Ransomware Recovery for VMware Cloud Foundation

VMware Live Cyber Recovery

At a Glance

VMware Live Recovery includes a comprehensive ransomware recovery solution for organizations using VMware Cloud Foundation, offering essential tools to protect critical virtualized workloads and ensure robust recovery from sophisticated ransomware attacks, even when conventional defenses fail. This is provided through the VMware Live Cyber Recovery capabilities of VMware Live Recovery solution.

Ransomware attacks pose a significant threat to IT infrastructure, demanding robust recovery solutions for data centers. Protecting business-critical applications and data requires thorough preparation and reliable recovery capabilities. VMware Live Cyber Recovery offers a flexible, scalable cloud-based solution that enables swift and confident recovery from ransomware attacks, minimizing downtime and ensuring business continuity.

Getting Started

With VMware Live Cyber Recovery, your team can create and implement a robust recovery strategy and cloud-based recovery solution that meets your business SLAs, accelerates time-to-protection, and simplifies VM recovery operations in the face of modern cyberattack disasters.

The solution starts when you establish a proper recovery basis using the base cloud recovery platform. This includes:

- Protecting VCF sites using connector appliances, enabling complete coverage of VMs in target workload domains.
- Easily defining protection group policies that snapshot VMs in accordance with business SLAs, including desired retention policies for ransomware recovery.
- Ensuring well-tested and monitored recovery plans that identify the scope of recovery and the necessary mappings for the recovery site orchestration.

When needed, it is simple to prepare and configure the isolated recovery environment in VMware Cloud on AWS to provide a safe, disconnected, controlled, and fully enabled environment to conduct restore and remediation tasks to recover cleaned versions of application VMs that have been impacted by ransomware attacks. This includes: networks, NSX-T Advanced Firewall customizations, and the necessary connectivity to the tools used for complete validation tasks.

Key Benefits

Isolated Recovery Environment (IRE): A safe, controlled recovery environment.

Immutable, Air-Gapped Recovery Points: Connected directly to the IRE.

Enhanced Recovery Point Selection: With deeper data insights such as VM data change rates and file entropy.

Guided Ransomware Recovery Workflow: A step-by-step process through all VM recovery tasks.

Push-Button VM Network Isolation: Quarantine VMs from one another to prevent lateral movement or unwanted access within the IRE.

Next-Generation Antivirus (NGAV) with Behavioral Analysis: To better identify modern fileless attacks in running VMs.

During solution testing or when needed for recovery, easily exercise the guided workflows enabled through the orchestration interface. This includes:

- Enhanced recovery point selection with VM change rate and entropy criteria, with deep recovery point inventory readily available.
- Individual or group VM operations to help with isolation of activities and a more complete divide-and-conquer approach to handling recovery tasks.
- Integrated tooling to assist with validation tasks for vulnerabilities, malware, and behavioral analysis.
- Improved cross-team communication support with annotations and recovery point badging capabilities.
- File and folder recovery from any recovery point to help minimize data loss during remediation and recovery iteration tasks.
- Robust and detailed, per-VM network isolation control to help perform recovery tasks in a safer and more controlled access configuration.

Incremental staging and recovery tasks during cyber recovery operations help manage the overall orchestration efforts. This includes:

- Staging snapshots that capture all remediation changes applied to the VMs during validation tasks.
- Delta-change, incremental data recovery to help optimize the amount of data transport required to replace the original impacted VM with the updated, recovered VM.
- Ability to recover to other Protected Sites should the primary still be unavailable.

Summary

Effective ransomware recovery is a crucial component of a robust defense strategy for any business. VMware Live Cyber Recovery offers a comprehensive framework to safeguard critical application VMs, enabling faster and more reliable recovery from ransomware attacks. This solution also includes tools to validate VM health before restoration, ensuring a secure return to normal operations.

vmware® by Broadcom

Solutions Brief – July 9, 2024 – VCF Product Management & Marketing