DELL Technologies

Solution Brief

Cyber Recovery Solutions for Utility Companies

Proven and Modern Protection for Critical Data from Ransomware and Destructive Cyber Attacks.

Cyber Recovery Solution Components.

Here are five components of a proven and modern cyber recovery solution:

1. **Data Isolation and Governance**
   An isolated data center environment that is disconnected from corporate and backup networks and restricted from users other than those with proper clearance.
2. **Automated Data Copy and Air Gap**
   Create unchangeable data copies in a secure digital vault and processes that create an operational air gap between the production/backup environment and the vault.
3. **Intelligent Analytics and Tools**
   Machine learning and full-content indexing with powerful analytics within the safety of the vault. Automated integrity checks to determine whether data has been impacted by malware and tools to support remediation if needed.
4. **Recovery and Remediation**
   Workflows and tools to perform recovery after an incident using dynamic restore processes and your existing DR procedures.
5. **Solution Planning and Design**
   Expert guidance to select critical data sets, applications, and other vital assets to deter-mine RTOs and RPOs and streamline recovery.

The evolving threat of cyberattacks in the utility industry

No longer satisfied to breach only your production systems and data, cyber criminals have become more sophisticated and can reach deep into backup systems, affecting critical systems, destroying data, and disrupting key business processes.

Cyberattacks have the potential to create significant physical consequences for utilities, especially as critical infrastructure operations become more integrated. Globally interconnected, remotely accessible third-party connections provide cyber attackers with increased access to supply chain targets, contributing to a growing number of cybersecurity challenges in the utility sector. As a result, in e.g. North America, the Federal Energy Regulatory Commission (FERC), will put new responsibilities on utility companies to assess their cybersecurity preparedness. These new rules necessitate that grid modernization initiatives include reliable and automated solutions to address cybersecurity.

The North American Electricity Reliability Corporation (NERC) has published cyber security guidelines[1] which outline the importance for recovery plans for critical cyber assets. The NIST Cyber Security Framework includes a published Guide for ‘Cyber Security Incident Recovery’ which provide best practices for the electric utility industry.

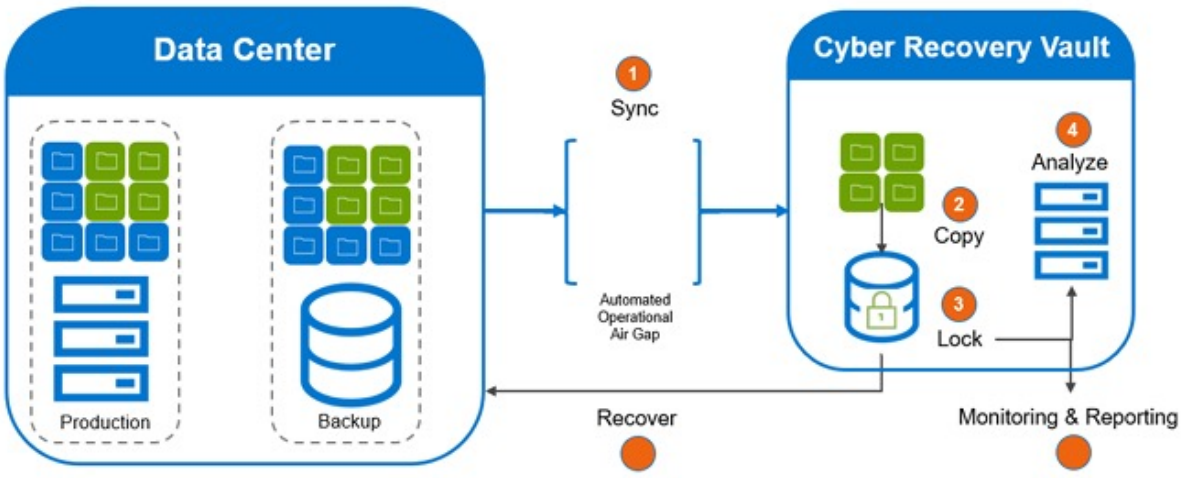

Figure 1: The Dell EMC PowerProtect Cyber Recovery Solution

The Dell Technologies approach to cyber recovery in the utility industry

In order to combat this evolving threat, guidance from the industry regulators is to "maintain backups offline and unavailable." Dell Technologies and its security partners are working together to help electric utilities of all types and sizes secure their data within these newly established parameters.

The Dell EMC PowerProtect Cyber Recovery Solution and implementation services create a secure vault to protect critical data inside the core systems 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, this solution provides utilities with plans and measures to undertake when combating active attacks.

The Dell EMC PowerProtect Cyber Recovery Solution provides proven, modern, and intelligent protection to isolate critical data, identify suspicious activity and accelerate data recovery allowing you to quickly resume normal business operations.

This includes:

• **Cyber Recovery Vault:** moves critical data away from the attack surface, physically isolating it within a protected part of the data center and requires separate security credentials and multifactor authentication for access. PowerProtect Cyber Recovery automates the synchronization of data between production systems and the vault creating immutable copies with locked retention policies.

• **CyberSense:** adds an intelligent layer of protection to help find data corruption when an attack penetrates the data center. This innovative approach provides full content indexing and uses machine learning (ML) to analyze over 100 content-based statistics and detect signs of corruption due to ransomware – all within the security of the vault.

• **Recovery and Remediation:** enables automated recovery from the vault as part of PowerProtect Data Manager and for customers running Dell EMC NetWorker Cyber Recovery - bringing business critical systems back online quickly and with confidence.

Protecting your vital data from cyber-attacks requires proven and modern solutions. PowerProtect Cyber Recovery and Dell EMC Advisory Services can give you confidence that you can quickly identify and restore known good data and resume normal business operations after a cyber-attack.

Reference:
1. Cyber Security — Recovery Plans for BES Cyber Systems: https://www.nerc.com/pa/Stand/Reliability Standards/CIP-009-5.pdf

Learn more about our solutions for utilities

Contact one of our utility industry experts

DELL Technologies