Cyber Attack Detection and Recovery

Security expertise is a challenge to build and maintain for many organizations. The Cyber security product market is fractured, confusing, and shifting rapidly, meanwhile cyber criminals have huge financial resources to develop new threat vectors.

Successful criminals are stealing billions with impunity.

Solution Overview

Dell EMC PowerProtect Cyber Recovery with CyberSense is a secure offsite vault for critical data, leveraging Microsoft Azure for geographic diversity and rapid deployment. It provides air gapped replication for immutable protection copies of data for recovery in the case of a cyber attack. Dynamic expansion and contraction of the vault size means flexibility and cost management.

The comprehensive solution carries out data scanning to quickly identify suspicious behavior and respond accordingly.

Solution Benefits

- Identify priority applications and data to protect based on business value.
- Detect cyber attacks automatically using a machine learning platform to keep you safe.
- Guarantee immutable (read-only) backup copies.
- Leverage Dell Technologies and ESTI data protection expertise to safeguard data.
- Acquire a complete "as a service" solution with a single monthly fee.

Cyber Security Vault
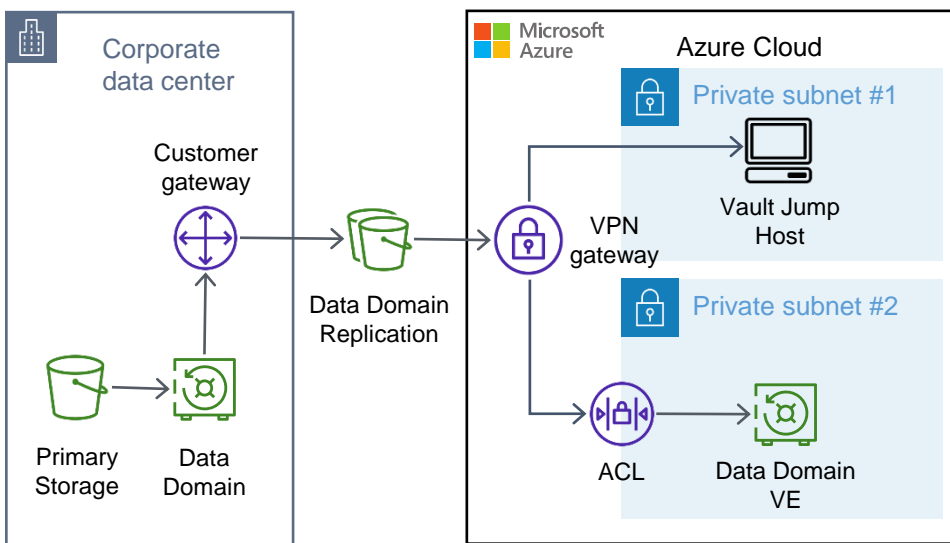

Cyber Recovery Best Practices

- Know what to protect
- Automate Breach Detection
- Save Immutable Copies
- Limit Access
- Audit Activity
- Bolster Data Location Diversity
- Leverage Enterprise Backup

Cyber Attack Detection and Recovery

Data Analysis Dashboard: CyberSense
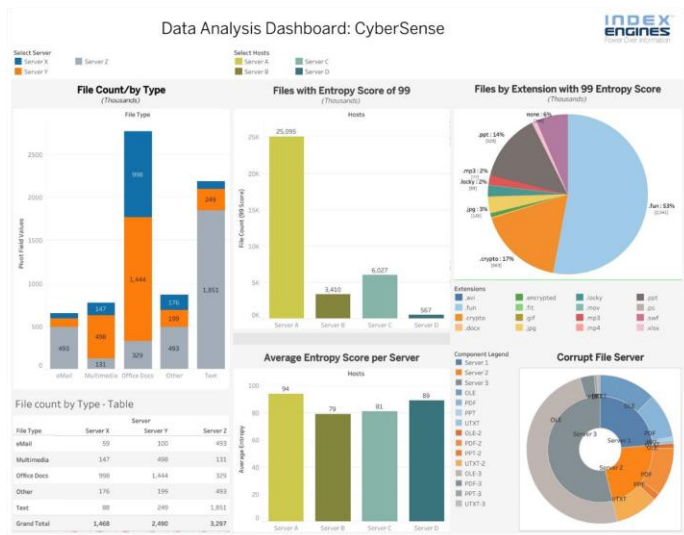
- ✔ Cyber Recovery alert panel
- ✔ CyberSense alert of data corruption
- ✔ Monitors the impact on the data – not only monitoring known threats
- ✔ Generate detailed reports to diagnose data corruption
- ✔ Understand the who, what, where, when of the attack

- Delivers reporting tools to detect indicators of compromise and attacks
- Detects common attacks including encryption, ransomware, destruction and slow corruption
- Direct indexing of content in backups without the need to rehydrate the data, which can result in activating ransomware
- Initial scan of backup image can detect an attack with up to 95% accuracy. Subsequent passes increase detection capabilities up to 99%.
- Forensic analysis tools help recover from cyber attack and diagnose attack vector.
- Fully integrated with Dell EMC Cyber Recovery

Timeline - Real Life Scenario
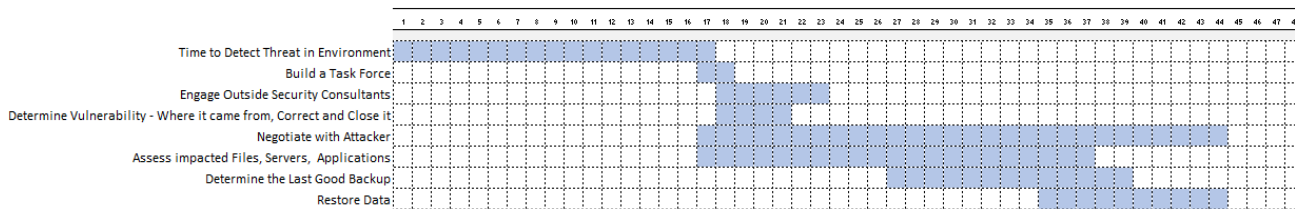
44 Total days of disruption, cost and risk before this customer felt comfortable and confident and could resume regular business operations

Timeline - Leveraging Dell Data Protection Cyber Recovery Solution
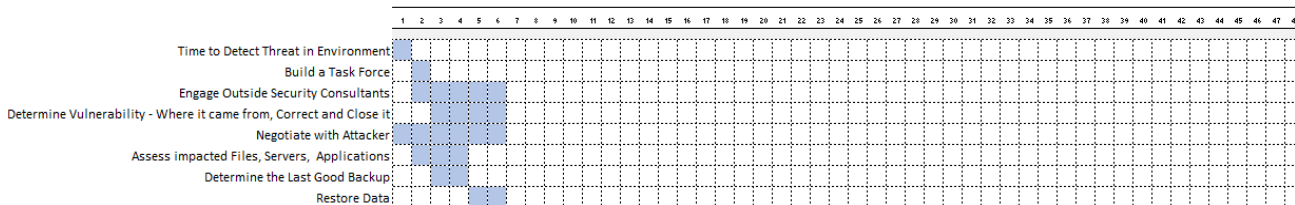
Time to Recovery window could have decreased by 38 days (84%), savings this customer signigicant financial costs, labour time and downtime/outage