



SUMMIT
TECHNOLOGY GROUP

ENABLE • INTEGRATE • OPERATE

What is Keeping You Up at Night?

Greg Colburn

SDDC Practice Director

gcolburn@thesummitgrp.com

Jill McKee

Sr. Account Executive

jmckee@thesummitgrp.com

Agenda

- Introductions
- The Threat Landscape
- What Can You Do?
- Introduction to VCDR
- Call to Action


STG Differentiated Solution Offerings & Capabilities



Data Center &
Cloud Solutions



Networking &
Security



Collaboration
Solutions



Strategic &
Operational Staff
Augmentation



Application
Development



Advanced
Consulting

<https://www.thesummitgrp.com/contact-us.html>



Two-thirds* of organizations were attacked by ransomware in 2022

76%* of them had their data encrypted

Ransomware is today (and will continue to be) a top CIO budget priority

Beyond direct monetary impact, it's an existential threat to organizations



2/3

Of organizations attacked in 2021; 76% had data encrypted¹

96%

Did not regain full access to data following a ransom payment¹

\$4.6M

Average cost of a ransomware breach²

\$42B

Projected worldwide damages in 2024 (up from \$20B in 2021)³

¹Sophos State of Ransomware 2022

²Cost of a Data Breach Report 2022, IBM Security

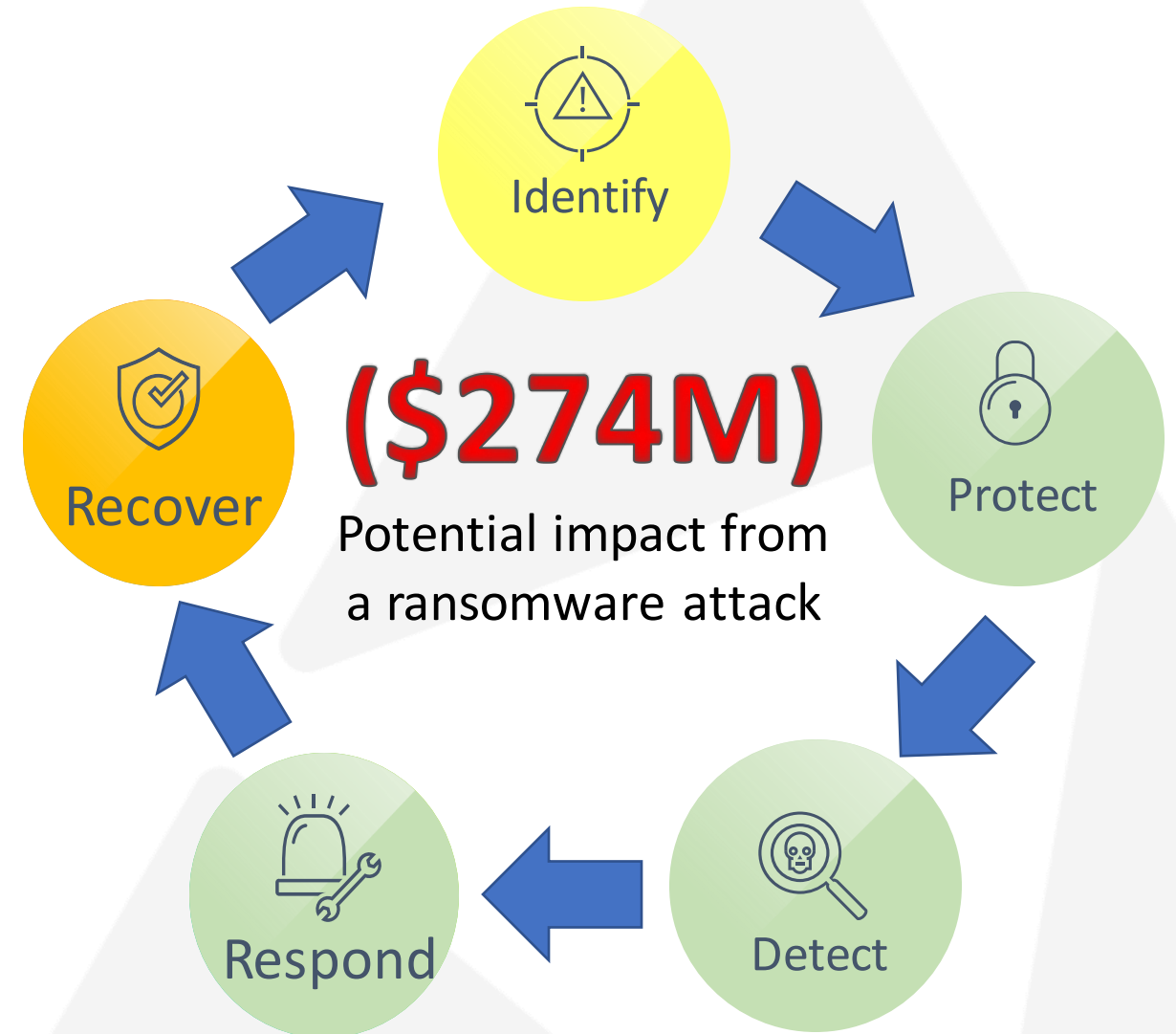
³Cybersecurity Ventures

Treat Ransomware Recovery as an Investment

Potential asset impact....

Current asset portfolio(EOY 2021):	\$ 3.6B
* Liabilities	\$ 2.9B
2022 growth projection: 6.9%	\$ 248M
Estimated Deposit impact: -5%	(\$145M)
Productivity impact/recovery cost:	(\$5M)
Estimated growth impact: -50%	(\$124M)
<u>Potential Total Impact:</u>	(\$274M)

- Based on average time to restore operations of 16 days
- 2021 & 2020 EOY Numbers Leveraged for calculations



Paradigm Shift in Ransomware Attacks

Until 2016

- File-based approach
- Examples:
 - TorrentLocker aka CryptoLocker
 - Cerber (Fast-changing files)
- Detected by signature match



Traditional-AV was usually sufficient

Post 2017

- Fileless, “Living off the Land”
 - Memory
 - Built-in OS programs & libraries
 - Stolen credentials (from black market)
- Disables security software ¹



Traditional-AV **fails**; need EDR, NGAV, XDR

Ransomware aaS? Yeah, it's a thing.



- The TAM or “Total Addressable Market” for Ransomware has led to the commoditization of malware.
- Subscription Service Model where malicious actors can pay a monthly or yearly subscription to access pre-written code for use.
- This expands the potential number of attack vectors as attackers no longer need to be deeply technical.
- Some subscriptions even have “Help Desk” offerings!

Source – [Cloudwards “Ransomware as a Service: What Is It and How Does it Work in 2022”](#)

A Pound of Prevention...

...Isn't always enough

- SOP has been focused on a traditional 3-tiered approach
 - People
 - Process
 - Technology
- Threat detection and avoidance along with corporate policies are evolving to meet the threat in new and more complex ways.
 - AI/ML based AV
 - Advanced firewalls
 - SASE
 - Micro-segmentation of networks
 - Security aaS offerings
 - Zero Trust models



Not If, But When

People are still the weak link



Phishing



Human
Error



Social
Engineering

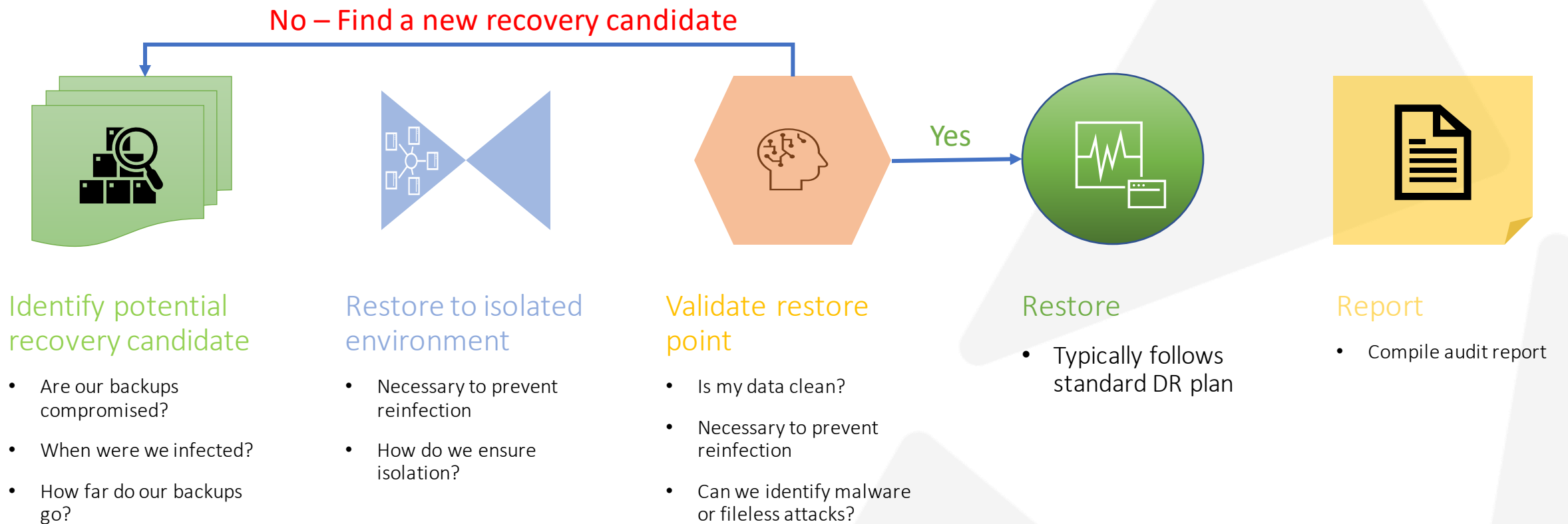


Disgruntled
Employees

What are you protecting against today?

- Traditional HA/DR planning has focused on the “Physical”
 - Data Center Outages
 - Network Interruptions
 - Data Corruption
 - “Smoking hole” scenarios
- RTO and RPO
- These are important – but in reality, are they really the biggest risk to your business?
 - Increasingly protection against malicious actors has come front and center

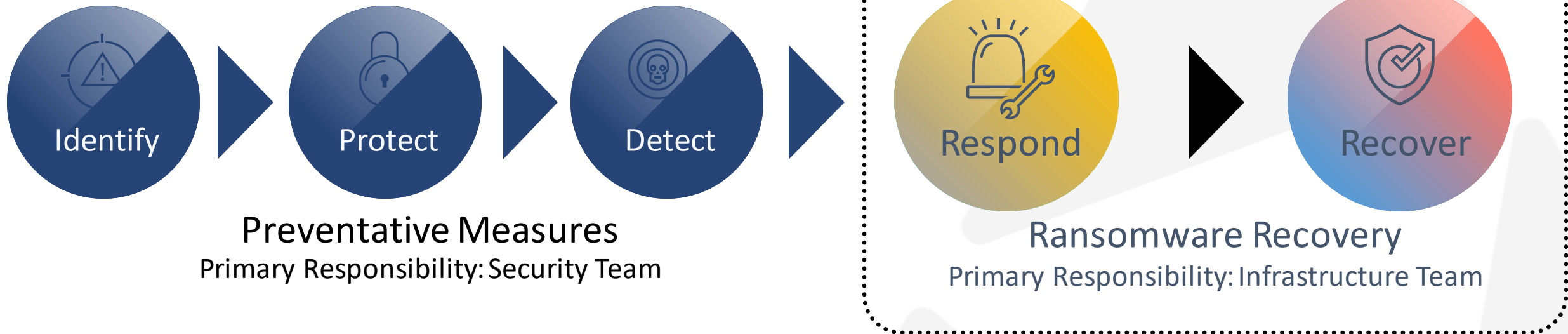
Ransomware Recovery \neq Disaster Recovery



Ransomware recovery is a critical last line of defense

Infrastructure Team is responsible for Recovery, working closely with Security Team

National Institute of Standards and Technology (NIST) Framework for Cybersecurity

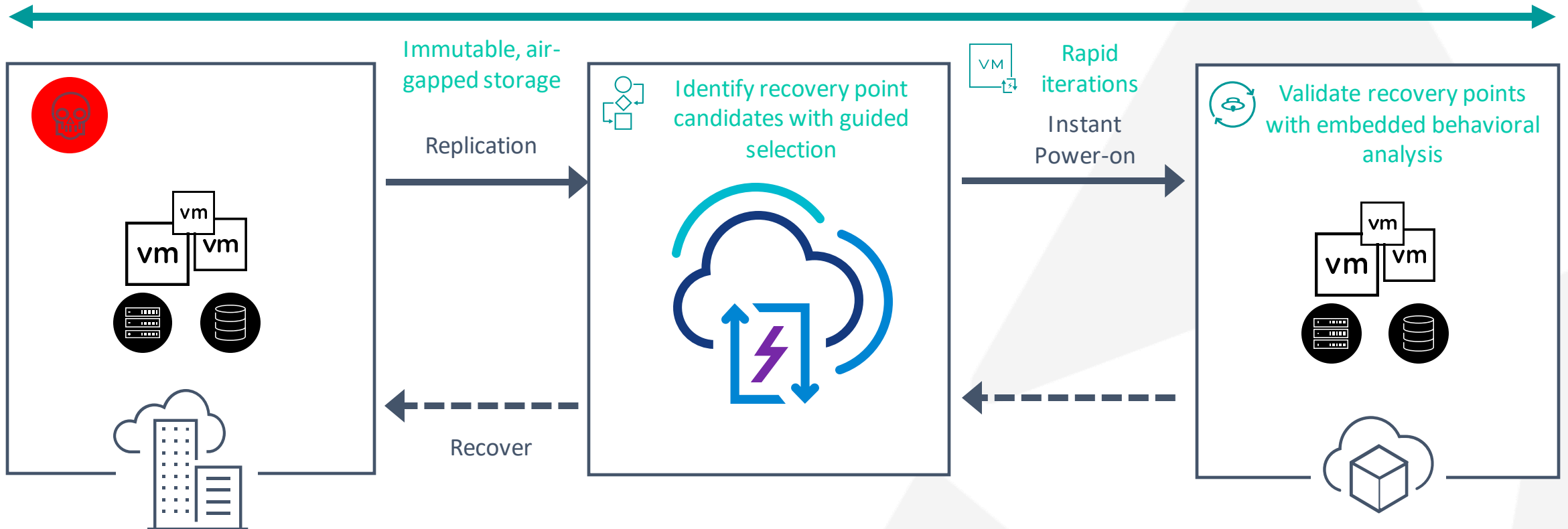


VMware Ransomware and Disaster Recovery

On-demand ransomware and disaster recovery, delivered as an easy-to-use SaaS solution



Streamline and automate operations with a dedicated ransomware recovery workflow



Blue: Disaster Recovery-as-a-Service Green: Next-Gen Ransomware Recovery-as-a-Service



Prevent reinfection with an Isolated Recovery Environment (Quarantined)

What makes VMware Ransomware Recovery Different?

A guided recovery workflow with embedded behavioral analysis in an on-demand IRE*

Build Your Own approach challenges



IREs* are built, secured and managed by YOU



Scanning of offline backups, which is ineffective against fileless attacks



Disconnected and manual experience, multiple tools and processes



Slow process to iterate and evaluate multiple snapshots or backups

vmware®



Provision a fully managed IRE* to prevent reinfection



Identify next-gen ransomware strains with embedded behavioral analysis

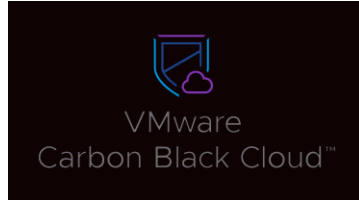


Streamline and automate recovery with a guided ransomware recovery workflow



Accelerate recovery with rapid, iterative evaluations of recovery points

Integrated by Design



vmware®

Cloud Disaster
Recovery™

VCDR Workflow & Product Walkthrough

The background is a solid dark blue color. It features several abstract geometric patterns and shapes in lighter shades of blue. These include concentric circles, a grid of small dots, wavy lines, and various solid and striped shapes. The overall aesthetic is modern and technical.

VMware Ransomware Recovery in Action

Configure adequate snapshot retention

Activate Isolated Recovery Environment

Guided restore point candidate selection

Restore from snapshot and scan workload

Evaluate using Behavioral Analysis

Final inspection and curated image build

Recover

Create protection group for site

General
Protection schedules

Protection schedules

Half-hourly

Take snapshots: Half-hourly, On :00 and :30, Keep snapshots for: 12 hours

Every 4 hours

Take snapshots: Every 4 hours, Starting at: 12 AM :00, Keep snapshots for: 2 days

Daily

Take snapshots: Daily, At: 12 AM :00, Keep snapshots for: 7 days

Weekly

Take snapshots: Weekly, On: Sun 12 AM :00, Keep snapshots for: 4 weeks

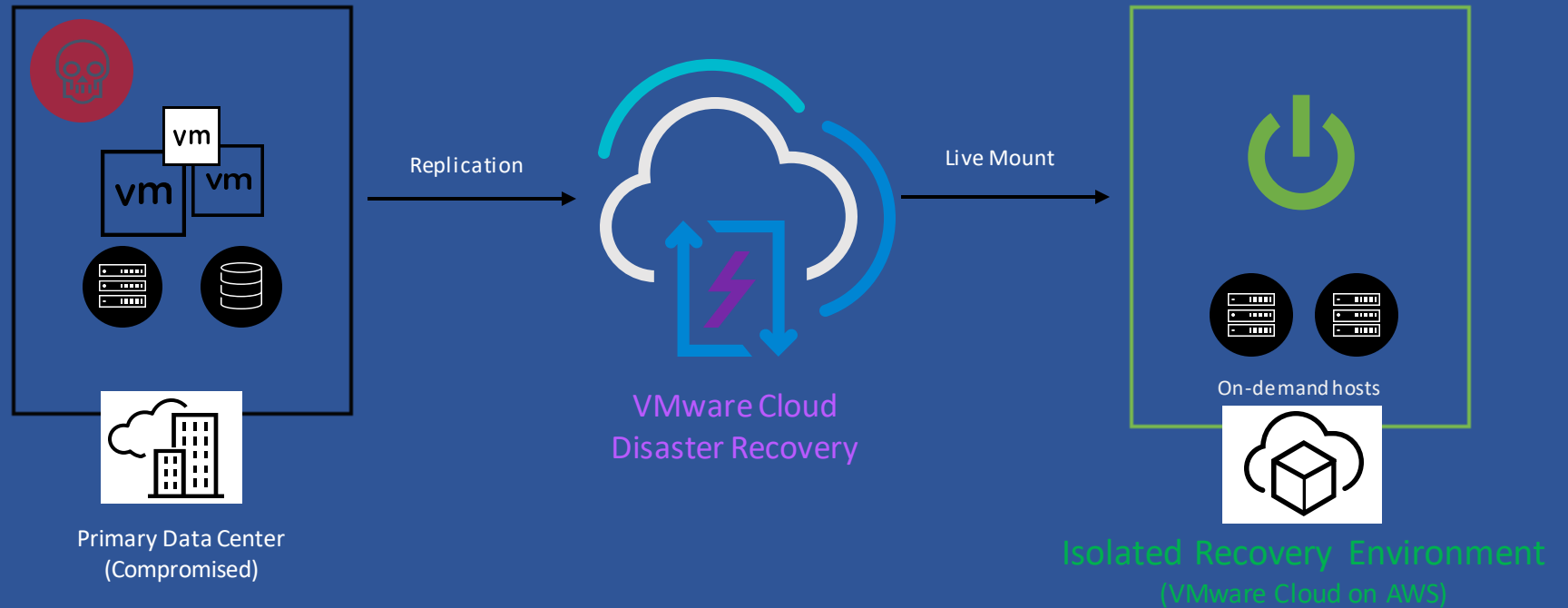
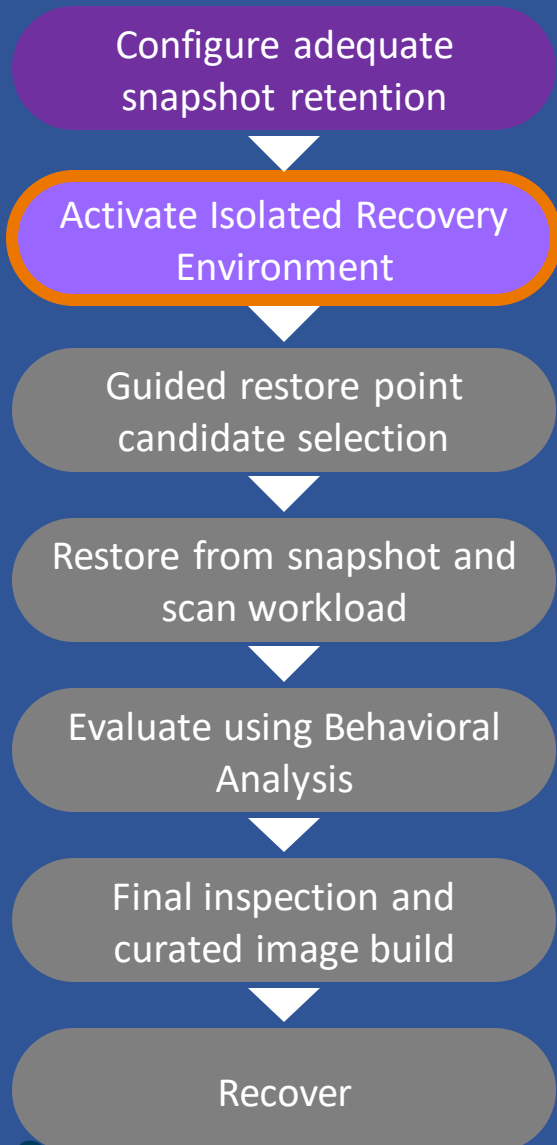
Monthly

Take snapshots: Monthly, On: 1st 12 AM :00, Keep snapshots for: 4 months

NEW SCHEDULE

CANCEL < BACK NEXT > FINISH

VMware Ransomware Recovery in Action



VMware Ransomware Recovery in Action

Configure adequate snapshot retention

Activate Isolated Recovery Environment

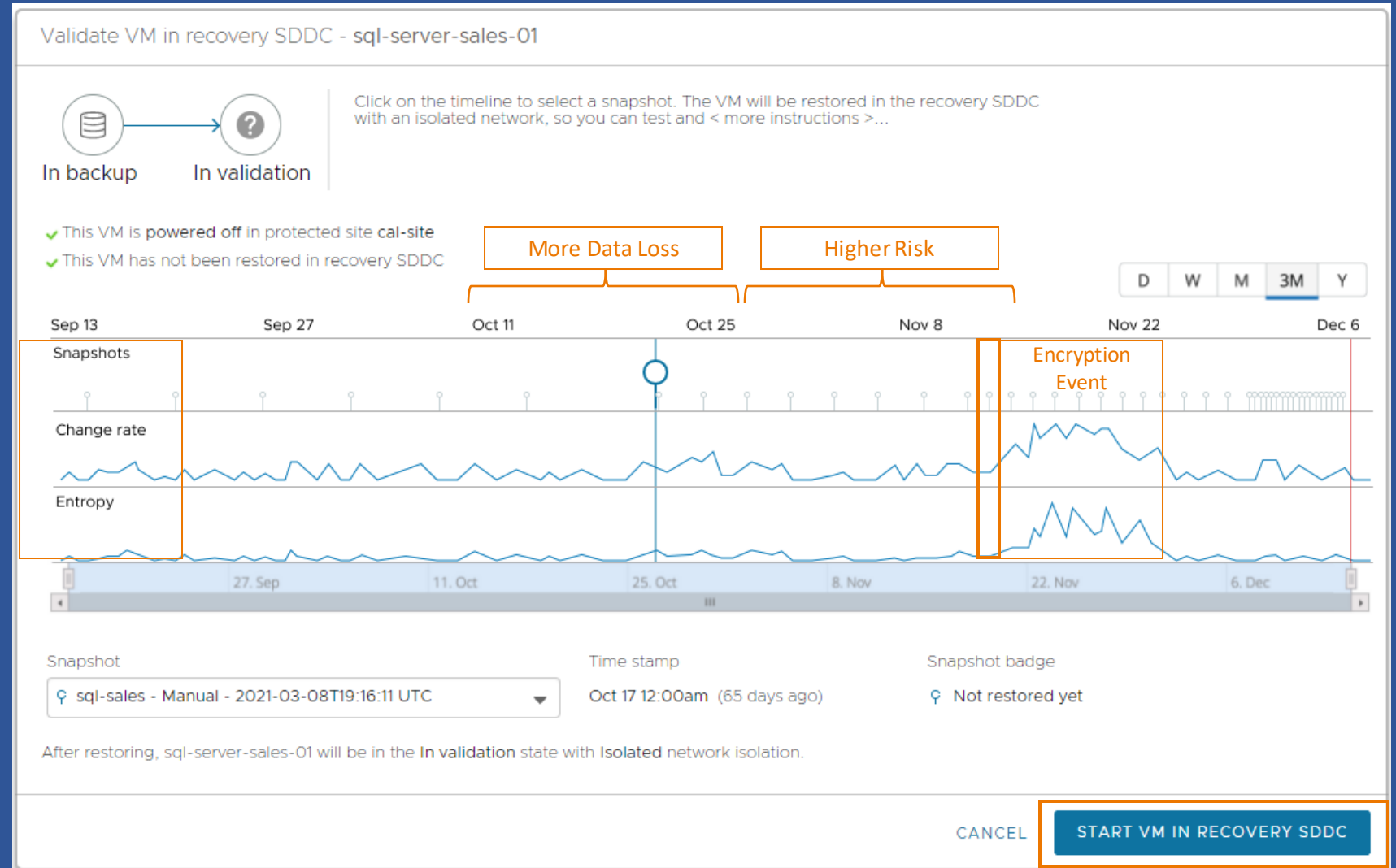
Guided restore point candidate selection

Restore from snapshot and scan workload

Evaluate using Behavioral Analysis

Final inspection and curated image build

Recover



VMware Ransomware Recovery in Action

Configure adequate snapshot retention

Activate Isolated Recovery Environment

Guided restore point candidate selection

Restore from snapshot and scan workload

Evaluate using Behavioral Analysis

Final inspection and curated image build

Recover

The screenshot displays the VMware Cloud Disaster Recovery interface for a plan named 'W2K16-APP1'. The left sidebar shows navigation options like 'Global console', 'Dashboard', 'Protected sites', and 'Recovery plans'. The main content area is divided into several sections:

- Workflow state:** A progress bar with four steps. The second step, 'In validation', is currently active and highlighted with a blue circle.
- Security and vulnerability analysis:** This section is highlighted with an orange border. It shows:
 - Vulnerability analysis: In progress
 - Malware signature scan: In progress - 0 file scanned - 0% done
 - Behavior analysis: Started Oct-27 03:56 pm (2m ago) - 8h recommended
- Risks:** Shows 'Threat severity' and 'Vulnerabilities' both as 'None' with green checkmarks.
- Protected site base snapshot:** Shows a badge 'Not badged', timestamp 'Oct-22 05:46 am (5d ago)', and name 'SERVERS - Half-hourly - 2022-10-22T12:45 UTC'.
- VM info:** Lists details such as 'Protection group: SERVERS', 'IP address: 192.168.100.118', and 'Operating system: Microsoft Windows Server 2016 or later (64-bit)'.
- Toolkit:** Includes options to 'OPEN VCENTER' and 'COPY IP ADDRESS'.

VMware Ransomware Recovery in Action

Configure adequate snapshot retention

Activate Isolated Recovery Environment

Guided restore point candidate selection

Restore from snapshot and scan workload

Evaluate using Behavioral Analysis

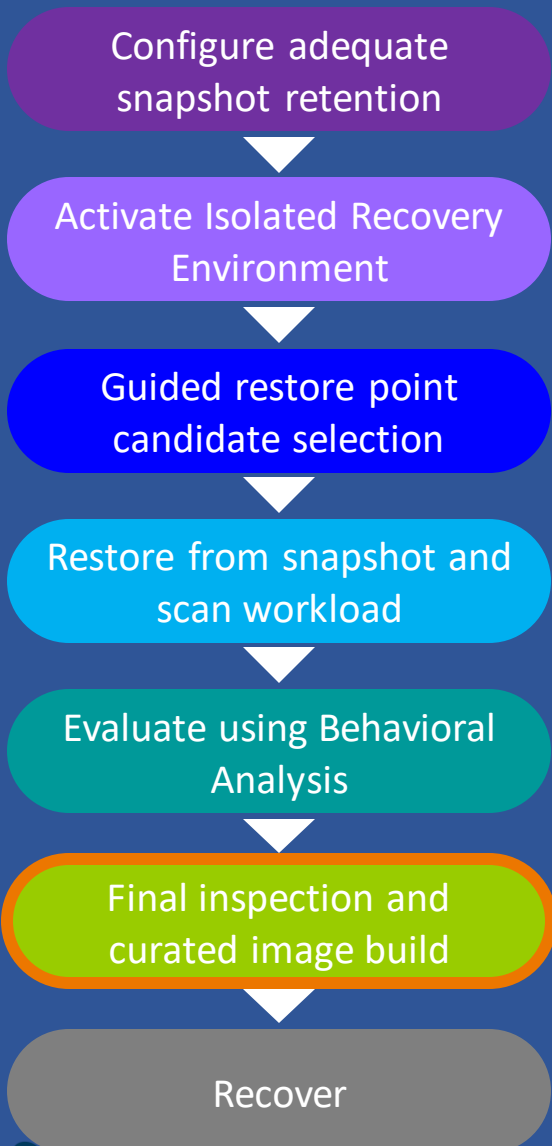
Final inspection and curated image build

Recover

The screenshot displays the VMware Cloud Disaster Recovery interface for device W2K16-APP1. The 'Analysis' tab is active, showing a summary of alerts and vulnerabilities. A red banner at the top indicates 'Highest threat alert severity is 5.' Below this, a table lists alerts with columns for 'First seen', 'Type', 'Severity', and 'Reason'. The most severe alert is highlighted, showing a 'Threat' with a severity of 5, detected on Oct-27 05:13 pm. A 'TOOLS' menu on the right offers options to 'Open in security console', 'Copy device ID', and 'Run vulnerability analysis'. A detailed view of the selected alert is shown at the bottom, confirming the threat level and the action taken: 'A Deny Policy Action was applied.'

First seen	Type	Severity	Reason
Oct-27 05:13 pm (1m ago)	Threat	5	A suspected virus was detected running. A Deny Policy Action was applied.
Oct-27 04:04 pm (1h ago)	Threat	4	A file (pe_lab_android.exe) with a reputation of known malware was found on disk.
Oct-27 04:05 pm (1h ago)	Threat	3	A known virus (Malware: Avira-Sig) was detected.
Oct-27 04:05 pm (1h ago)	Threat	3	A Known Malware was detected [x:\test\cbc-testing\pe_lab_w16.exe]
Oct-27 04:05 pm (1h ago)	Threat	3	A known virus (Malware: Avira-Sig) was detected.
Oct-27 04:05 pm (1h ago)	Threat	3	A Known Malware was detected [x:\test\cbc-testing\pe_lab_android.exe]
Oct-27 04:05 pm (1h ago)	Threat	3	A known virus (Trojan: TestFile) was detected.
Oct-27 04:05 pm (1h ago)	Threat	3	A Known Malware was detected [x:\test\cbc-testing\apc\apc-test-risk-level-6.exe]
Oct-27 04:05 pm (1h ago)	Threat	3	A known virus (Trojan: TestFile) was detected.
Oct-27 04:05 pm (1h ago)	Threat	3	A Known Malware was detected [x:\test\cbc-testing\apc\apc-test-risk-level-7.exe]

VMware Ransomware Recovery in Action



The screenshot displays the VMware Cloud Disaster Recovery console for VM W2K16-APP1. It features several key components:

- Change VM network isolation - W2K16-APP1**: A dialog box with radio buttons for network isolation rules:
 - Isolated: Fully isolated. No network access.
 - Quarantined + Analysis: Only access network and integrated analysis services. (Selected)
 - External outbound: Allow outbound access to the internet. Use to expose ransomware behavior.
 - Internal inbound: Allow inbound access from internal network.
 - Internal inbound + outbound: Allow inbound access from internal network and outbound access to the internet.
 - Open: Allow all network access.
- Power off and stage - W2K16-APP1**: A dialog box showing a progress bar from 'In validation' to 'Staged'. It includes a 'Protected site base snapshot' section with a 'Not badged' badge and a 'Staging snapshot' section with options to 'Take a new staging snapshot' or 'Discard changes in recovery SDDC and stage with the protected site base snapshot'. A 'POWER OFF AND STAGE' button is highlighted.
- Protected site base snapshot**: A summary card showing 'Not badged' badge, timestamp 'Oct-22 05:46 am (5d ago)', and name 'SERVERS - Half-hourly - 2022-10-22T12:45 UTC'. A 'SET BADGE' button is highlighted.
- VM info**: A card showing details like Protection group (SERVERS), IP address (192.168.100.118), Operating system (Microsoft Windows Server 2016 or later (64-bit)), VMware Tools (11365), Protected site folder (vSAN-DC/vm/PROD), and Recovery SDDC folder (SDDC-Datacenter/vm/DR Site/PROD). A 'Tag' button is highlighted.
- End validating iteration**: A card with buttons for 'TRY DIFFERENT SNAPSHOT', 'POWER OFF AND STAGE', and 'OTHER'.

• Push Button Isolation control

• Stage recovery point with changes

VMware Ransomware Recovery in Action

Configure adequate snapshot retention

Activate Isolated Recovery Environment

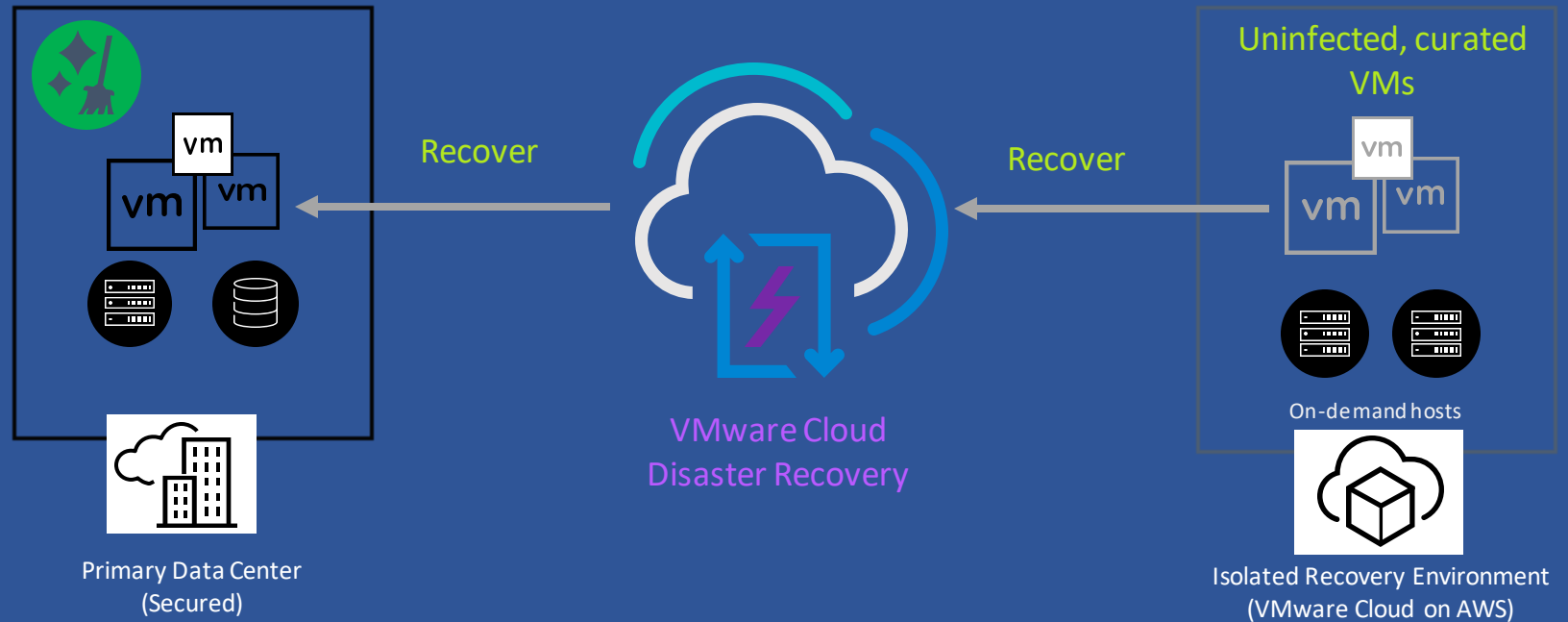
Guided restore point candidate selection

Restore from snapshot and scan workload

Evaluate using Behavioral Analysis

Final inspection and curated image build

Recover



Key Take-aways

- Ransomware threat continues to evolve
- Traditional HA/DR/Back-up is not sufficient
- DIY isn't a small undertaking
- VCDR provides DRaaS with Ransomware Recovery and cloud scale and economics



Call to Action

vmware®

 **SUMMIT**
TECHNOLOGY GROUP



Ransomware Recovery Maturity

Ransomware Recovery Maturity assessment is a comprehensive evaluation of an organization's ability to recover from a ransomware attack using the capabilities provided by VMware Cloud Disaster Recovery and VMware Ransomware Recovery. The assessment would analyze the organization's current disaster recovery and backup procedures to identify potential vulnerabilities and recommend improvements to strengthen their resilience against ransomware attacks. The assessment would also evaluate the organization's readiness to quickly failover to a cloud-based recovery environment, validate backups, and perform at-scale recoveries. The goal of the assessment is to ensure that the organization has a robust and effective ransomware recovery plan in place to minimize the impact of an attack and ensure business continuity.

If you take a few minutes to assess these capabilities you will get an instant performance dashboard and will be able to request an executive report.

[Begin Assessment](#)

[The Summit Technology Group Privacy Policy](#)

<https://tinyurl.com/rw-assessment>

- Take the free Ransomware Recovery Maturity assessment!
- Engage with Summit to do a deeper dive.
 - <https://www.thesummitgrp.com/contact-us.html>
- Prepare!

THANK YOU



SUMMIT
TECHNOLOGY GROUP