The Challenge: Cyberattacks are the enemy of data-driven businesses

Data is the currency of the internet economy and a critical asset that must be protected, kept confidential and made available at a moment’s notice. Today’s global marketplace relies on the constant flow of data across interconnected networks, and digital transformation efforts put more sensitive data at risk.

This makes your organization’s data an attractive and lucrative target for cyber criminals. Cybercrime has been called the greatest transfer of wealth in history, and it’s all about the data. In fact, Cybersecurity Ventures estimates that $6 trillion is the estimated global impact of cybercrime in 2021.

Regardless of the industry or size of the organization, cyberattacks continually expose business and governments to compromised data, lost revenue due to downtime, reputational damage and costly regulatory fines. According to Accenture Insights, $13 million is the average cost to organizations resulting from cybercrime.

Having a cyber recovery strategy has become a mandate for business and government leaders, yet many organizations lack confidence in their data protection solutions. The Global Data Protection Index reported that 67% of IT decision makers are not very confident that all business-critical data can be recovered in the event of a destructive cyberattack.

So, what can you do to protect your organization and its valuable data?

The Solution: PowerProtect Cyber Recovery

Dell PowerProtect Cyber Recovery 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.
PowerProtect Cyber Recovery – proven, modern and intelligent protection to reduce business risks from cyber threats

Cyber Recovery vault
The PowerProtect Cyber Recovery vault offers multiple layers of protection to provide resilience against cyberattacks even from an insider threat. It 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 multi-factor authentication for access. Additional safeguards include an automated operational air gap to provide network isolation and eliminate management interfaces which could be compromised. PowerProtect Cyber Recovery automates the synchronization of data between production systems including open systems and mainframes, and the vault creating immutable copies with locked retention policies. If a cyberattack occurs you can quickly identify a clean copy of data, recover your critical systems and get your business backup and running.

CyberSense
PowerProtect Cyber Recovery is the first solution to fully integrate CyberSense which 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. CyberSense finds corruption with up to 99.5% confidence, helping you identify threats and diagnose attack vectors while protecting your business-critical content – all within the security of the vault.

Recovery and Remediation
PowerProtect Cyber Recovery provides automated restore and recovery procedures to bring business critical systems back online quickly and with confidence. Recovery is integrated with your incident response process. After an event occurs, the incident response team analyzes the production environment to determine the root cause of the event. CyberSense also provides post-attack forensic reports to understand the depth and breadth of the attack and provides a listing of the last good backup sets before corruption. Then, when the production is ready for recovery Cyber Recovery provides management tools and the technology that performs the actual data recovery. It automates the creation of the restore points that are used for recovery or security analytics. Dell and its ecosystem partners provide a comprehensive methodology for protecting data, as well as performing damage assessments and forensics to provide an organization with the confident and most reliable path to recovery of business-critical systems.

Solution Planning and Design
Optional Dell Advisory Services help you determine which business critical systems to protect and can create 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.

Protecting your vital data from cyberattacks requires proven and modern solutions. PowerProtect Cyber Recovery can give you confidence that you can quickly identify and restore known good data and resume normal business operations after a cyberattack.

1Cybersecurity Ventures: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021
3Based on research by Vanson Bourne commissioned by Dell Technologies, "Global Data Protection Index 2021 Snapshot," carried out February – March, 2021. Results were derived from a total of 1,000 IT decision makers worldwide from both private and public organizations with 250+ employees.