Cyber Recovery Solution

Protecting Your Critical Data

Businesses today rely heavily on technology and data. Though most organizations have developed strategies to access critical data during an outage caused by natural disasters or power disruptions, these strategies have proven to be ineffective during a cyber attack. Interconnected users, servers, cloud devices, and continuous web access results in an environment that is open for cyber criminals to significantly disrupt operations and/or take an entire network hostage.

The primary goal of Business Continuity and Disaster Recovery (BCDR) is to keep your data safe and ensure timely restoration of a clean network environment. In the case of ransomware or a malware attack, the standard solutions of replicating data to redundant locations and backup centers will be catastrophic. In this environment, a network that was presumed to be resilient and flexible is fully exposed to a cyber compromise across all production and backup environments.

Optiv Solutions

Optiv’s Cyber Recovery Solution (CRS) exists to support the identification and protection of critical data that must be shielded from the impact of cyber attacks, while also enabling rapid recovery to a secure state. Backup copies are automatically stored in a malware-protected, air-gapped vault or a remote cloud-based solution that safeguards your data’s confidentiality, integrity and availability.

CRS provides a solution that ensures data is verified and clean prior to entering the vault and is maintained in an immutable state while within the vault, significantly reducing recovery time by guaranteeing that you are recovering to a known good state.

How We Do It

CRITICAL DATA PROTECTION

- Identification of critical assets and systems that are essential to continued business operations and must be protected in the event of a cyber attack.
  - Analysis of organizational data, ensuring critical data that requires protection from cyber-attacks is properly classified
  - Development of a cyber resilient strategy for critical assets and infrastructure

CYBER RESILIENCE SOLUTION

- Developing a framework that integrates traditional backup solutions, enhanced security controls (e.g., automated host isolation) and a vaulted ‘air-gapped’ backup solution, with associated governance and procedures to secure business critical systems from destruction or deletion.
  - Implementation of a vaulted, air-gapped, data-isolated solution
  - Application of automated workflows that securely move business-critical data into the isolated environment

RECOVERY PLAYBOOK

- Developing and maintaining accurate recovery steps, ensuring resilience processes are identified, documented and tested.
  - Development of response plans that accelerate recovery and ensure system and data accuracy
  - Cyber recovery table tops that test and continuously improve response procedures
Optiv is a security solutions integrator — a “one-stop” trusted partner with a singular focus on cybersecurity. Our end-to-end cybersecurity capabilities span risk management and transformation, cyber digital transformation, threat management, cyber operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more cost-efficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are leading a completely new approach to cybersecurity that enables clients to innovate their consumption models, integrate infrastructure and technology to maximize value, achieve measurable outcomes, and realize complete solutions and business alignment. For more information about Optiv, please visit us at www.optiv.com.