Table of Contents

VMware Cloud Disaster Recovery

General

Q. What is VMware Cloud Disaster Recovery?

A. VMware Cloud Disaster Recovery is an easy-to-use, on-demand disaster recovery (DR) solution, delivered as SaaS, with cloud economics.

Q. What is the difference between VMware Cloud Disaster Recovery, VMware Site Recovery, and VMware Site Recovery Manager?

A. VMware Cloud Disaster Recovery is a Disaster Recovery as-a-service (DRaaS) solution that can be used to cost-effectively protect a broad set of your virtualized applications, with fast recovery capabilities. VMware Site Recovery is also a DRaaS solution that can be used to protect mission-critical applications that have a very low RPO and RTO. VMware Site Recovery Manager is an enterprise software solution, deployed and managed by you in your data center to facilitate DR protection to a secondary DR datacenter that you manage yourself.

Q. How is VMware Cloud Disaster Recovery a cost-effective DRaaS solution?

A. There are three primary ways in which VMware Cloud Disaster Recovery is cost-effective. First, you no longer need to own and continuously maintain a secondary DR site. Second, you can utilize an efficient cloud storage layer provided by the service to store your backups during the steady state and only consume failover compute and primary storage capacity when a disaster event occurs. Finally, this service provides an operationally consistent and familiar vSphere experience across the production and DR sites, so your IT staff doesn't need to learn new tools.

Q. What regions are currently supported?

US West (Oregon)	Europe (Stockholm)
US East (N. Virginia)	Asia Pacific (Singapore)
US West (N. California)	Asia Pacific (Mumbai)
US East (Ohio)	Asia Pacific (Sydney)
Canada (Central)	Asia Pacific (Tokyo)
S. America (Sao Paulo)	Asia Pacific (Seoul)
Europe (Ireland)	Asia Pacific (Osaka)
Europe (London)	Asia Pacific (Hong Kong)
Europe (Milan)	Africa (Cape Town)
Europe (Frankfurt)	Middle East (Bahrain)
Europe (Paris)	

Getting Started

Q. How do I get started?

A. Getting started is easy. Simply reach out to us by going to VMware Cloud DR's *website* and clicking on "Get Started".

Q. How do I learn more about VMware Cloud DR before purchasing the service?

A. You can learn more about VMware Cloud DR by accessing Launchpad directly from *VMware Cloud Console* and access step-by-step guidance, relevant tools, and a rich set of resources. Click on "Learn More" under "Disaster Recovery" to navigate to launch your DR journey. This experience is available to everyone without requiring login to VMware Cloud.

Q. Do I need to learn new tools?

A. You use the same consistent, familiar vCenter management console and vSphere constructs on both your production and DR sites. For the DR service itself, you use an easy-to-use, SaaS-based management console.

Q. Do I need VMware Site Recovery to use VMware Cloud Disaster Recovery?

A. You do not need to enable VMware Site Recovery to use VMware Cloud Disaster Recovery.

Q. Do I need Site Recovery Manager (SRM) or vSphere Replication (VR) on my on-premises site to use VMware Cloud Disaster Recovery?

A. You do not need to deploy Site Recovery Manager (SRM) or vSphere Replication (VR) on your on-prem protected site to use VMware Cloud Disaster Recovery.

Q. What do I need to deploy on my source site?

A. You need to deploy one or more DRaaS Connector virtual machines on your source site vSphere environment to connect to the VMware Cloud Disaster Recovery components. DRaaS Connector is available as an easy-to-deploy OVA. You do not need to deploy any other appliance or hardware to connect to the VMware Cloud DR components in the cloud.

Q. Can I bring my own existing AWS account for VMware Cloud Disaster Recovery to use for the cloud storage?

A. The AWS account will be owned and managed by VMware, so you cannot bring your own AWS account.

Q. Can I setup Site Recovery Manager (SRM) style protection groups and recovery plans?

A. VMware Cloud Disaster Recovery supports grouping VMs into protection groups as well as creating DR plans managed by its SaaS Orchestrator component, like Site Recovery Manager. Protection groups can be based on VM names patterns or VM folder selection.

Q. Do I need a VMware Cloud on AWS SDDC in the steady state when I am only replicating to the cloud?

A. You do not need a VMware Cloud on AWS SDDC to be provisioned in the steady state. However, for customers that value low recovery times, we recommend a "pilot light" SDDC, which can currently be as small as a two host SDDC. Having a pilot light SDDC allows you to avoid the additional time needed to deploy an SDDC at the time of an outage and makes it possible to get alerts on the full set of automated DR health checks. Depending on your environment, it may also be helpful in pre-configuring the networking for your recovery SDDC and running foundational components such as Domain Controllers.

Q. Can I use the pilot light SDDC for running other VMs in the steady state, i.e., while I am only replicating?

A. Yes, the pilot light SDDC can be used for any purpose as it is a standard VMware Cloud on AWS SDDC in all respects.

Q. Can I use an existing VMware Cloud on AWS SDDC deployed from VMware Cloud console for recovery?

A. Yes, you can leverage an existing VMware Cloud on AWS SDDC deployed from VMware Cloud console for recovery. Clusters and hosts added from VMware Cloud console to this SDDC are automatically recognized by VMware Cloud DR.

Q. What are the bandwidth requirements with VMware Cloud Disaster Recovery?

A. The bandwidth required for replication would depend on the number, size, change rate, and RPO of the VMs that you are protecting. Upon recovery, you only need as much bandwidth to the cloud as is needed to communicate with your live workloads from your other sites and user endpoints.

Q. What are the connectivity requirements with VMware Cloud Disaster Recovery?

A. Connectivity between your protected site and VMware Cloud DR components can be over Internet, Direct Connect (DX) public and private Virtual Network Interface (VIF).

Technical

Q. How does VMware Cloud Disaster Recovery work?

A. Using a simple, cloud-based UI you can configure backup policies protect your VMs and DR plans to orchestrate recovery of those VMs. Backups are encrypted and stored in the native vSphere VM format in a highly efficient cloud storage layer called the Scale-out Cloud File System (SCFS) instead of primary storage in a VMware Cloud on AWS SDDC. When disaster strikes, with a few clicks you can recover your VMs to VMware Cloud on AWS using your pre-tested DR plans. The service can be used to quickly provision VMware resources and SDDCs in VMware Cloud on AWS. The recovered VMs can be immediately powered-on using the stored backups via a "live mount", i.e. an NFS datastore automatically mounted to all hosts in that SDDC.

Q. How can I be sure that my disaster recovery plan will work when I need it?

A. DR compliance checks are automatically run every 30 minutes to increase your confidence that your DR plan will work when you need it. Additionally, SLA Status view shows status for items related to Protection and Recoverability, including DR plans. You will be notified should an item require attention.

Q. How do I achieve fast recovery times?

A. The "live mount" capability of VMware Cloud DR provides fast recovery without a time-consuming rehydration of the backup data from cloud storage to VMware Cloud on AWS hosts. The backed-up data is immediately made available in the recovery SDDC via an NFS datastore mounted to the SDDC hosts. Having a small deployment of pre-provisioned pilot light hosts makes the recovery process even faster.

Q. Does VMware Cloud Disaster Recovery convert the VMs to a different format for backup and recovery?

A. Unlike many other cloud-based data protection solutions, VMware Cloud DR keeps your protected VMs in their native vSphere VM format which eliminates the need for brittle VM conversions that slow down recovery and make failback error-prone.

Q. Can I failover my workloads to an existing cluster of my pilot light SDDC?

A. At the time of outage, you can expand your existing cluster of your pilot light SDDC to recover your workloads. You need to make sure that the cluster can accommodate the new hosts that might get added to accommodate recovery of your workloads. Once your production site is back up, you can failback, after which the VMs on your recovery SDDC will be turned off, the hosts will be undeployed and cluster will be scaled down.

Q. Does VMware Cloud Disaster Recovery support failback?

A. Yes, VMware Cloud DR supports an efficient, delta-based orchestrated failback back of the recovered VMs to your protected site when it becomes available again.

Q. How does failback work?

A. When you are ready, you can use the VMware Cloud DR management console to initiate failback. The changed data is compressed, encrypted, and automatically sent back to the original protected site.

Q. Does VMware Cloud Disaster Recovery support multiple backups for a single VM?

A. Yes, both VMware Site Recovery and VMware Cloud Disaster Recovery support the ability to retain multiple point-in-time snapshots for any protected VM. VMware Site Recovery allows you to retain up to 24 copies per VM. VMware Cloud DR allows you to retain more than 24 point-in-time snapshots for every VM. You can configure multiple schedules for each VM, and each schedule can have a different retention period.

Q. Can I recover from an older point-in-time snapshot?

A. You can recover from any point-in-time snapshot that is available based on your configured retention policies. Any of these snapshots – including the most recent one – can be used to immediately power-on your VMs, using the "live mount" capability.

Q. What storage options do you support for protection with VMware Cloud Disaster Recovery?

A. VMware Cloud DR supports the protection of vSphere VMs running on any vSphere compatible storage on a VMFS, NFS, vVols or vSAN datastore.

Q. How does the DRaaS Connector get updated?

A. DRaaS Connector will be updated automatically and seamlessly without your intervention so that it stays compatible with the cloud service.

Q. Can I run my recovered workloads on SCFS instead of VMware Cloud on AWS SDDC?

A. You can choose to run recovered VMs directly from the SCFS. If you select this option, failover is faster and there is no dependency on SDDC hosts for storage capacity. With this option, the SDDC can be substantially smaller in size because VMs are kept on the SCFS, eliminating the vSAN storage capacity constraints. This configuration can be more cost effective, however there is a potential performance degradation for very large or I/O intensive workloads running on SCFS. In the case of underperforming workload performance, storage vMotion to vSAN on the SDDC is available on a per-VM basis once failover is completed for the DR plan.

Q. Can I configure my DR Plans to always run recovered workload storage on the VMware Cloud on AWS SDDC?

A. Yes, you have the option to configure DR plans to run recovered workloads on the SCFS or on the VMware Cloud on AWS SDDC.

Support & Additional Resources

Q. How can I get support when using VMware Cloud Disaster Recovery?

A. You can contact VMware Support for any issues you face while using VMware Cloud DR.

Q. Where can I see a demo of VMware Cloud Disaster Recovery?

A. You can view pre-recorded demos *here*, which cover key VMware Cloud Disaster Recovery capabilities. Please reach out to your VMware Cloud Sales representative if you are interested in a live demo of the service.

Q. Is there a Hands-on-Lab that I can use?

A. A Hands-on-Lab for VMware Cloud Disaster Recovery is available in VMware HOL catalog *here*.

Q. Is there technical documentation available?

A. You can find the official technical documentation for VMware Cloud DR *here*.

Q. Where can I find operational limits for VMware Cloud DR?

A. You can find the operational limits for VMware Cloud DR *here*. Select "VMware Cloud Disaster Recovery" under "Select Product" and check all options under "All Categories" to view all the operational limits for VMware Cloud DR.

Q. Where can I find the datasheet for VMware Cloud Disaster Recovery?

A. You can find the datasheet for VMware Cloud Disaster Recovery *here*.

Q. What versions of other VMware software such as vCenter Server and ESXi work with VMware Cloud DR?

A. You can find the versions of VMware software that interop with VMware Cloud DR *here*.

Q. Where can I learn about the product roadmap for VMware Cloud Disaster Recovery?

A. The product roadmap for VMware Cloud DR is available under the "Disaster Recovery" category *here.*

Q. What service level agreement (SLA) do you offer for VMware Cloud Disaster Recovery?

A. Please refer to the Service Level Agreement document for VMware Cloud Disaster Recovery available *here.*

Q. Where can I find the terms and conditions for using VMware Cloud Disaster Recovery?

A. You can find VMware General Terms, located *here*. Additionally, refer to the Cloud Services Exhibit (located *here*) and review the VMware Cloud Disaster Recovery section of the VMware Cloud Services Guide, located *here*.

Q. Where can I find information about the most recent updates to VMware Cloud Disaster Recovery?

A. For information about the latest features and updates to the service, please refer to the release notes *here*.

Pricing

Q. Where can I find the price for VMware Cloud Disaster Recovery?

A. You can find the pricing for VMware Cloud Disaster Recovery on our *pricing page*.

Q. How can I purchase VMware Cloud Disaster Recovery?

A. Please refer to the *Getting Started with VMware Cloud Disaster Recovery* webpage to explore several options for purchasing VMware Cloud Disaster Recovery.

Q. What currencies are supported for purchasing VMware Cloud Disaster Recovery?

A. The following six currencies are supported for purchasing VMware Cloud Disaster Recovery: USD, GBP, EURO, JPY, AUD and CNY. You can transact in these currencies and protect your workloads in one of the AWS regions where VMware Cloud DR is available.

Q. How do I pay for VMware Cloud Disaster Recovery?

A. If you purchased VMware Cloud Disaster Recovery directly through VMware, you could pay for the service by redeeming SPP (Subscription Purchasing Program) credits, including SPP credits specifically appliable to VMware Cloud on AWS. Refer to the *VMware Subscription Purchasing Program* guide for further information on SPP credits.

As an alternative to SPP credits, you can also purchase VMware Cloud Disaster Recovery through *Pay by Invoice*, by *using a credit card*, or through a 2-tier commerce model where distributors will receive the opportunity to enable a significant volume discount for a specific reseller/end customer combination. Distributors make payments monthly on their upfront commitment by signing a Commitment Based Contract (CBC) with VMware and committing to spend a certain amount of money on behalf of the reseller/end customer combination over a specified period. The distributor will be charged monthly by VMware based on your associated consumption of VMware Cloud DR. You have the complete freedom of self-service to configure your service and purchase VMware Cloud DR subscriptions.

If you purchased VMware Cloud Disaster Recovery though AWS, the payment instruments, terms of service, region, currency, and so on, are determined by your relationship with AWS and the Enterprise Discount Program (EDP) credits that you purchased through them. Contact your AWS sales team for all questions related to pricing and billing.

Q. When will I pay for VMware Cloud Disaster Recovery service?

A. You will be charged for the service at the following points:

- When you purchase a 1-year or 3-year committed term subscription, you will be charged upfront for the full amount of the one- or three-year subscription. You can also choose to pay monthly for the one- or three-year subscription, in which case you will be charged every month until the end of your subscription term.
- Every month, you will be charged in arrears for any metered data capacity usage, protected VM count or ransomware recovery add-on VM count that exceeds your active committed term subscriptions.
- When you elect to purchase data capacity, protected VM count or ransomware recovery VM count on-demand, every month, you will be charged in arrears for your metered usage.

Q: How are charges determined for VMWare Cloud Disaster Recovery?

A. VCDR pricing consists of a per-VM charge for each protected VM and a per-TiB charge which consists of the sum of logical storage size of the protected VMs, and all incremental cloud backups retained. The service is offered on a term subscription or on-demand or basis, with a minimum charge of 10 TiB per recovery region. VMware Ransomware Recovery add-on pricing consists of a per-VM charge for each protected VM.

Service usage for components is metered hourly and billed monthly at on-demand rates if no subscription exists. Term subscriptions do not auto-renew at the end of their term. Continued service use beyond an expired subscription term will be billed at the then current on-demand rate until on-demand use is terminated. Disaster recovery "failback" data transfer (i.e., egress) charges billed by cloud hosting providers will be borne by VMware up to 50% of the protected VM storage capacity. VMware reserves the right to charge for excessive failback data transfer, which is more than 50% of VM storage capacity.

Q. Can I try out the service before committing to a long-term subscription?

A. VMware Cloud DR can be purchased completely on-demand. This means that every month you will be charged in arrears for your metered usage of data capacity and protected VM count. There is a 10 TiB minimum per Orchestrator Recovery Region, irrespective of actual usage. There are no limitations to how long to run VMware Cloud DR on-demand for.

Q. Does the VMware Cloud Disaster Recovery pricing include VMware Cloud on AWS hosts?

A. No, you must separately purchase the VMware Cloud on AWS hosts required for DR testing and recovery of your protected VMs. VMware Cloud on AWS hots are not included in VMware Cloud Disaster Recovery pricing. More information about host pricing can be found on the *VMware Cloud on AWS pricing page*.

Q. I am using VMware Cloud DR to protect workloads on VMware Cloud on AWS SDDC. How will I get charged for data transfer between source SDDC and recovery site?

A. When using VMware Cloud DR to protect workloads on VMware Cloud on AWS SDDC, there will be replication traffic going out from the protected SDDC to VMware Cloud DR. Depending on the network connectivity and the location of your source and target site, you might get charged for data transfer. Data transfer charges show up on your VMware Cloud on AWS bill. Refer to *this article* to find your VMware Cloud on AWS data transfer costs.

Q. Are there any other costs that I should be aware about?

A. The VMware Cloud DR price includes the underlying cloud infrastructure used by the service including cloud storage, cloud compute instances, managed databases, cloud network devices, and cloud management tools.

Additionally, egress data charges incurred during typical use of the service for replication from on-premises to the cloud and failback to the original protected site over the internet are also covered by VMware Cloud DR price. However, VMware reserves the right to bill you for additional charges corresponding to excessive egress data transfers for failback.

Q. What do you consider excessive egress data transfers, for which I might be billed additional charges?

A. After you have recovered your virtual machines into a VMware Cloud on AWS SDDC, you may choose to use the failback capability to move your VMs back to your original protected site. To facilitate this failback in an efficient manner, VMware Cloud DR transfers only the VM data that has changed since the VMs were recovered into VMware Cloud on AWS. You will not receive a separate bill from AWS for the egress data transfer charges over the internet incurred in this process, and instead these charges will be borne by VMware. However, the amount of data transferred can become excessively large if there is a long delay between the recovery and the failback or if none of the old data is available on the protected site anymore. VMware reserves the right to bill you for additional charges corresponding to excessive egress data transfers as part of a failback operation – defined as more than 50% of the protected data capacity. The following rates apply to these excessive egress data transfer over the internet:

VMware Cloud on AWS region	Applicable rate per GiB* transferred
US East (N. Virginia)	$0.050
US East (Ohio)	$0.050
US West (N. California)	$0.050
US West (Oregon)	$0.050
Asia Pacific (Singapore)	$0.080
Asia Pacific (Mumbai)	$0.080
Asia Pacific (Osaka)	$0.084
Asia Pacific (Sydney)	$0.092
Asia Pacific (Tokyo)	$0.084
Asia Pacific (Seoul)	$0.108
Asia Pacific (Hong Kong)	$0.080
Canada (Central)	$0.050
South America (Sao Paulo)	$0.114
Europe (Frankfurt)	$0.050
Europe (London)	$0.050
Europe (Ireland)	$0.050
Europe (Paris)	$0.050
Europe (Stockholm)	$0.050
Europe (Milan)	$0.050
Africa (Cape Town)	$0.112
Middle East (Bahrain)	$0.065

* 1 GiB equals 2^{30} bytes

Q. Does the VMware Cloud Disaster Recovery price include egress data transfers for VMs running on the recovery SDDC in VMware Cloud on AWS?

A. No, you will be separately charged for egress data transfers incurred by the recovered VMs when they are running in a VMware Cloud on AWS SDDC at the applicable VMware Cloud on AWS rates.

Q. Is there a minimum purchase required for VMware Cloud Disaster Recovery?

A. No, there are no minimum purchase requirements. However, there is a 10 TiB minimum per Orchestrator Recovery Region, irrespective of actual usage.

See example in table below:

Recovery Region	Data capacity usage per Recovery Region	Total data capacity usage	Total minimum charge
US West	20 TiB	26 TiB	3 Regions x 10TiB per region = **30 TiB**
US East	5 TiB		
Central	1 TiB		

Q. How is data capacity calculated?

A. Data capacity in TiB is calculated as the sum of the logical storage size of the protected VMs and all the incremental cloud backups you choose to retain (where 1 TiB is equal to 2^{40} or 1,099,511,627,776 bytes). For an accurate calculation of data capacity, please engage your VMware Cloud Sales representative.

Q. Can I co-term VMware Cloud Disaster Recovery subscriptions with VMware Cloud on AWS host subscriptions or VMware Site Recovery subscriptions?

A. No, co-terming capabilities are not available. You will have to manage the terms of the different subscription offerings.

Q. How can Managed Service Providers (MSP) purchase VMware Cloud Disaster Recovery?

A. VMware cloud providers who have signed up for the MSP agreement and have a VMware Cloud on AWS commit contract can purchase VMware Cloud Disaster Recovery service. Service providers must have both a VMware Cloud on AWS commit contract and a VMware Cloud Disaster Recovery commit contract in place. See *FAQ for VMware Cloud Disaster Recovery on Cloud Partner Navigator* for further details.

VMware Ransomware Recovery

General

Q. What is VMware Ransomware Recovery for VMware Cloud DR?

A. VMware Ransomware Recovery is designed to address the top challenges organizations face when recovering from ransomware attacks:

- Identifying recovery point candidates
- Validating restore points
- Preventing reinfection
- Minimizing data loss
- Minimizing downtime

It is a purpose-built ransomware recovery as-a-service solution that delivers industry-leading capabilities to aid in recovery from ransomware attacks. For more details, please refer to our *Announcement Blog*.

Q. Does VMware Ransomware Recovery help protect me from ransomware attacks?

A. VMware Ransomware Recovery is the last line of defense to help recover business operations when all other ransomware detection and preventative measures have failed. It focuses on the recovery aspect when systems have been encrypted.

Q. Is VMware Ransomware Recovery a standalone product?

A. No. VMware Ransomware Recovery is sold as an add-on to VMware Cloud DR.

Q. Are VMware Cloud DR's base ransomware recovery capabilities available if I decide not purchase VMware Ransomware Recovery?

A. Yes. Immutable backups, operational air-gapping, instant power-on, and guest file restore capabilities will continue to be available in the base VMware Cloud DR offering. The VMware Ransomware Recovery add-on builds on these capabilities by adding additional features that aid in recovering from ransomware attacks.

Q. In what regions will the VMware Ransomware Recovery service be available?

A. VMware Ransomware Recovery will be offered globally in all AWS regions where VMware Cloud DR is supported.

Getting Started

Q. How do I get started with VMware Ransomware Recovery?

A. It is a prerequisite that VMware Cloud DR be configured for use. Once the DRaaS service is configured and ready, the VMware Ransomware Recovery add-on can be enabled and configured for use with each of your recovery plans.

Technical

Q. How does VMware Ransomware Recovery work?

A. VMware Ransomware Recovery is a purpose-built ransomware recovery as-a-service solution that extends our existing VMware Cloud DR offering delivering the following capabilities:

- Provides air-gapped immutable cloud-based VMDK backups from which users can protect and then recover their VMDKs and data
- An on-demand Isolated Recovery Environment for safely and securely powering on infected VMs for the purpose of inspection and cleansing
- A guided ransomware recovery workflow that guides users through the end-to-end process across identification, validation and restore of recovery points
- Guided restore point selection that surfaces metrics such as VMDK rate of change and file entropy to inform selection of recovery point candidates
- Embedded NGAV and behavioral analysis of powered-on workloads in an on-demand, VMware-managed Isolated Recovery Environment (IRE)
- Push-button VM network isolation levels to prevent reinfection during restore point validation in the IRE

This is integrated into the VMware Cloud DR UI, and all of these workflows and features can be invoked directly from there.

Q. Is technical documentation available for VMware Ransomware Recovery?

A. Online documentation on VMware Ransomware Recovery can be found *here*.

Q. How do I enable VMware Ransomware Recovery?

A. VMware Ransomware Recovery is enabled via a new recovery plan configuration setting. If protection is desired on VMs that span multiple plans, each plan must be enabled individually.

Q. How do I specify which VMs are protected with VMware Ransomware Recovery?

A. All VMs included in a ransomware recovery-enabled recovery plan are protected with VMware Ransomware Recovery.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com

Q. What is an Isolated Recovery Environment (IRE)?

A. An IRE is a secure and safe environment used for validating VMs infected with ransomware that leverages VMware Cloud on AWS.

Q. Can I use my VMware Cloud DR pilot light SDDC hosts as the Isolated Recovery Environment?

A. Yes

Q. Can I use VMware Cloud DR on-demand SDDC hosts as the Isolated Recovery Environment?

A. Yes

Q. How is VMware Ransomware Recovery's Isolated Recovery Environment different from other vendors or approaches?

A. By leveraging VMC on AWS and using a small Pilot Light or on-demand deployment, customers can avoid the expense of building secondary / isolated datacenter infrastructure stacks to build and manually manage their own IREs (Isolated Recovery Environments).

Q. Does VMware Ransomware Recovery analyze and scan recovery-candidate snapshots to find ransomware attack indicators and related malicious code?

A. Yes. VMware Ransomware Recovery embeds NextGen Antivirus (NGAV) and behavioral analysis directly inside of the ransomware recovery workflow and automatically analyzes snapshots for ransomware attack Indicators of Compromise (IOCs), searches for workload vulnerabilities (unpatched software) and performs malware scanning.

Q. What is NextGen Antivirus and behavioral analysis and why does it help identify ransomware attacks vectors?

A. NextGen Antivirus takes traditional antivirus software to a new, advanced level of endpoint security protection. It goes beyond known file-based malware signature searches by using predictive analytics driven by machine learning and artificial intelligence and combines with threat intelligence to:

- Detect and prevent malware and fileless non-malware attacks
- Identify malicious behavior and Tactics Techniques & Procedures (TTPs) from unknown sources
- Collect and analyze comprehensive endpoint data to determine root causes
- Respond to new and emerging threats that previously go undetected

Learn more about NGAV and behavioral analysis by clicking *here*.

Q. Is traditional file scanning effective at finding ransomware?

A. No. Ransomware bad actors learned many years ago how to avoid being detected by traditional file scanning tools. They often change file hashes prior to loading a malicious payload on the victim's machine and delete the malicious file(s) immediately after being utilized to begin the attack sequence – both of these (and other TTPs) defeat the traditional file scanning approach.

Q. Can I integrate other EDR products with VMware Ransomware Recovery (i.e., CrowdStrike, MSFT Defender)?

A. While other EDR products may continue to be used on the Protected site, use of non-VMware NGAV and behavioral analysis tools in conjunction with VMware Ransomware Recovery will require a manual process of opening Isolated Recovery Environment networking paths to allow VM access to third party cloud-based security tools.

Support & Additional Resources

Q. How can I get support when using VMware Ransomware Recovery?

A. You can contact VMware Support for any issues you face while using VMware Ransomware Recovery.

Pricing

Q. Where can I find the price for VMware Ransomware Recovery?

A. You can find the pricing for VMware Ransomware Recovery on our *pricing page*.

Q. What is the licensing metric for VMware Ransomware Recovery?

A. The licensing metric is per protected VM.

Q. Does the VMware Ransomware Recovery pricing include VMC hosts?

A. No, like VMware Cloud DR, VMC hosts must be purchased separately.

Q. Will I need to purchase extra storage capacity for the ransomware recovery use case?

A. Ransomware attacker "dwell time" can range from days to months. To ensure adequate recovery options in the event of an attack, you must have sufficient snapshot history. A minimum of 3–6 months of snapshot retention is recommended.

Q. Do I need to include all VMs protected by VMware Cloud DR with VMware Ransomware Recovery?

A. No. While most VMs will benefit from VMware Ransomware Recovery protection, you can select which recovery plans to protect with VMware Ransomware Recovery.

Q. Can I consume VMware Ransomware Recovery via a subscription and/or on-demand metered pricing?

A. Both. VMware Ransomware Recovery is offered in 1- & 3-year subscriptions, on-demand, or a combination of both based on your ransomware protection needs.