Why VMware Ransomware Recovery

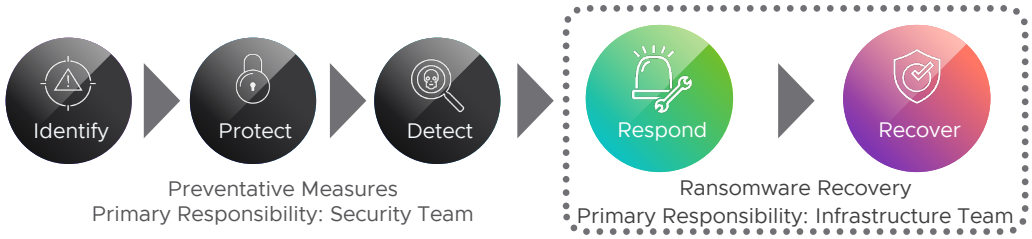
What is VMware Ransomware Recovery?

A fully managed Ransomware Recovery-as-a-Service solution that offers confident recovery from existential threats, quick recovery with guided automation, and simplified recovery operations.

Ransomware attacks are becoming prevalent and sophisticated

66%[1]	30 days[1]	4%[1]	$4.62M[2]
of organizations were attacked in 2021.	on average to recover from a ransomware attack.	who paid ransom and recovered all their data.	is the average total cost of a ransomware breach.

Ransomware recovery is a critical last line of defense



Preventative Measures
Primary Responsibility: Security Team

Ransomware Recovery
Primary Responsibility: Infrastructure Team

Yesterday's solutions cannot address Modern Ransomware

1989	2017	Today
Ransomware 1.0	**Modern Ransomware**	
Attacker conceals malicious code in executable files. When opened, the malware is activated.	*Fileless attacks that leverage legitimate programs (e.g. memory-based or living-off-the-land). Hard to detect and lies dormant. Represents 60-70% of attacks today.*	

Table stakes capabilities	Why it is not enough today	What you need to address Modern Ransomware
Immutable and air-gapped backups	Modern Ransomware can remain dormant in backups and reinfect systems after recovery.	A dedicated and secure **Isolated Recovery Environment (IRE)** for staging and validating recovery points to prevent reinfection of the production environment.
Traditional file scanning	Modern Ransomware does not rely on files and cannot be detected with file scanning.	**Next-Gen Anti-Virus with behavioral analysis** of running workloads to identify Modern Ransomware, which is only observable when the workload is running and exhibiting anomalous behavior.

The VMware Ransomware Recovery advantage

- On-demand provisioning of a **fully-managed IRE with advanced software-based firewall rules** to prevent reinfection at recovery
- Identify Modern Ransomware by inspecting powered-on workloads with **Next-Gen Anti-Virus with behavioral analysis**.
- Streamline and automate recovery with a **guided ransomware recovery workflow**, which integrates identification, validation and restore of recovery points.

The only solution in the market that will help your organization recover from Modern Ransomware. VMware is the only vendor that provides all these capabilities in a single, integrated experience.

To learn more:

Visit our webpage

[1]Sophos State of Ransomware 2022
[2]IBM Cost of a Data Breach Report 2022

Why VMware Ransomware Recovery (Q&A)

Q. What are fileless attacks in Modern Ransomware?

A. Historically, most ransomware attacks were file-based, which would entice users to open certain types of files, and when opened, execute malicious code. Starting in 2017, fileless attacks started to emerge. A fileless attack is one in which an attacker uses existing software, legitimate applications and authorized protocols to carry out malicious activities. Examples include embedding malicious code directly into memory and hijacking native tools like PowerShell to encrypt files. In the notorious Log4j vulnerability that exposed hundreds of thousands of systems to attacks, cybercriminals were able to remotely inject malicious code into a target network and gain control. More and more attackers are moving away from traditional malware – in fact, 60-70%[1] of today's attacks involve 100% fileless techniques.

VMware Ransomware Recovery was purpose-built to identify and cleanse fileless attacks, so that customers can confidently recover from Modern Ransomware.

Q. Why can't traditional file scanning detect fileless attacks?

A. Fileless attacks use legitimate programs and are never written to disk themselves, so they cannot be detected by traditional file scanning of at-rest backup copies. They are only observable leveraging Next-Gen Anti-Virus with behavioral analysis, which looks for abnormal behaviors in running workloads. VMware Carbon Black is an example of an Endpoint Detection & Response software that leverage Next-Gen Anti-Virus with behavioral analysis.

VMware Ransomware Recovery embeds Next-Gen Anti-Virus with behavioral analysis directly into the ransomware recovery workflow to help customers identify both file-based and fileless attacks, and thereby properly validate the recovery points.

Q. How can fileless attacks "reactivate" themselves? Why do you need an Isolated Recovery Environment (IRE)?

A. Fileless attacks can remain undetected and dormant in the backups, and "reactivate" themselves when the backup VMs are powered-on again. This is because the first two priorities of bad actors are to establish persistence and then enable command-and-control capabilities. Restoring VMs without identifying and removing these attack points during the remediation process could re-introduce ransomware back into the production environment, causing more harm than good.

The recommended approach is to restore the backup data to an Isolated Recovery Environment (IRE), which is a dedicated and secure environment that isolates the powered-on VMs from other networks, the internet, and other VMs in the IRE. Using an IRE allows the remediation process to proceed without encountering external ransomware triggers and without the risk of infecting other workloads.

VMware Ransomware Recovery delivers a fully-managed IRE, which enables customers to prevent reinfection at recovery, and removes the need for them to build, secure and manage their own IRE. Next-Gen Anti-Virus, which is embedded into the recovery workflow is then used to identify both file-based and fileless attacks to ensure the VM is safe to restore back into a production environment.

[1] How to Combat Fileless Attacks, VMware Carbon Black.