrik Licensing: Subscribe to Simplicity,” accessed March 20, 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/data-sheet/rubrik-licensing-data-sheet.pdf.
18. Rubrik, “Workloads require third-party tools for recovery,” accessed May 6, 2024, https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html.
19. Rubrik, “Recoverable workloads during RSC service disruption,” accessed May 6, 2024, https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html.
20. Rubrik, “Workloads require third-party tools for recovery.”
21. Dell, “Strengthen your security posture with Managed Detection and Response,” accessed April 2, 2024, https://www.delltechnologies.com/asset/pl-pl/services/managed-services/technical-support/managed-detection-and-response-datasheet.pdf.
22. Dell, “Dell PowerProtect Cyber Recovery 19.13 Installation Guide,” accessed March 20, 2024, https://www.dell.com/support/manuals/en-us/cyber-recovery/irs_p_19.13_installation/installing-the-cyber-recovery-software?guid=guid-8718978d-ddd0-4dc0-bca7-fb04a2f3d1fb&lang=en-us.
23. Dell, “Dell PowerProtect Cyber Recovery 19.13 Installation Guide.”
24. Dell, “Dell PowerProtect Cyber Recovery 19.13 Installation Guide.”
25. Dell, “Installing CyberSense in Dell PowerProtect Cyber Recovery,” accessed March 20, 2024, https://infohub.delltechnologies.com/en-US/l/ransomware-protection-secure-your-data-on-dell-powerflex-with-powerprotect-cyber-recovery-1/installing-cybersense-in-dell-powerprotect-cyber-recovery-1/.
26. Dell, “Dell PowerProtect Cyber Recovery Solution Guide.”
27. Rubrik, “Downloading and installing Rubrik CDM,” accessed March 20, 2024, https://docs.rubrik.com/en-us/saas/install/download_install_cdm_on_appliance_nodes.html.
28. Rubrik, “Setting up a Rubrik cluster using the UI,” accessed March 20, 2024, https://docs.rubrik.com/en-us/saas/install/setting_up_ui.html.
29. Rubrik, “Setting up a Rubrik cluster using the CLI,” accessed March 20, 2024, https://docs.rubrik.com/en-us/saas/install/setting_up_cli.html.
30. Rubrik, “Registering Rubrik clusters using the online method,” accessed March 20, 2024, https://docs.rubrik.com/en-us/saas/install/registering_clusters_online.html.
31. Rubrik, “Registering Rubrik clusters using the offline method,” accessed April 2, 2024, https://docs.rubrik.com/en-us/saas/install/registering_clusters_offline.html.
32. Rubrik, “Enabling MFA,” accessed March 21, 2024, https://docs.rubrik.com/en-us/saas/install/rsc_enabling_mfa.html.
33. Rubrik, “Adding the initial account,” March 21, 2024, https://docs.rubrik.com/en-us/saas/saas/adding_the_initial_account.html.
34. TrustRadius, “Learning Rubrik by putting the pieces together Brik by Brik,” accessed March 21, 2024, https://www.trustradius.com/reviews/rubrik-2023-09-20-21-03-04.
35. Dell, “Dell PowerProtect Cyber Recovery Solution Guide.”

36. Index Engines, “CyberSense®: How it Works,” accessed March 21, 2024, https://www.indexengines.com/how-it-works.
37. Rubrik, “Anomaly event details,” accessed March 21, 2024, https://docs.rubrik.com/en-us/saas/saas/anomaly_event_details.html.
38. Rubrik, “Events page,” accessed March 21, 2024, https://docs.rubrik.com/en-us/saas/saas/common/events_page.html.
39. Rubrik, “RSC Data Threat Analytics,” accessed March 21, 2024, https://docs.rubrik.com/en-us/saas/saas/ri_ransomware_monitoring.html.
40. Rubrik, “RSC Data Threat Analytics.”
41. Dell Technologies, “Dell PowerProtect Cyber Recovery: Reference Architecture,” accessed May 6, 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/h18661-dell-powerprotect-cyber-recovery-reference-architecture-wp.pdf.
42. Dell Technologies, “Dell EMC Avamar for Hyper-V,” accessed May 16, 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu89876.pdf.
43. Dell Technologies, “Dell EMC NetWorker Module for Microsoft for Hyper-V,” accessed May 16, 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu92011.pdf.
44. VMware, “Accelerate IT. Innovate with your cloud.,” May 9, 2024, https://www.vmware.com/files/pdf/VMware-Corporate-Brochure-BR-EN.pdf.
45. Statista, “Cloud infrastructure services vendor market share worldwide from fourth quarter 2017 to first quarter 2024,” July 17, 2024, https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/.
46. Rubrik, “RSC Data Threat Analytics.”
47. Dell Technologies, “CyberSense® for PowerProtect Cyber Recovery,” accessed June 27, 2024, https://www.delltechnologies.com/asset/en-gb/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf.
48. Rubrik, “RSC Data Threat Analytics.”
49. Index Engines, “CyberSense® Support Matrix,” accessed March 21, 2024, https://www.indexengines.com/csmatrix.
50. Dell Technologies, “CyberSense® for PowerProtect Cyber Recovery.”
51. Rubrik, “Keep Your Databases Running in the Face of Any Threat.”
52. Index Engines, “CyberSense® Support Matrix.”
53. Dell Technologies, “Dell EMC Avamar for Hyper-V.”
54. Dell Technologies, “Dell EMC NetWorker Module for Microsoft for Hyper-V.”
55. Rubrik, “Anomaly incidents,” accessed April 2, 2024, https://docs.rubrik.com/en-us/saas/saas/anomaly_incident.html.
56. Rubrik, “Data Threat Analytics events,” accessed April 2, 2024, https://docs.rubrik.com/en-us/saas/saas/ri_events.html.
57. Rubrik, “Viewing Anomaly Detection,” accessed April 2, 2024, https://docs.rubrik.com/en-us/saas/saas/viewing_ri_investigations.html.
58. Rubrik, “VM Encryption Detection,” accessed April 2, 2024, https://docs.rubrik.com/en-us/saas/saas/vm_encryption_detection.html.
59. Rubrik, “Viewing the Threat Monitoring page,” April 2, 2024, https://docs.rubrik.com/en-us/saas/saas/viewing_the_threat_monitoring_page.html.
60. Rubrik, “Initiating a threat hunt,” accessed April 2, 2024, https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html.
61. Rubrik, “Quarantining matched files or objects,” accessed April 2, 2024, https://docs.rubrik.com/en-us/saas/saas/quarantining_matched_objects_or_files.html.
62. Dell, “CyberSense® for PowerProtect Cyber Recovery.”
63. Dell, “CyberSense® for PowerProtect Cyber Recovery.”
64. Index Engines, “The Power of CyberSense’s Machine Learning,” accessed April 2, 2024, https://go.indexengines.com/csmachinelearning.
65. Index Engines, “The Power of CyberSense’s Machine Learning.”
66. Index Engines, “The Power of CyberSense’s Machine Learning.”
67. Dell, “CyberSense® for PowerProtect Cyber Recovery.”
68. Rubrik, “Anomaly Detection behavioral model,” accessed May 20, 2024, https://docs.rubrik.com/en-us/saas/saas/anomaly_detection_behavioral_model.html.
69. Amazon, “Training ML Models,” accessed April 2, 2024, https://docs.aws.amazon.com/machine-learning/latest/dg/training-ml-models.html.
70. Rubrik, “Defense in Depth with Polaris Radar,” accessed March 21, 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/Defense-In-Depth-Polaris-Radar-Technical-White-Paper.pdf.
71. Rubrik, “Data Threat Analytics dashboard,” accessed March 21, 2024, https://docs.rubrik.com/en-us/saas/saas/ri_dashboard.html.
72. Rubrik, “Initiating a threat hunt,” accessed March 21, 2024, https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html.
73. SentinelOne, “What Is A Malware File Signature (And How Does It Work)?” accessed April 4, 2024, https://www.sentinelone.com/blog/what-is-a-malware-file-signature-and-how-does-it-work/.

[74] Rubrik, “Threat hunts,” accessed March 21, 2024, https://docs.rubrik.com/en-us/saas/saas/ri_threat_hunts.html.

[75] Rubrik, “Anomaly Detection features,” accessed March 22, 2024, https://docs.rubrik.com/en-us/saas/saas/ri_features.html.

[76] Rubrik, “Behavioral model.”

[77] Index Engines, “The Power of CyberSense’s Machine Learning.”

[78] Dell, “CyberSense® for PowerProtect Cyber Recovery.”

[79] Rubrik, “Behavioral model.”

[80] Rubrik, “Anomaly Detection features.”

[81] Rubrik, “Behavioral model.”

[82] Dell, “CyberSense® for PowerProtect Cyber Recovery.”

[83] Morningstar, “Index Engines’ CyberSense Announces 99.99% SLA in Detecting Ransomware Corruption, Empowering Smarter Recovery,” accessed July 17, 2024, https://www.morningstar.com/news/pr-newswire/20240618ny41171/index-engines-cybersense-announces-9999-sla-in-detecting-ransomware-corruption-empowering-smarter-recovery.

[84] Rubrik, “Threat Monitoring,” accessed March 22, 2024, https://docs.rubrik.com/en-us/saas/saas/threat_monitoring.html.

[85] Index Engines, “The Power of CyberSense’s Machine Learning.”

[86] Index Engines, “The Power of CyberSense’s Machine Learning.”

[87] Rubrik, “Anomaly Detection features,” accessed March 22, 2024, https://docs.rubrik.com/en-us/saas/saas/ri_features.html.

[88] Index Engines, “The Power of CyberSense’s Machine Learning.”

[89] Rubrik, “Investigating and recovering anomalous files for filesets,” accessed March 22, 2024, https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files.html.

[90] Rubrik, “Investigating and recovering anomalous files for virtual machines,” accessed March 22, 2024, https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files_for_virtual_machines.html.

[91] Rubrik, “Full snapshot recovery of a virtual machine,” accessed March 22, 2024, https://docs.rubrik.com/en-us/saas/saas/full_snapshot_recovery_of_a_virtual_machine.html.

[92] Rubrik, “Recovery of a batch of virtual machines,” accessed March 22, 2024, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.

[93] Rubrik, “Performing bulk recovery for Recovery Plans,” accessed March 22, 2024, https://docs.rubrik.com/en-us/saas/saas/performing_bulk_recovery_for_recovery-plans.html.

[94] Rubrik, “Recovery of a batch of virtual machines,” accessed April 4, 2024, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.

[95] Rubrik, “Recovery of virtual machines,” accessed April 16, 2024, https://docs.rubrik.com/en-us/saas/saas/vs_recovery_vm.html.

[96] The recovered data store is usually on the Rubrik cluster and not in the production environment.

[97] Rubrik, “Recovery of a batch of virtual machines,” accessed April 16, 2024, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.

[98] Dell, “Restore plan,” accessed April 16, 2024, https://infohub.delltechnologies.com/en-US/l/powerprotect-data-manager-protection-for-vmware-cloud-foundation-on-dell-emc-vxrail-1/restore-plan/.

[99] Dell, “PowerProtect Data Manager overview,” accessed April 16, 2024, https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-data-manager-deployment-best-practices-1/powerprotect-data-manager-overview-4/.

[100] Dell, “PowerProtect Data Manager 19.9 Administration and User Guide,” accessed April 16, 2024, https://www.dell.com/support/manuals/en-us/enterprise-copy-data-management/pp-dm_19.9_ag/file-level-restore-of-a-powerprotect-backup-in-the-vsphere-client.

[101] Dell, “Recovery Orchestration with PowerProtect Data Manager Overview,” accessed April 16, 2024, https://www.youtube.com/watch?v=po2oMnAg_x4.

[102] Rubrik, “Quarantine files or objects,” March 24, 2024, https://docs.rubrik.com/en-us/saas/saas/quarantine.html.

[103] Rubrik, “Downloading quarantined files for forensic analysis,” March 24, 2024, https://docs.rubrik.com/en-us/saas/saas/downloading_quarantined_files_for_forensic_analysis.html.

[104] Forrester, “The Total Economic Impact™ Of Dell PowerProtect Cyber Recovery,” accessed April 16, 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/the-total-economic-impact-dell-powerprotect-cyber-recovery.pdf.

[105] Rubrik, “Workload recovery during an RSC service disruption,” accessed April 16, 2024, https://docs.rubrik.com/en-us/saas/saas/workload_recovery_during_rsc_outage.html.

[106] Rubrik, “Rubrik CDM APIs and service account workflows,” accessed April 16, 2024, https://docs.rubrik.com/en-us/saas/saas/rubrik_apis_sa_workflows.html.

[107] Rubrik, “Recoverable workloads during RSC service disruption,” accessed April 16, 2024, https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html.

[108] Rubrik, “Workloads require third-party tools for recovery,” accessed April 16, 2024, https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html.

109. NIST, “Computer Security Resource Center Glossary: air gap,” accessed July 29, 2024, https://csrc.nist.gov/glossary/term/air_gap.

110. Dell, “Dell PowerProtect Cyber Recovery Solution Guide.”

111. Dell, “Dell PowerProtect Cyber Recovery: Reference Architecture.”

112. Adam Eckerle, “Debunking the Myths about Air Gaps,” accessed March 14, 2024, https://www.rubrik.com/blog/technology/2021/11/debunking-the-myths-about-air-gaps.

113. Rubrik, “Air-Gap, Isolated Recovery, and Ransomware - Cost vs. Value,” accessed March 14, 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/Air-Gap-Isolated-Recovery-and-Ransomware-Cost-vs.-Value.pdf.

114. Brian Williams, “Rubrik Air Gap and Immutability,” accessed March 14, 2024, https://vimeo.com/561870246.

115. Rubrik, “Retention locks in the Rubrik cluster,” accessed March 18, 2024, https://docs.rubrik.com/en-us/9.0/sg/security_guide/retention_locks_in_the_rubrik_cluster.html.

This project was commissioned by Dell Technologies.

Principled Technologies®

Facts matter.®

DISCLAIMER OF WARRANTIES; LIMITATION OF LIABILITY:
Principled Technologies, Inc. has made reasonable efforts to ensure the accuracy and validity of its testing, however, Principled Technologies, Inc. specifically disclaims any warranty, expressed or implied, relating to the test results and analysis, their accuracy, completeness or quality, including any implied warranty of fitness for any particular purpose. All persons or entities relying on the results of any testing do so at their own risk, and agree that Principled Technologies, Inc., its employees and its subcontractors shall have no liability whatsoever from any claim of loss or damage on account of any alleged error or defect in any testing procedure or result.

In no event shall Principled Technologies, Inc. be liable for indirect, special, incidental, or consequential damages in connection with its testing, even if advised of the possibility of such damages. In no event shall Principled Technologies, Inc.’s liability, including for direct damages, exceed the amounts paid in connection with Principled Technologies, Inc.’s testing. Customer’s sole and exclusive remedies are as set forth herein.