EHR Cyber Recovery Solutions with Dell Technologies and Cerner

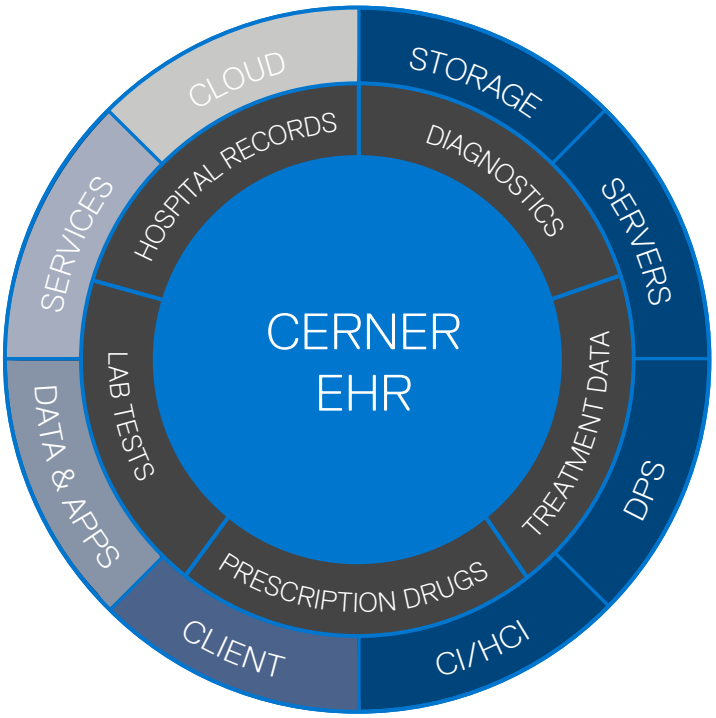
Modern protection for EHR data from ransomware and destructive cyberattacks

HEALTH SECURITY LANDSCAPE

Regardless of industry, today's organizations are data driven. This presents ample opportunity for cyber criminals using sophisticated tools to leverage data for ransom, corporate espionage, or even cyber warfare.

These cyber threats are becoming more targeted and sophisticated at an accelerating rate. In late 2020, SolarWinds, and as many as 18,000 public and private sector organizations and government agencies across the globe, fell victim to the broadest, most advanced supply chain attack in history, allegedly planned and executed by a nation state.[1] And it seems that organizations are not as prepared as they need to be. The recent Global Data Protection Index reported that 67 percent of IT decision makers are not confident that all business-critical data can be recovered in the event of a destructive cyberattack.[2]

Hospitals and health systems have more to lose than organizations in other industries when it comes to hacks. Patient data sells for more money than any other kind of information on the black market, which is why almost 90 percent of attacks hit hospitals.[3] The impact extends beyond the financial bottom line by eroding patient trust and destroying caregiver reputations when private patient data is exposed. With more than 24 million patient records already exposed in 2021 cyber events to date,[4] being attacked is a question of 'when,' not 'if.'



Teaming up with Cerner on EHR Cyber Recovery Solutions

DELL TECHNOLOGIES CYBER RECOVERY SOLUTION

Cyberattacks are designed to destroy, steal or otherwise compromise your valuable data – including your backups. Protecting your critical data and recovering it with assured integrity is key to resuming normal business operations post-attack. Could your business survive? 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

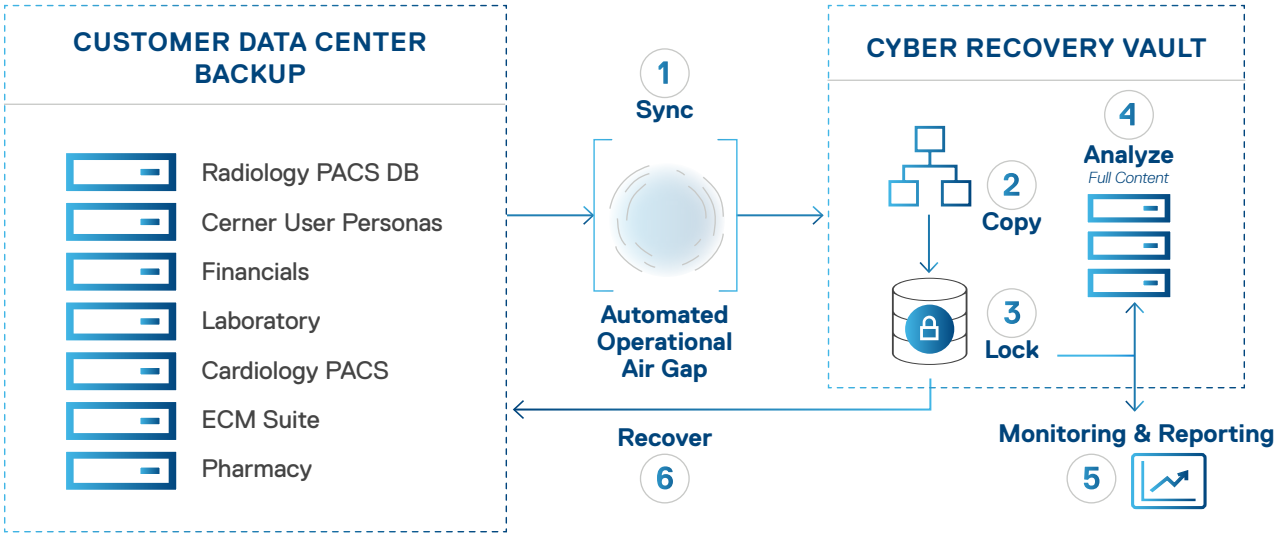
Workflows and tools to perform recovery after an incident using dynamic restore processes and your existing DR procedures.

5

SOLUTION PLANNING AND DESIGN

Expert guidance from Dell Technologies and Cerner to select critical data sets, applications and other vital assets to determine RTOs and RPOs and streamline recovery.

DATA VAULTING AND RECOVERY PROCESS



"ALWAYS ON" CONNECTIVITY: A DOUBLE EDGE SWORD

Advances in technology have allowed healthcare providers to perform clinical tasks on the move—from the bedside to nursing stations and beyond, in some cases from one side of the globe to the other. The always-on connectivity in today's modern healthcare systems presents an unprecedented opportunity for organizations to treat patients with near real-time responsiveness. Cerner and Dell Technologies are working with caregivers on solutions to connect diagnostic, treatment, prescription, lab test and hospital data from disparate sources into a "single source of truth" for each patient. The goal is to deliver Electronic Health Records (EHRs) "anywhere, anytime."

However, this level of connectivity brings its own set of challenges, requiring Health IT departments to rethink the technologies needed to ensure the security of the patient health information (PHI). As a result, having a cyber recovery strategy has become a mandate for healthcare leaders.

CYBER RECOVERY SOLUTIONS WITH DELL TECHNOLOGIES AND CERNER

The purpose of a cyber recovery solution is to provide a clean, protected copy of healthcare institutions' most critical workloads, which typically include EHRs and imaging data sets. By maintaining a backup copy that is air-gapped, or isolated and separated from the network, healthcare IT departments can provide more reliable ransomware protection for these critical workloads.

Cerner is both a healthcare software leader, and a Dell Technologies resale partner. In addition, Cerner fully understands the EHR application and workflow impact—allowing healthcare organizations to adopt a cyber recovery platform customized for healthcare providers. This includes assistance with an audit of the most critical healthcare enterprise workloads, a deep understanding of mapping application dependencies, and the ability to perform a complete risk assessment and business analysis. Dell Technologies and Cerner offer support beyond what can be provided without this collaboration. In the event of a recovery need, health IT departments have access to joint support with their EHR application company (Cerner) and technology partner (Dell Technologies) to enable the restoration of their EHR workloads quickly and accurately.

Protecting patient data from cyber-attacks requires proven and modern solutions. Cerner applications, wrapped in the Dell EMC PowerProtect Cyber Recovery solution, can give you confidence that you can quickly identify and restore known good data and resume normal business operations after a cyberattack.

Learn more about our solutions for healthcare

Contact one of our healthcare experts

Join the conversation with #TransformHIT

1. SolarWinds: businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12
2. Global Data Protection Index Survey 2020 Snapshot
3. beckershospitalreview.com/healthcare-information-technology/hospitals-are-hit-with-88-of-all-ransomware-attacks.html
4. ocrportal.hhs.gov/ocr/breach/breach_report.jsf - from 1/1/2021 to 06/30/2021

DELL Technologies