SOLUTION BRIEF

CYBER RECOVERY

The Last Line of Data Protection Defense Against Cyber-Attacks

WHY 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 WORM-locked data copies to a secondary set of arrays and backup targets 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 integrity checks to analyze whether it is impacted by malware along with mechanisms to trigger alerts on suspicious executables and data.

Recovery & Remediation - Procedures to perform recovery / remediation after an incident using dynamic restore processes and your existing DR procedures.

The Challenge: Cyber Attacks on Business-Critical Systems

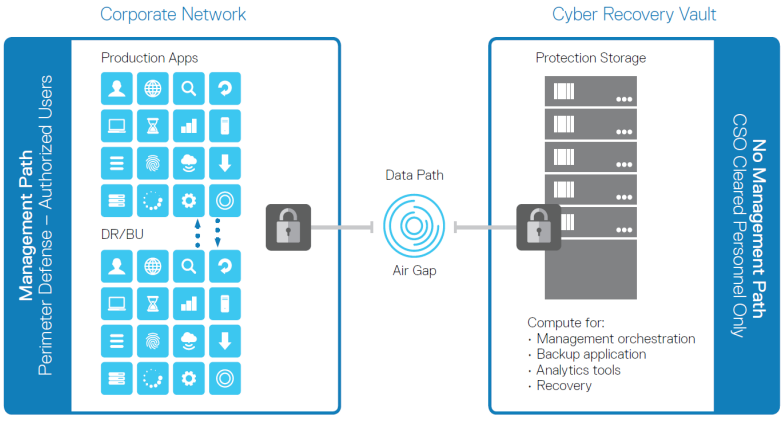
No matter the industry or size of the organization, Cyber Attacks are on the rise. The number of attacks is growing exponentially led by hacking and malware with 48% and 30% of the attack tactics respectively[1].

According to RSA, 70% of organizations report that they've had a security incident that has negatively impacted their operations, and 72% of organizations say they are still "immature" (or worse) in capabilities involving incident response and recovery.[2] Remediation from a destructive cyberattack is often painful and time consuming, with a direct and negative impact on your bottom line.

All organizations are concerned about a destructive cyberattack and 76% of businesses see ransomware as a significant business threat[4].

Hackers' primary entry mode is via our many end-user devices, or they resort to phishing techniques, along with zero-day malware entering the environment via email for 93% and 96% of the breaches respectively.[1] The likelihood that all malware will be discovered before harm is done is slim, and the discovery time for an attack is still likely to be measured in weeks or months[1]. This time gap provides opportunity to map the network, escalate privileges and plan a devastating attack,

The Solution: Cyber Recovery



ranging from extortion (ransomware) to outright destruction of business-critical systems. These types of Cyber Attacks can cripple an organization, leading to expensive remediation, revenue loss, negative publicity, and lasting customer distrust. As fast as organizations build defenses against different attack vectors, hackers devise new ways to circumvent them.

In order to create a more comprehensive approach to cyber-risk mitigation, organizations need to evolve and automate their recovery and business continuity strategies in addition to focusing on threat detection analysis and remediation. Dell EMC Cyber Recovery provides the power to enable an automated workflow to augment data protection infrastructure with true data isolation, data forensics, analytics, and -- most importantly -- data recovery for increased business resiliency.

Dell EMC 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 (CR Vault)** – The centerpiece of Dell EMC Cyber Recovery is the CR Vault, an isolated and protected part of the data center. The CR Vault hosts your critical data on Dell EMC technology used for recovery and security analytics. The goal of the CR 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 Verizon Data Breach Investigations Report 2017, 25% of reported cyberattacks involved insiders. Dell EMC Cyber Recovery automates the synchronization of data between production systems and the CR 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 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 CR 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. 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.

[1][*Source: Verizon Data Breach Investigations Report 2018*]
[2][*Source: RSA Cybersecurity Poverty Index*]
[3][*Source: SecureWorks Ransomware Defense Survey Report 2017*]

Learn more about Dell EMC Cyber Recovery Solutions

Contact a Dell EMC Expert

View more resources

Join the conversation with #CyberRecovery