Accelerated Ransomware Recovery with Dell PowerProtect Backup Services

Recover from ransomware in hours, not day

Key Features

Ransomware attacks are becoming more frequent, advanced, and expensive

- Inability to quickly identify and restore uninfected backups or files
- Contamination spread and reinfected from recovery data
- Data loss, inability to recover a complete data set
- Difficulties coordinating incident response orchestration
- Demands for faster RPO/ RTO times
- Costly business downtime leading to loss of revenue and damage to brand reputation
- Legal and regulatory fines from inadequate data protection

The Challenge

Ransomware is a serious threat to every enterprise. Cyberattacks occur frequently and can cause catastrophic damage. 79% of organizations are concerned that they will experience a disruptive event in the next 12 months1. Companies that lose their data are at risk of filing for bankruptcy after a disaster. Ransomware attacks are not only happening more frequently but have also become more technologically advanced and expensive.

The Solution

Fast reliable recovery eliminates any reason to even think of paying a ransom. But when a security incident or cyber-attack occurs, organizations need to understand the blast radius and root cause before recovery. With pristine, air-gapped snapshot of workloads and virtual machines available 24/7, continuous monitoring for user and data anomalies, integration with security tools, and automated recovery of clean data, you can improve your security posture and transform a devastating ordeal into a survivable incident.

The Capabilities

For all workloads:

• Ensure you have immutable, air-gapped backups available 24x7

• Recover clean data on-premises or in the cloud with RPO/RTO of hours, not days or weeks

• Managed Data Detection and Response (MDDR) service provides 24x7x365 real-time monitoring of backup environments

• Restore workloads and VMs across any AWS region/account using data from your production org, and creating many copies of it, storing it in multiple places, you are putting your organization at great risk.

Accelerated ransomware recovery for key workloads:

• Monitor and proactively detect anomalies with ML based algorithms

• Orchestrate response and recovery activities via SIEM and SOAR integrations

• Scan snapshots for malware before recovery and delete infected snapshots and files from backups

• Automatically recover the most recent clean version of every file in a specified time frame from a golden snapshot

Protection

The first step in preventing damage from ransomware is ensuring that you have an air-gapped and immutable copy of your data. Built on highly resilient cloud infrastructure, Dell PowerProtect Backup Services makes it impossible for ransomware to encrypt backup data. Zero trust architecture, including multi- factor authentication, envelope encryption, and separate account access ensures that ransomware cannot use compromised primary environment credentials to tamper with the backup environment or data. Finally, excess deletion prevention and soft-delete (recycle bin) features provide a further layer of security to safeguard backups against deletion.

Detection

Detecting a ransomware attack as soon as possible can help incident response teams and prevent contamination spread. The Dell PowerProtect Backup Services accelerated ransomware recovery module provides a security command center to monitor the posture of your backup environment. With access insights and anomaly detection you can quickly identify unusual activity across your environment and data. See the location, identity, and activity information for all access attempts by users and APIs. Detect anomalies with proprietary ML algorithms that provide alerts for unusual data activity (e.g., deletion, encryption, etc.). The algorithm learns the patterns for your specific backup environment, so it doesn't require any rules setup or tuning. It also uses entropy-based insights to reduce false positives

Response

When a security or IT analyst detects a suspicious event, or worse, confirms that a ransomware incident has occurred, the speed of response becomes critical. While there are many valuable primary environment security tools that can be used for detection and response orchestration, analytics and change log data from secondary data (backup systems) improve investigation, response, and forensic activities. The Dell PowerProtect Backup Services accelerated ransomware recovery module offers robust API integrations out of the box that make it easy to fit the solution into your overall security ecosystem. Orchestrating response activities using SIEM and SOAR solutions can dramatically reduce your mean time to respond (MTTR) by automatically completing actions like quarantining infected systems or snapshots or scanning backups for IOCs based on a predetermined ransomware playbook.

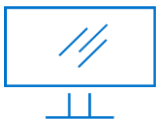
Recovery

After the initial response phase comes the hard work of recovery. For many companies this is a manual and time- consuming process. Dwell time for malicious actors and ransomware can range from weeks to months making it difficult to know how far back to go to find clean data. Even after the best snapshot is identified, hidden malware can cause reinfection. Yet, a recovery point of 2 weeks ago isn't acceptable to

most business users. Yet, finding and validating more recent data after a ransomware incident is manual, tedious and often insurmountable.

Dell PowerProtect Backup Services eases this burden with an effective backup architecture and automated tools to accelerate recovery. The Dell PowerProtect Backup Services cloud platform backs up workloads directly to the cloud, ready for immediate recovery in the event of a ransomware attack.

The accelerated ransomware recovery module enables you to recover with confidence by ensuring the hygiene of recovery data. You can scan snapshots for malware and IOCs using built-in antivirus detection or using threat intelligence from your own forensic investigations or threat intel feeds. Scanning snapshots before recovery eliminates reinfection.



Learn More about PowerProtect Backup Services

Contact a Dell Technologies Expert

DELL Technologies