TITAN
CLOUD STORAGE

DATASHEET

DATA RECOVERY

Ransomware poses a critical challenge for business continuity, requiring advanced data recovery strategies. Effective recovery methods include restoring from backups, decrypting data, and reprocessing transactions. Prioritizing the protection of Vital Digital Assets (VDAs) is essential. Titan Cloud Storage's Compromised Data Risk Management (CDRM) framework integrates disaster recovery and cyber incident management, enhancing preparedness. Leverage Titan Cloud Storage’s expertise to build a robust cyber recovery program and ensure your business is ready for any threat.

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 activities. Thus, a well-prepared and adaptable strategy for compromised data recovery is crucial for both mitigating damage and ensuring a successful recovery.

Prioritizing Data Protection Investments

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

Developing a Roadmap to Data Recovery Readiness

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

Diverse Strategies for Compromised Data Recovery

To minimize IT downtime and 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 transactions directly from original documents, such as emails.
- **Recreate:**
  Manually redo tasks, such as re-inventorying in a warehouse.