DELL Technologies

Solution Brief

Dell EMC PowerProtect Cyber Recovery for Healthcare

The Last Line of Data Protection Defense Against Cyber-Attacks

Why Dell EMC Power Protect Cyber Recovery?

Recovery is the key, ensuring your business-critical data can withstand a cyberattack designed to destroy your data including backups and replicas. Could you survive? Here are the five steps to building a last line of defense:

Solutions Planning - Selection of application candidates, recovery time, and recovery point objectives.

Isolation & Governance – An isolated data center environment that is disconnected from the network and restricted from users other than those with proper clearance.

Automated Data Copy and Air Gap Software to create immutable data copies to a tertiary backup target as well as processes to create an operational air gap between the production environment and the isolated recovery zone.

Integrity Checking & Alerting - Workflows to stage replicated data in the isolated recovery zone and perform validation checks to analyze whether it is impacted by malware along with mechanisms to trigger alerts on suspicious executables and data.

Recovery & Remediation - Enable procedures to perform recovery / remediation after an incident using dynamic restore processes and your existing DR procedures. Automated recovery is available with Dell EMC NetWorker.

Data Breaches in Healthcare are going up, up, up – an industry under attack

Ripe with rich financial, personal and medical information, healthcare finds itself a prime target for cyberattacks. The consequences of a data breach in healthcare go beyond identity theft – compromised data can put a patient at risk, incur costly fines, harm a provider's reputation, and hinder organizational efficiency. Dell EMC and its security partners are working together to help healthcare organizations of all types and sizes secure their healthcare data, achieve compliance, protect their brand and reputation, control access to their technology infrastructure, and mitigate risk of breaches and ransomware.

Data Center Security – layered data protection preserves continuity of vital patient services

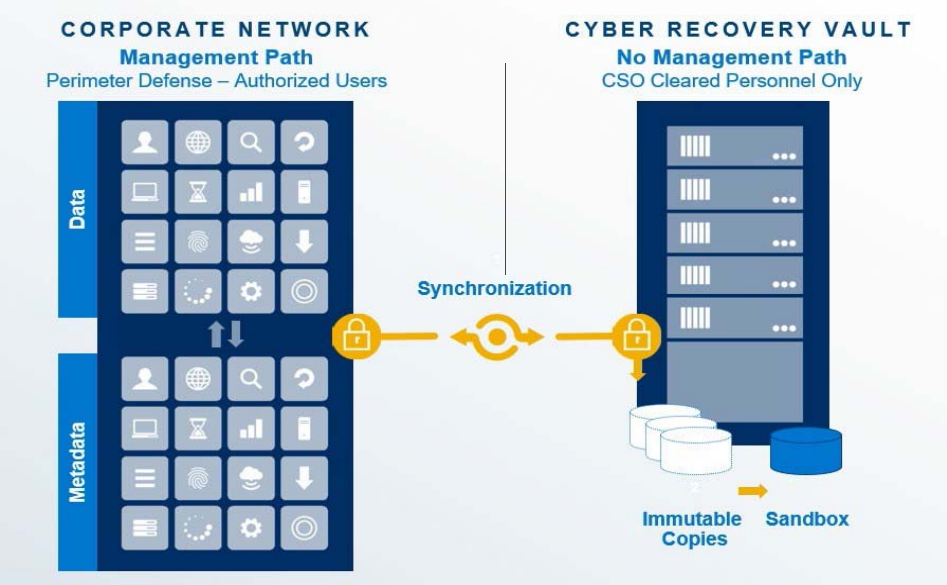
No longer satisfied to breach only your production data, cyberattack points can reach deep into backup systems and archives including your EMR, affecting critical systems, destroying patient data, and disrupting and endangering patient care. In order to combat this evolving threat, guidance from the HHS Ransomware Fact sheet is to "maintain backups offline and unavailable". Dell EMC PowerProtect Cyber Recovery solution and implementation services create a secure vault to protect critical data at the core with an isolated environment without any active network links or way for intruders to breach. Along with hidden point in time copies, the solution employs isolation or an "air gap" to enable data recovery as a last line of defense from malicious attacks. In addition, Dell EMC PowerProtect Cyber Recovery solution provides healthcare organizations with plans and measures to undertake when combating active attacks. Healthcare organizations can also protect all of their data – any workload in any consumption model with Dell EMC Data Protection portfolio.

Dell EMC PowerProtect Cyber Recovery – Robust business resiliency through automated data isolation, analytics, and recovery:

- **Planning and Design** – Optional Dell EMC Advisory Services determine which business critical systems to protect and creates dependency maps for associated applications and services, as well as the infrastructure needed to recover them. The service also generates recovery requirements and design alternatives, and it identifies the technologies to analyze, host and protect your data, along with a business case and implementation timeline.
- **Cyber Recovery Vault** – The centerpiece of Dell EMC PowerProtect Cyber Recovery is the vault, an isolated and protected extension of the data center. The vault hosts your critical data on Dell EMC technology used for recovery and security analytics.

The goal of the vault is to move data away from the attack surface, so that in the event of a malicious cyber-attack you can quickly resort to a good clean copy of data to recover your critical business systems. Using vault protections around the isolated data also protects it from insider attacks. According to the 2019 HIMSS Cybersecurity Survey, 56% of cyberattacks were from external attack vectors while 31% were from inside the organization. Dell EMC PowerProtect Cyber Recovery automates the synchronization of data between production systems and the vault and creates immutable data copies.

- **Security Analytics** – Cyber Recovery's automated workflow includes the ability to create sandbox copies that you can use for security analytics. Analytics can automatically be performed on a scheduled basis using integration provided within the Cyber Recovery vault management UI or through native REST APIs. Cyber Recovery applies over 40 heuristics to determine indicators of compromise and alert the user. The rapidly changing threat landscape (over 95% CAGR in ransomware variants) demands an adaptive analytics framework; so Cyber Recovery stays ahead of the bad actor by enabling tools incorporating Artificial Intelligence (AI) and Machine Learning (ML) analytics methods to the Cyber Recovery vault.
- **Recovery and Remediation** – Cyber Recovery allows customers to leverage dynamic restore / recovery procedures using existing Disaster Recovery procedures that bring business critical systems back online. For customers running Dell EMC NetWorker controlled backup environments integration with Cyber Recovery provides for automated recovery from the vault. Dell EMC and its Ecosystem partners provide a comprehensive methodology for protecting data, as well as performing damage assessments and forensics to either recover your systems or remediate and remove the offending malware.



Learn more about Dell EMC PowerProtect Cyber Recovery

Contact a Dell Technologies Expert

View more resources