WILDFLOWER

DELL Technologies
FEDERAL PLATINUM PARTNER

Accelerated ransomware recovery with Dell APEX Backup Services

Recover from ransomware in hours, not days

Essentials

Business challenges

- 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 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. 93% of organizations have experienced a data-related business disruption1. Companies that lose their data are at risk of filing for bankruptcy after a disaster. Ransomware attacks are not only happening more frequently, but they are also becoming more technologically advanced and expensive.

The solution

Fast, reliable data recovery eliminates any reason to even think of paying a ransom. When pristine snapshots of workloads and virtual machines (VM) can be restored in minutes, you can transform a ransomware attack from a devastating ordeal to a survivable incident.

Key capabilities

For all workloads:

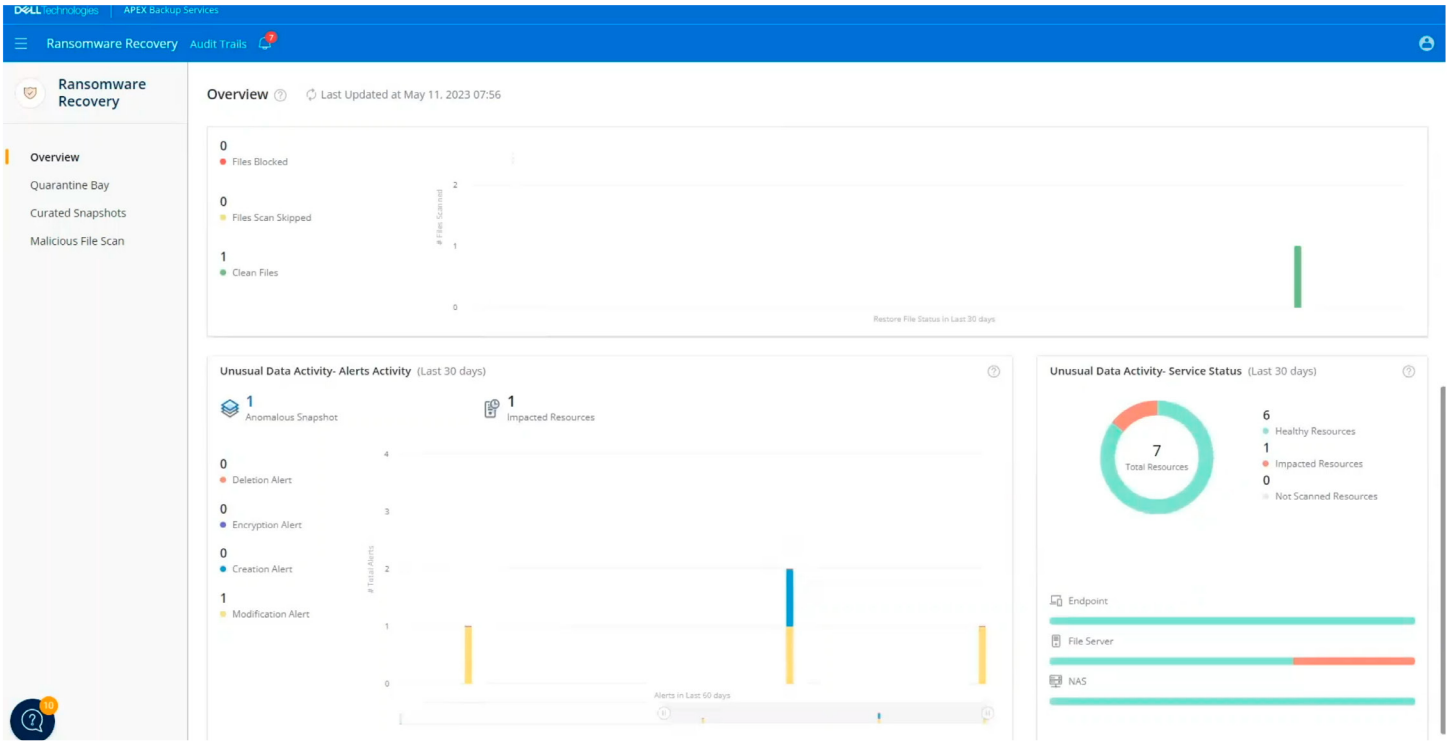
- Ensure you always have clean backup data to restore from in the event of an attack
- Recover on-premises or in the cloud with RPO/RTO of hours, not days or weeks
- Restore workloads and VMs across any AWS region/account
  Accelerated ransomware recovery for endpoints, file servers, and NAS:
- Monitor and proactively detect anomalies with machine learning (ML) based algorithms
- Orchestrate response and recovery activities via built-in Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) integrations
- Scan snapshots for malware and Indicator of Compromise (IOC) before recovery
- Delete infected snapshots and files on all endpoint backups
- Automatically recover the most recent clean version of every file in a specified time frame

Protection

The first step in preventing damage from ransomware is ensuring that you have a clean backup copy of your data. Built on highly resilient cloud infrastructure, Dell APEX Backup Services makes it impossible for ransomware to encrypt backup data. Zero trust architecture, including multifactor authentication, envelope encryption, and separate account access ensures that ransomware cannot use compromised primary environment credentials to tamper with backup 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 prevent contamination spread. The Dell APEX Backup Services accelerated ransomware recovery module provides access insights and anomaly detection that help you quickly identify possible ransomware attacks. Access insights lets you see location, identity, and activity information for all access attempts. Anomaly detection uses proprietary ML algorithms to provide alerts for unusual data activity. The algorithm learns the norms 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.



Gain insight into access requests and receive alerts for anomalous data activity.

Response

Once you've detected an attack, rapid response is vital to ensure a fast recovery. There are many valuable primary environment security tools that can be used for detection and orchestration. The Dell APEX 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 based on a predetermined ransomware playbook.

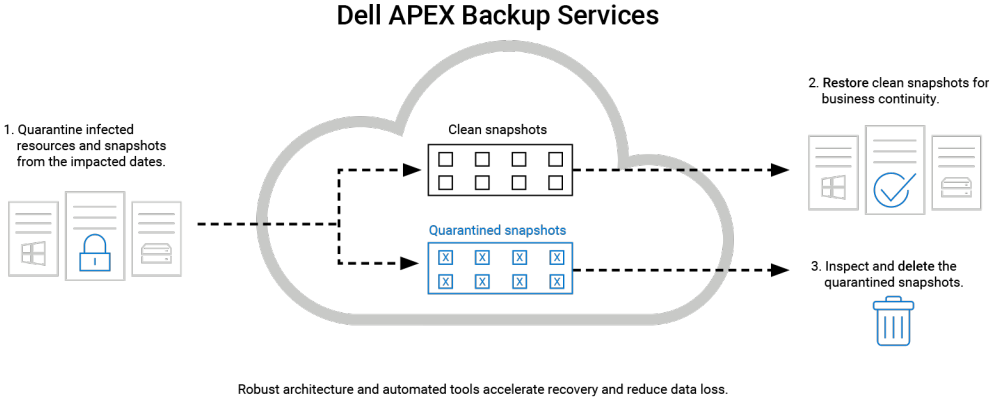
Recovery

After the initial response phase comes the hard work of recovery. For many companies this is a manual and time consuming process. On average, ransomware quietly spreads within a system for 90 days before an actual ransom demand, so it can be difficult to identify the best backup snapshot to use for recovery. Even after the best snapshot is identified, hidden malware can cause reinfection. Plus, if data is recovered from a point in time weeks or even months in the past, you'll need to manually find and recover clean versions of important files that were created or modified in the intervening time.

Dell APEX Backup Services eases this burden with effective backup architecture and automated tools to accelerate recovery. The Dell APEX 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.

Accelerated ransomware recovery also solves the problem of data loss due to point-in-time recovery. Now you can automatically identify the most recent clean version of every file within a specified timeframe and consolidate those versions into a single "Golden Snapshot". Eliminating the manual search and recovery process drastically reduces time to recover and prevents data loss.



Robust architecture and automated tools accelerate recovery and reduce data loss.

GSA | CHESS ITES-3H | SBA WOSB Woman Owned Small Business | HUBZone Historically Underutilized Business Zone CERTIFIED | First Source II | SEWP Approved SEWP V Federal Government IT Provider

www.wildflowerintl.com

Wildflower International Ltd. | 1516 Pacheco Street, Santa Fe, NM 87505
505-466-9111 | information@wildflowerintl.com