February 2025

Isolated Recovery Environment

Ransomware Recovery IRE

vmware by Broadcom

Ransomware Recovery – Do you have an IRE?

When it comes to ransomware recovery tasks, an IRE is an essential part of the recovery infrastructure. But what is it and how do you get one?

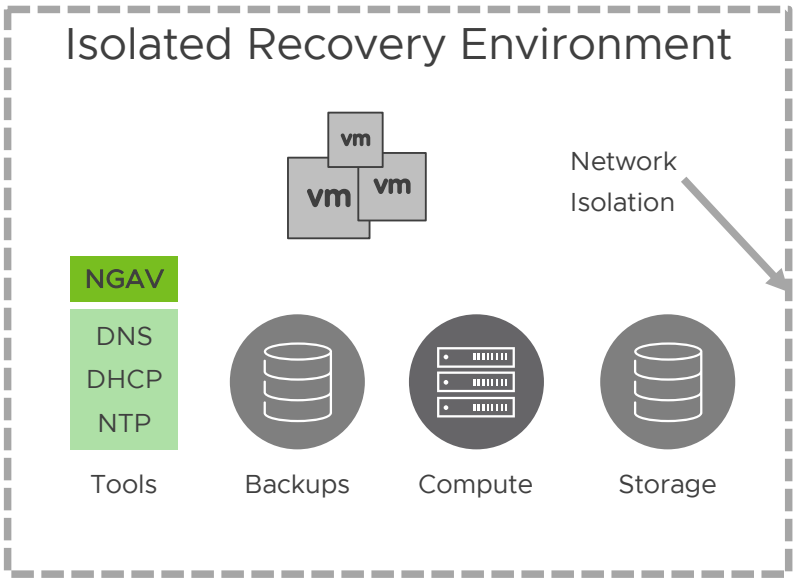
In this article, IRE stands for Isolated Recovery Environment – and the VMware Live Recovery ransomware recovery solution makes it quick and easy to provision one – leading to faster recovery times, less risk in operations and reduced systems complexity. As shown in this video, this solution can also lower costs by leveraging cloud-based, SaaS capabilities to provide the IRE capability for you when needed.

What is an IRE?

Search the internet for a definition of an IRE and you'll find several common capabilities identified such as:

- dedicated, secure recovery environment that is inaccessible to attackers,
- equipped with resources and tools to aid the response team to verify and recover data,
- efficient access to immutable backup copies to enable rapid iteration of recovery points if needed.

Many organizations understand the value of and IRE and are considering the likely large and expensive investment to build and manage their own IRE for ransomware preparedness. This investment often comes in addition to their primary data center infrastructure responsibilities. The basics structure of an IRE looks something like this:



But instead of building your own IRE, what if the IRE could be:

- acquired through simple subscription means and managed for you,
- consumption based (i.e., only pay for what you use),
- available off-site, in the cloud where compute and storage resource elasticity allow for scaling up and down of the environment as needed.

Why do you need an IRE?

When faced with a ransomware attack that has penetrated your operational defense systems in your production environment and a VM recovery from a backup recovery point is the next option, organizations must work from the premise that their

backup data has also been infected to some degree. Simply restoring a previous point in time that appears uninfected back into operations is insufficient.

It is likely you will not know exactly when the malware infection occurred as ransomware can sit dormant (dwell time) long before inflicting the visible damage. Not properly handling the selected recovery point might end up re-introducing the ransomware into the environment causing more harm than good.

The recommended approach and usually the first step in recovery from many 3rd party security companies is to restore the backup data to an isolated recovery environment (IRE), so that the ransomware can be contained and remedied before migrating the impacted virtual machines – and their data - back into a production environment.

An IRE provides a staging area for restored virtual machines that is, by definition, isolated from other networks. This allows the remediation process to proceed without encountering external ransomware triggers and without the risk of infecting other workloads.

NOTE: In addition to recovery needs, an IRE is useful for regular recovery testing and can provide a safe environment for the security teams to run attack simulations.

How can you get an IRE?

Building and running a dedicated isolated recovery environment can be cumbersome, time consuming, and expensive. A physical IRE must be in place prior to any attack to be useful, requiring significant capital and effort to acquire and deploy, patch, and maintain over time. VMware Cloud services such as VMware Cloud on AWS make it easy to quickly build an IRE, something as simple as a two-node VMware Cloud software defined data center (SDDC) can be the IRE. In just a couple of hours for provisioning and configuration, you could have a new, clean environment to run your VMs as they are analyzed and remediated to eliminate the ransomware threats.

Leveraging the advanced firewall capabilities of the VMware Cloud on AWS SDDC, with full automation provided by the built-in VMware Live Recovery ransomware recovery workflows, you can easily create the desired network isolation – even down to the individual VM level. This helps assure that VMs running in the IRE do not inadvertently get infected by other VMs – or cause re-infection from their own behavior.

Integrating NGAV tools into the SDDC IRE provides a robust configuration for conducting the desired malware scanning tasks needed to detect: (1) system vulnerabilities, (2) known malware file signatures, and (3) most importantly, behavior analysis of running systems. This last detection method of behavior analysis is critical to help catch the more recent and problematic fileless methods being exploited in ransomware attacks.

The VMware Live Recovery ransomware recovery solution also provides the source of your off-site, immutable backups and safely presents these recovery points directly to the SDDC in your VMware Cloud on AWS configuration. From this setup, you can quickly bring any recovery point into inventory in the safety of the IRE. VMware Live Cyber Recovery can also make the process of provisioning or decommissioning an SDDC for recovery fast and easy from a common UI.

How VMware helps with ransomware recovery

For immutable backups, VMware Live Cyber Recovery provides the protection of production VM workloads into hundreds of easily and quickly accessible recovery points to use in the IRE. These are kept in the Scale-Out Cloud File System (SCFS). This repository is presented directly to the IRE SDDC for restoring the VMs.

For network isolation control, VMware Live Recovery integrates with built-in firewall capabilities and provides push-button network isolation functionality based on the VMs protected in the SCFS. These network isolation control rules are built into the IRE as part of the overall ransomware solution.

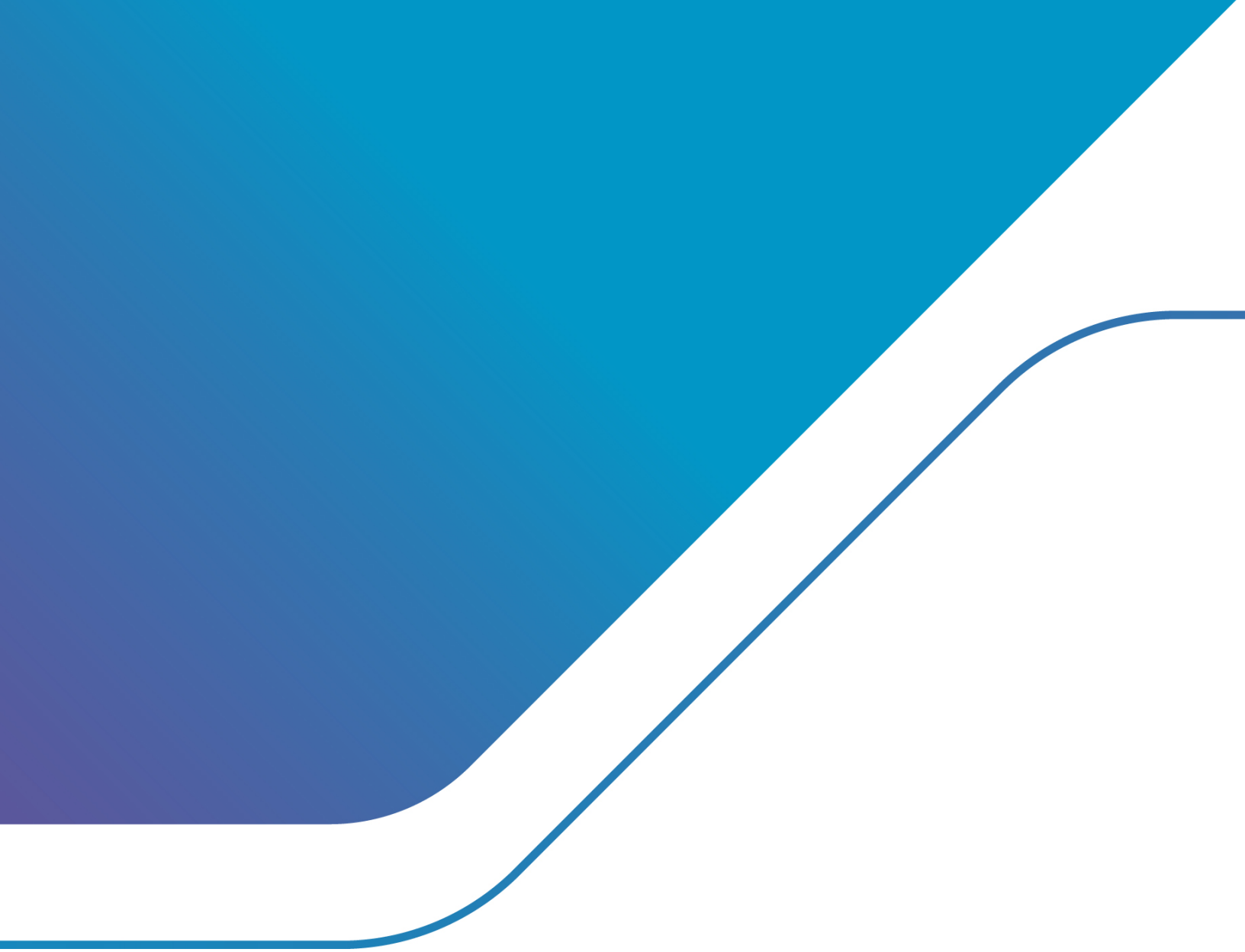
For the needed tools to help with analysis and remediation, VMware Live Cyber Recovery integrates with Broadcom Carbon Black Cloud and installs the cloud workload appliance directly into the IRE. The ability to inject the malware detection sensors into the VMs when being recovered into the IRE further simplifies and automates the validation processes.

And finally, the infrastructure to run the IRE is provisioned from VMware Cloud on AWS – either directly in VMware Cloud on AWS and then attached to the recovery solution – or from within VMware Live Cyber Recovery interface.

Once the remediation process is complete, workloads can be migrated back into the original production site without fear of re-introducing ransomware. When finished with the IRE, it can simply be deleted. You can create and pay for an IRE only when needed.

These capabilities help simplify the entire ransomware recovery workflow, minimizes risk, and provide significant cost savings versus other on-premises and Cloud-based ransomware recovery solutions.

For more information visit VMware Live Recovery or the VMware Resource Center.



vmware® by Broadcom

Item No: vmw-bc-wp-tech-temp-uslet-word-2025 1/24