DELL Technologies

Service Overview

CYBER RECOVERY SERVICES

Develop your cyber recovery strategy and implement your recovery program

ESSENTIALS

Dell Technologies Cyber Recovery Services:

- Create a minimum viable company in the cyber recovery vault which is trusted to recover core business functions after a cyber attack
- Advise on your recovery strategy and integration points with organization-wide incident response plans
- Integrate a NIST Cybersecurity Framework aligned recovery solution which plans for a wide variety of threat vectors
- Develop and test recovery plans and procedures

Business Challenge

Cyber-attacks have become a common occurrence. They can result in extended downtime, bringing business operations to a halt for days and even weeks—costing millions. Beyond the concern of exposure of sensitive information or proprietary data, the growing reality is that many cyber attacks are specifically designed for data destruction or encrypting data and holding it for ransom. Many recent ransomware attacks were particularly damaging to manufacturing systems, hospital information systems, banking systems and local governments. These attacks can bypass traditional security controls at the perimeter, allowing the attacker to go undetected for months or sometimes even years, impacting the most amount of systems possible, and leaving the business even less prepared to recover. In addition to bad actors outside of your organization, the unfortunate truth is that insiders are involved in a growing number of cyber attacks and leadership needs to be prepared to protect their business against all types of threats. These factors have caused business leaders across all industries to ask for assurances that they can recover in the event of a cyber attack.

Because cyber attacks are becoming more sophisticated and devastating, companies must consider new data protection and cyber security use cases that represent a “last line of defense” to ensure they will be able to survive a destructive cyber-attack.

Service Description

The latest approach emphasizes keeping an isolated copy of your most critical data (e.g., essential applications, data, and intellectual property) off the production network and separated from production backup systems. With no direct network connection and multiple roll-back points available, you ensure an uncompromised “gold copy” is ready for recovery.

Dell EMC PowerProtect Cyber Recovery helps achieve an air-gapped data protection vault, and in conjunction with Dell Technologies Services, accelerates your adoption of the technology and processes to increase confidence in your ability to recover from a cyber attack. Our services are focused in two primary areas, advisory and implementation.

The Advisory phase focuses on providing recommendations to integrate and optimize the Cyber Recovery in your data protection environment. This is accomplished by analyzing both your current and future state to create a tailored strategy for cyber recovery preparedness, ensuring tight alignment with the business needs for protection and recovery.

A key component of the advisory phase is a workshop and information session to collect data on your applications and understand their criticality to normal business operations. These considerations will help drive recommendations of what should be protected by the Cyber Recovery Vault and make up your Minimum Viable Company – a collection of your most critical data and applications which can be used to rebuild core functions first and get the business running again.

The Implementation phase integrates the Cyber Recovery Solution into your data protection environment. In this phase we can use information gathered through the advisory to further tailor the solution to your exact needs. We can also integrate additional technologies and capabilities with your Cyber Recovery environment, such as:

- Deploy vault infrastructure
- Deploy CyberSense analytics to analyze data and identify early indicators of compromise
- Modify production backups to support Cyber Recovery Vault requirements
- Harden additional production Dell Technologies infrastructure
- Integrate Cyber Recovery Vault and capabilities with mainframe environments
- Create Cyber Recovery Vault to include multiple platforms, heterogeneous technologies, retentions policies and applications
- Develop detailed operational procedures (Recovery Runbooks) to execute a recovery out of the vault
- Support for creation of extended recovery runbooks and additional test scenarios

Summary of Benefits

Due to the proliferation of cyber attacks, it's now a question of when, not if, and organization will be impacted. Every business has unique goals, objectives and IT requirements which need to be met by their cyber incident response and cyber recovery strategies. Our Consulting experts work with you to develop processes and procedures that enable you to protect and recover your business in the event of a destructive cyber-attack.

Dell Technologies Services Delivers:

- An air-gapped Cyber Recovery vault solution and recommendations to create your Minimum Viable Company in the vault and enable recovery in the event of a cyber attack.
- Help you meet your compliance goals with increasingly stringent regulatory pressures by protecting and proving recovery capabilities of specific core applications.
- Incorporate a NIST Cybersecurity Framework aligned recovery strategy into your incident response preparations

Learn more about Dell Technologies Services

Contact a Dell Technologies Expert

View more resources

Join the conversation with #DellTechnologies

Reference Number: H18544