Implement Ransomware Protection and Recovery

VCF Professional Services

At a glance

Create and implement a ransomware recovery strategy, leveraging VMware Live Recovery, that enables protection and full recovery of your workloads on VMware Cloud Foundation® (VCF).

Key benefits

- Implement a ransomware protection and recovery strategy quickly and efficiently
- Simplify recovery operations
- Establish ongoing processes to validate recovery plans and remove configuration drift
- Reduce risk and complexity
- Minimize disruption to existing operations
- Free up your IT staff to work on business-critical tasks

Ransomware attacks continue to grow and evolve. To protect your business-critical applications and data, you need to prepare for and be able to recover from any cyber attack. Implementing a reliable and scalable ransomware protection and recovery strategy can help you respond to and recover from an attack quickly. Do you have a ransomware protection strategy in place? Do you have visibility into your application complexities and dependencies? Are you able to recover your applications and data in a safe environment for analysis? Does your team have the required experience, skills, and time? Our VMware Pro Cloud Service™ to Implement Ransomware Protection and Recovery can help.

Service overview

VCF Professional Services can help you create and implement a ransomware recovery strategy that enables protection and full recovery of your business-critical workloads on VCF. Delivered by a cross-functional team of VMware technology experts, we leverage reference architectures to provide a standardized and prescriptive approach to defining and implementing your recovery strategy.

Develop a protection and recovery strategy

We start by creating your strategy. We work with you to develop an approach based on your business goals and constraints. We identify risks, time constraints, cost constraints, storage constraints, and application constraints and requirements. Then we define a high-level recovery plan with specific execution tasks.

Discover and analyze the environments

Next, we discover and analyze the environments to be protected. This includes information on virtual workloads, applications, and virtual infrastructure. We evaluate packet flow between workloads in the current environment. Based on packet flow we determine dependencies within each application and between applications, define protection groups, and establish restart priorities. We

Learn more

Visit vmware.com/services

configure replication timing and snapshot frequency to match your required RPO and RTO.

Create a recovery plan

Your recovery strategy may consist of multiple recovery plans. Recovery plans control all the steps in the recovery process. A recovery plan can contain one or more protection groups, and a protection group can be included in more than one recovery plan. This flexibility allows for the construction of robust, composite plans as well as very focused subsystem plans depending on your testing and failover objectives. For example, you may have a recovery plan to recover a single web app, a recovery plan to recover email, and a recovery plan to recover an entire site. We define the scope of each recovery plan as well as the recovery steps and sequence.

Design and configure the solution at the isolated recovery environment (IRE)

We design and configure an IRE, which is a clean and secure network environment used specifically for recovery from ransomware attacks. We configure the solution and map protected site resources, such as network segments, to recovery site resources. We configure the replication timing and snapshot frequency to match your identified RPOs and RTOs based on threat scan frequency. We also configure the disk image snapshot frequency as well as the duration of the snapshot retention.

Validate the guided recovery workflow

To validate the guided recovery workflow, we verify that all protected VMs are isolated and remediate if necessary. We verify replication timing and snapshots. Then we test run the recovery steps for resources in the IRE. We determine any changes that are needed, update the recovery plan(s), and then revalidate. This is performed until the workflow is reliable.

Get started operating your recovery solution

To help you effectively manage and operate your ransomware protection and recovery solution, we provide best practices and standard operating procedures. This includes establishing ongoing processes to detect and manage configuration drift. We provide guidance on how to integrate these operating procedures with your existing procedures. We also help enable your IT team through knowledge transfer throughout the engagement.

Benefits

VCF Professional Services can help fast-track your path to cyber resilience. We can create and implement a ransomware protection and recovery strategy that meets your security objectives, accelerate time-to-protection, and simplify ransomware recovery operations. We use a proven, scalable, and repeatable methodology to help ensure fast and consistent implementation and establish ongoing processes to continuously validate recovery plans and remove configuration drift.

vmware® by Broadcom