TITAN
CLOUD SOLUTIONS

DATA RECOVERY

DATA SHEET

RANSOMWARE: THE PREVAILING DISASTER RECOVERY CHALLENGE

Ransomware remains a significant threat to the operational continuity of businesses, necessitating a multifaceted approach to data recovery strategies. Traditional disaster recovery methods often fall short when dealing with data compromised through malicious activites. Thus, a well-prepared & adaptabke strategy for compromised data recovery is crucial for both mitigating damage & ensuring a successful recovery.

Priortizing Data Protection Investments

Investments in readiness for data recovery should be aligned with the critical importance of the data to the organizations continued viability. Emphasis should be placed on protecting Vital Digital Assets (VDAs) that are essential to the organization's core functions.

Developing a Roapmap to Data Recovery Readiness

Organizations must identify the business & infrastructure data that warrant extra protection, which goes beyond traditional disaster recovery measures. Validating the effectiveness of these strategies through rigorous testing & reviews is essential to ensure their reliability & to communicate readiness to executive leadership.

DIVERSE STRATEGIES FOR COMPROMISED DATA RECOVERY

To minimize IT downtime & data loss, organizations need a robust suite of recovery strategies. These strategies must be versatile enough to be deployed individually or in combination, depending on the specifics of a cyber intrusion.

Key Recovery Tactics include:

RESTORE:
Revert to a previous point in time using extended retention backups.

DECRYPT:
Unlock data using an acquired decryption key.

REPROCESS:
Re-run transactions from original data sources, such as Electronic Data Interchange (EDI) systems.

REBUILD:
Regenerate data from other systems like data warehouses

REENTER:
Input transcations directly from original documents, such as emails.

RECREATE:
Manually redo tasks, such as re-inventorying in a warehouse