

# New Principled Technologies research study compares Dell PowerProtect Cyber Recovery and Rubrik Security Cloud

*Based on research, Principled Technologies (PT) determined that Dell PowerProtect Cyber Recovery can offer helpful backup and data protection advantages*

DURHAM, NORTH CAROLINA, UNITED STATES, August 13, 2024 /EINPresswire.com/ -- To reduce or even potentially avoid the increasing costs of a data breach, some organizations choose to utilize cyber recovery solutions. An efficient solution can enable businesses to recover from incidents promptly, reduce data loss, minimize downtime, and, in the process, preserve their brand integrity. PT researched publicly available sources to compare two competing solutions: Dell PowerProtect Cyber Recovery (Cyber Recovery) and Rubrik Security Cloud (RSC). They looked at features and functionality that customers may find important, including the recovery vault, scanning technology, and more.

According to the report, "PowerProtect Cyber Recovery isolates backup copies of critical data in a physically air-gapped vault and ensures its recoverability in the event of a cyberattack. The physical air gap is something Cyber Rubrik Secure Cloud cannot claim—the solution relies on a logical air gap. 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 anomalous user behavior only 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."



**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

The average cost of a ransomware attack increased almost 20 percent over two years to USD \$5.23 million.<sup>1</sup> 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.

- 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

**Bolster your data protection plan with a fast-acting, more robust cyber recovery solution** August 2024

To learn more, read the report at <https://facts.pt/x5n2NqR> or see the infographic at <https://facts.pt/TEt27Z0>.

About Principled Technologies, Inc.

Principled Technologies, Inc. is the leading provider of technology marketing and learning & development services.

Principled Technologies, Inc. is located in Durham, North Carolina, USA. For more information, please visit [www.principledtechnologies.com](http://www.principledtechnologies.com).

Sharon Horton

Principled Technologies, Inc.

[email us here](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/735204608>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2024 Newsmatics Inc. All Right Reserved.