CXS2308BCN

vmware® EXPLORE

Disaster Recovery in the Ransomware Era

Andrea Siviero

Principal Architect, VCDX #240

#vmwareexplore #CXS2308BCN

Required Disclaimer

- This presentation may contain product features or functionality that are currently under development.
- This overview of new technology represents no commitment from VMware to deliver these features in any generally available product.
- Features are subject to change, and must not be included in contracts, purchase orders, or sales agreements of any kind.
- Technical feasibility and market demand will affect final delivery.
- Pricing and packaging for any new features/functionality/technology discussed or presented, have not been determined.

OVER

4000

ATTACKS EVERY DAY [1]

EVERY

11 seconds

A NEW ORG FALLS VICTIM [2]

DAMAGE [3]

2021	$20B
2019	$11.5B
2018	$8B

FULL FUNDED
ADVERSARY SYNDICATES

Ransomware

AS-A-SERVICE

[1] Justice.gov [2] Cybersecurity Ventures (Oct, 2019) [3] Cybersecurity Ventures (Oct. 2019)

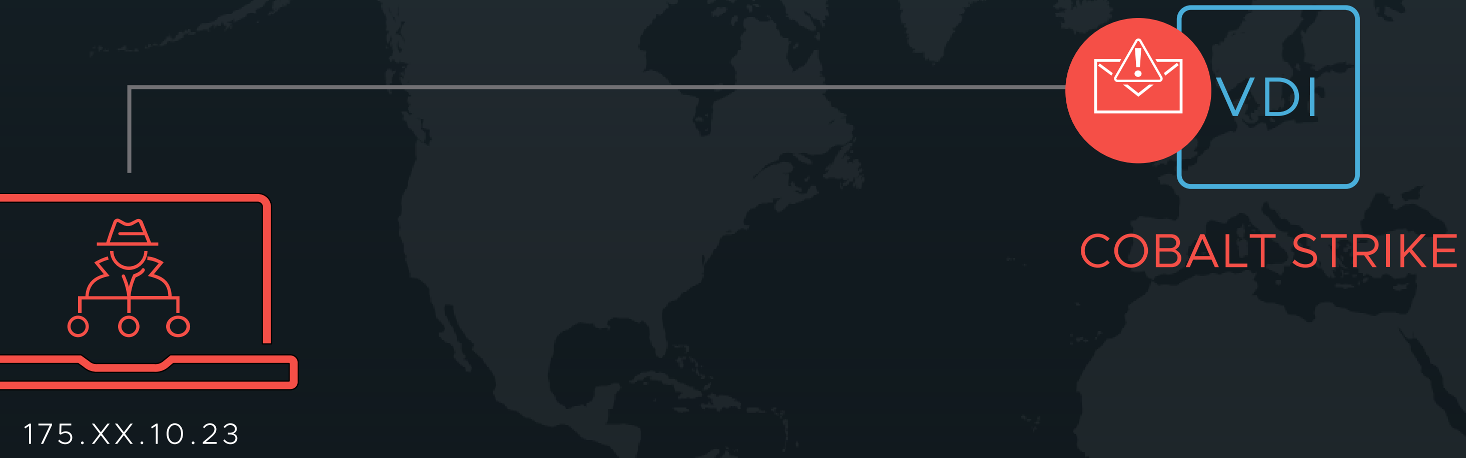
ATTACK SEQUENCE

- INITIAL ACCESS/ESTABLISH PERSISTENCE
- COMMAND AND CONTROL

INITIAL ACCESS

COMMAND AND CONTROL

6:30 PM



10.2.1.34

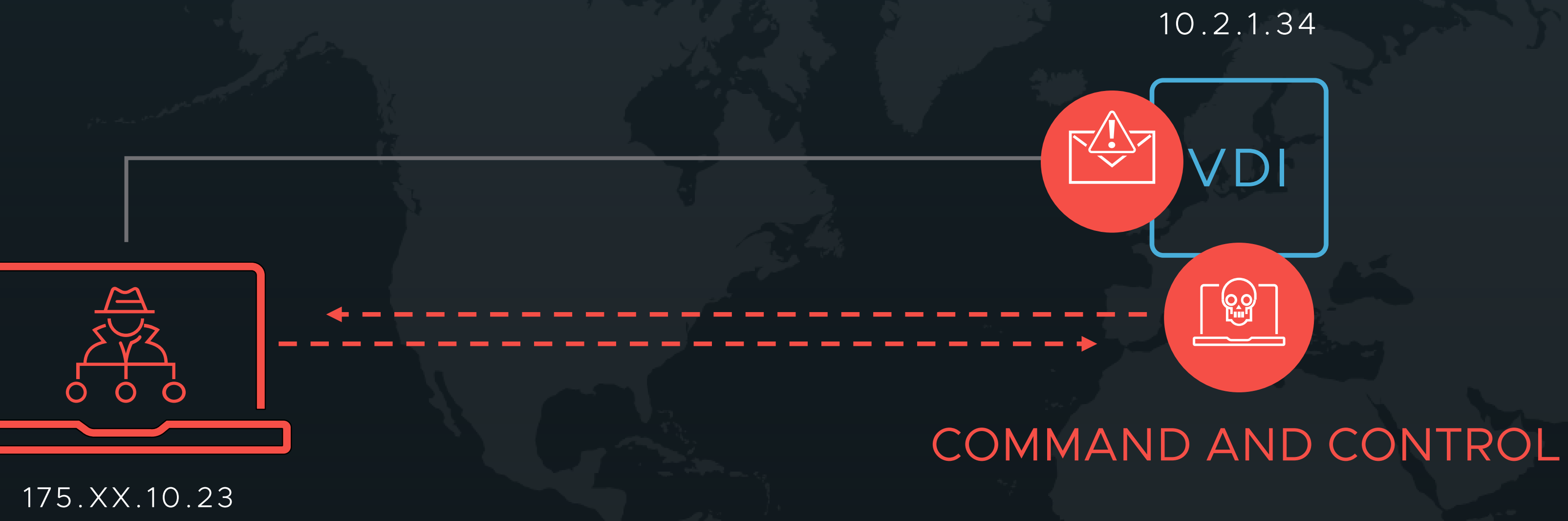
VDI

COBALT STRIKE

175.XX.10.23

- INITIAL ACCESS
- COMMAND AND CONTROL

6:36 PM



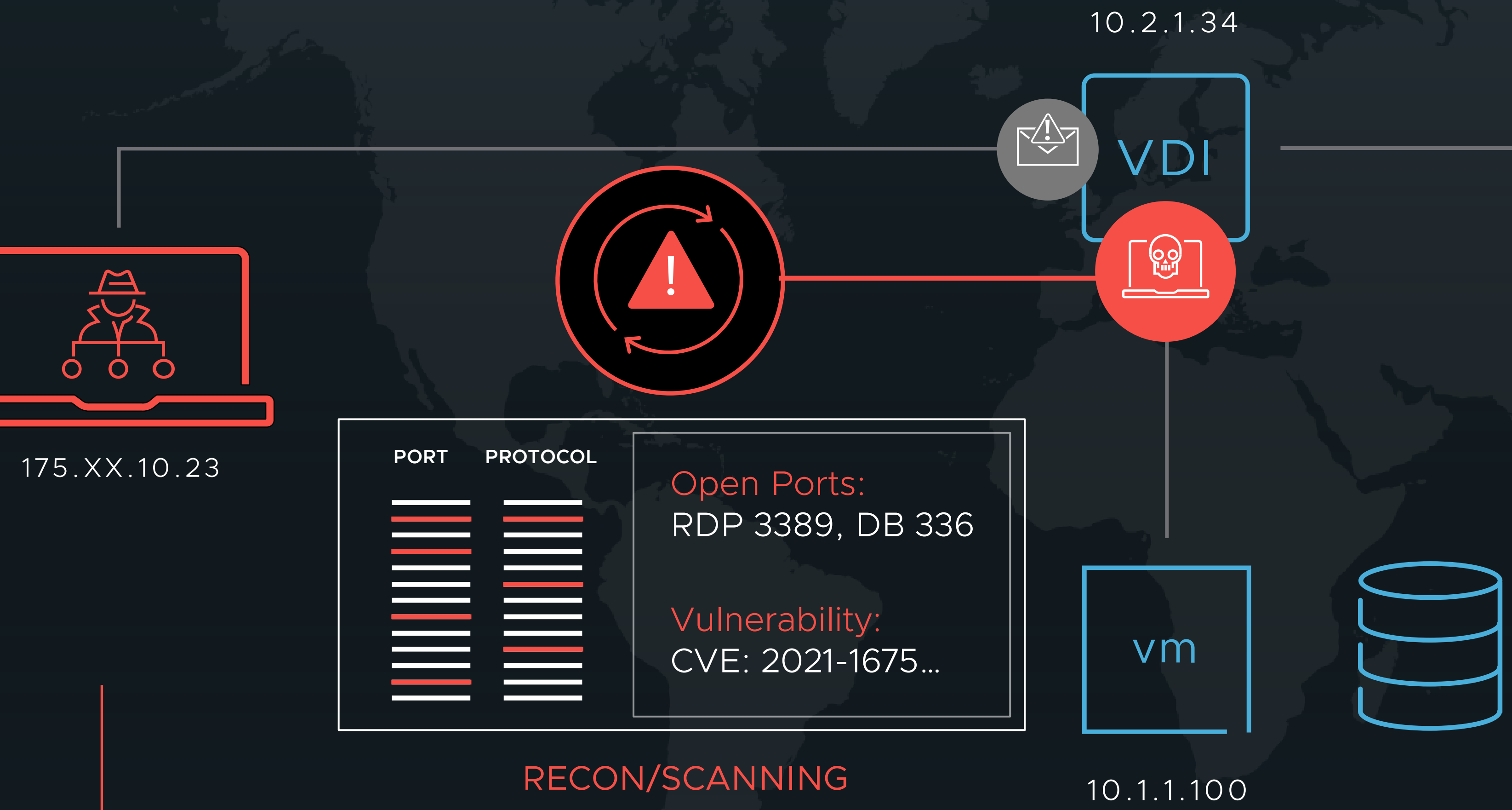
ATTACK SEQUENCE

- INITIAL ACCESS → ESTABLISH PERSISTENCE
- COMMAND AND CONTROL
- **LATERAL MOVEMENT**

vmware®

RECON

9:12 PM



Open Ports:
RDP 3389, DB 336

Vulnerability:
CVE: 2021-1675...

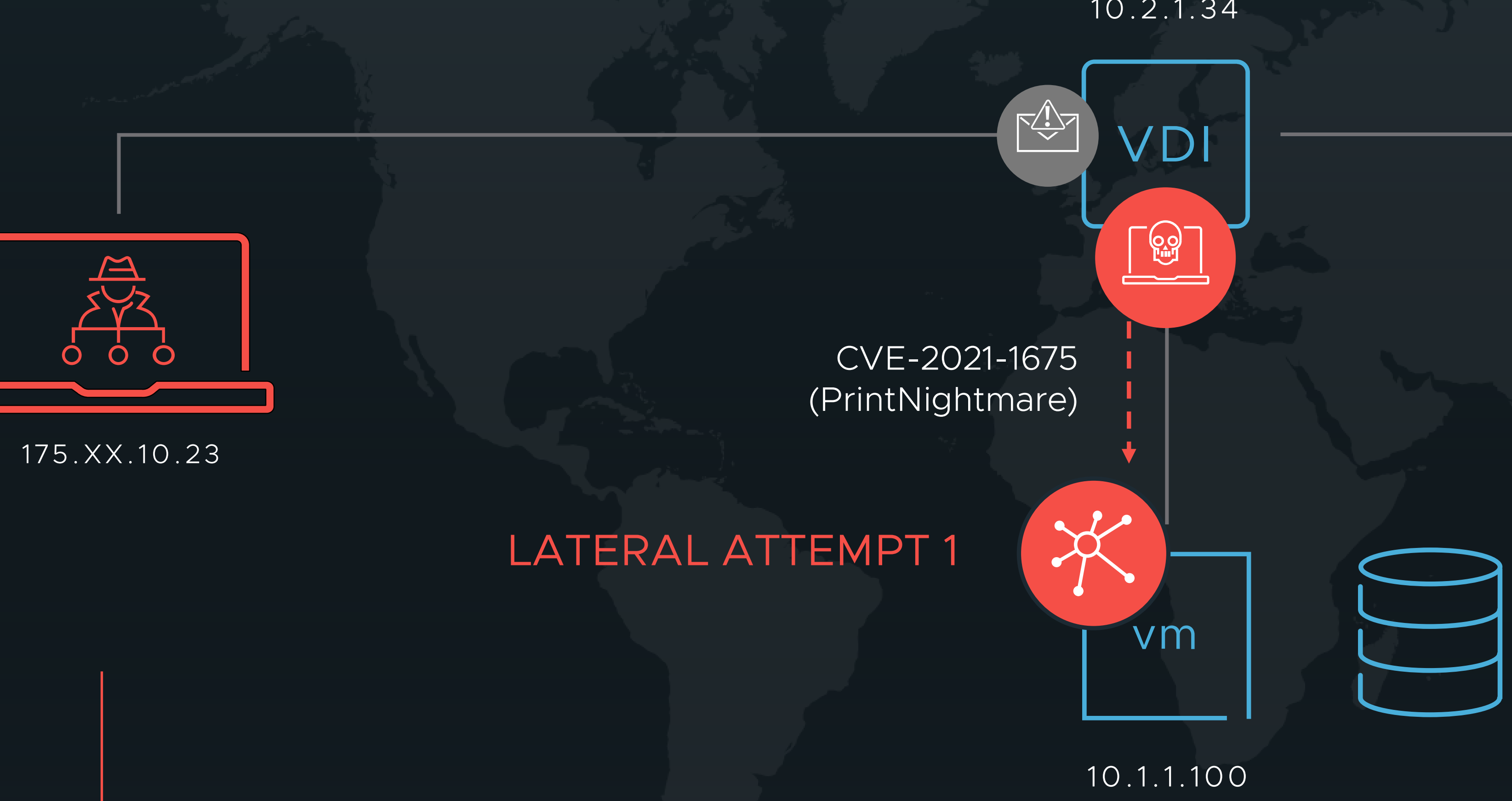
RECON/SCANNING

INITIAL ACCESS

COMMAND AND CONTROL

LATERAL MOVEMENT

9:12 PM



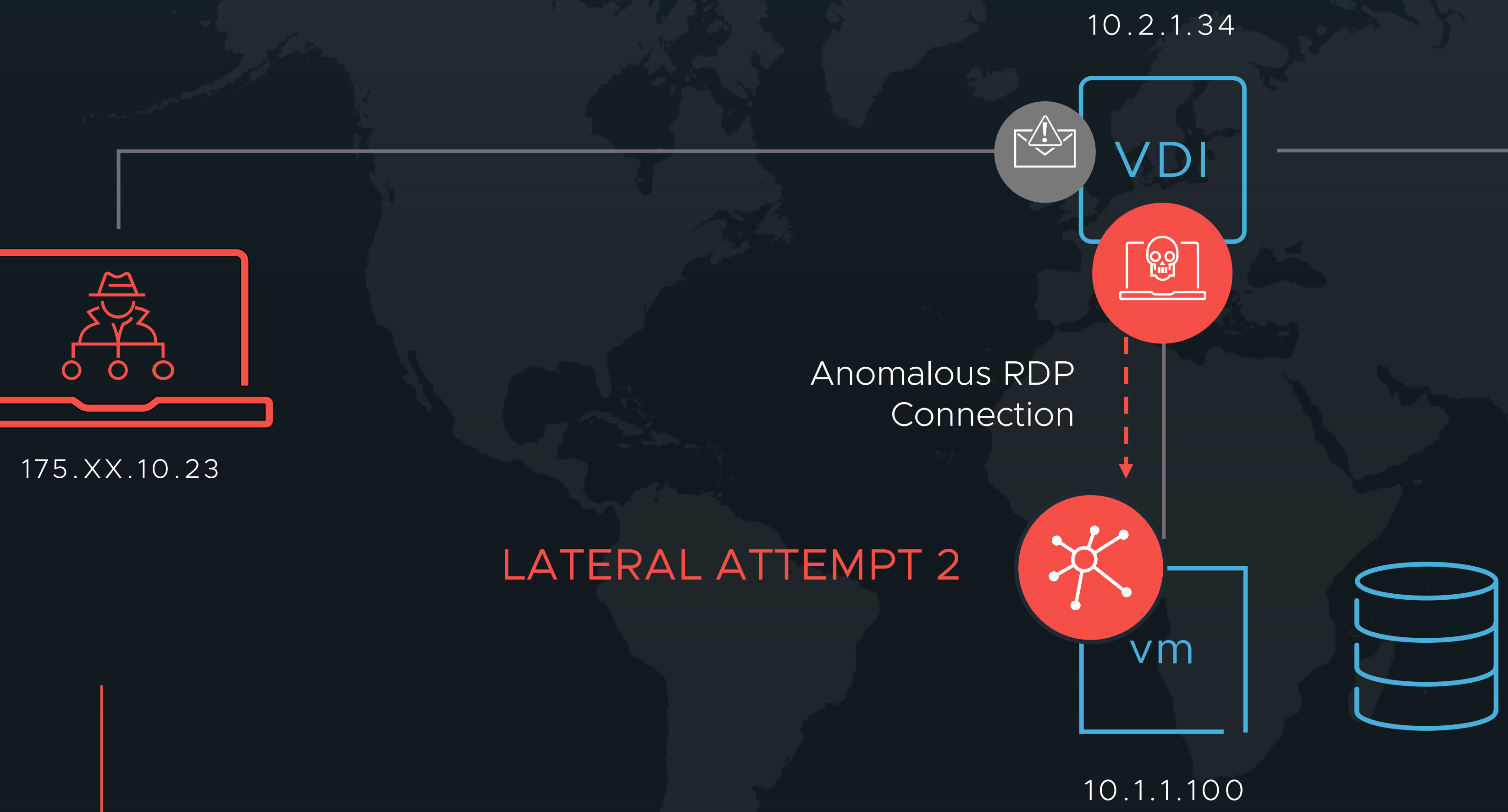
vmware®

INITIAL ACCESS

COMMAND AND CONTROL

LATERAL MOVEMENT

10:45 PM



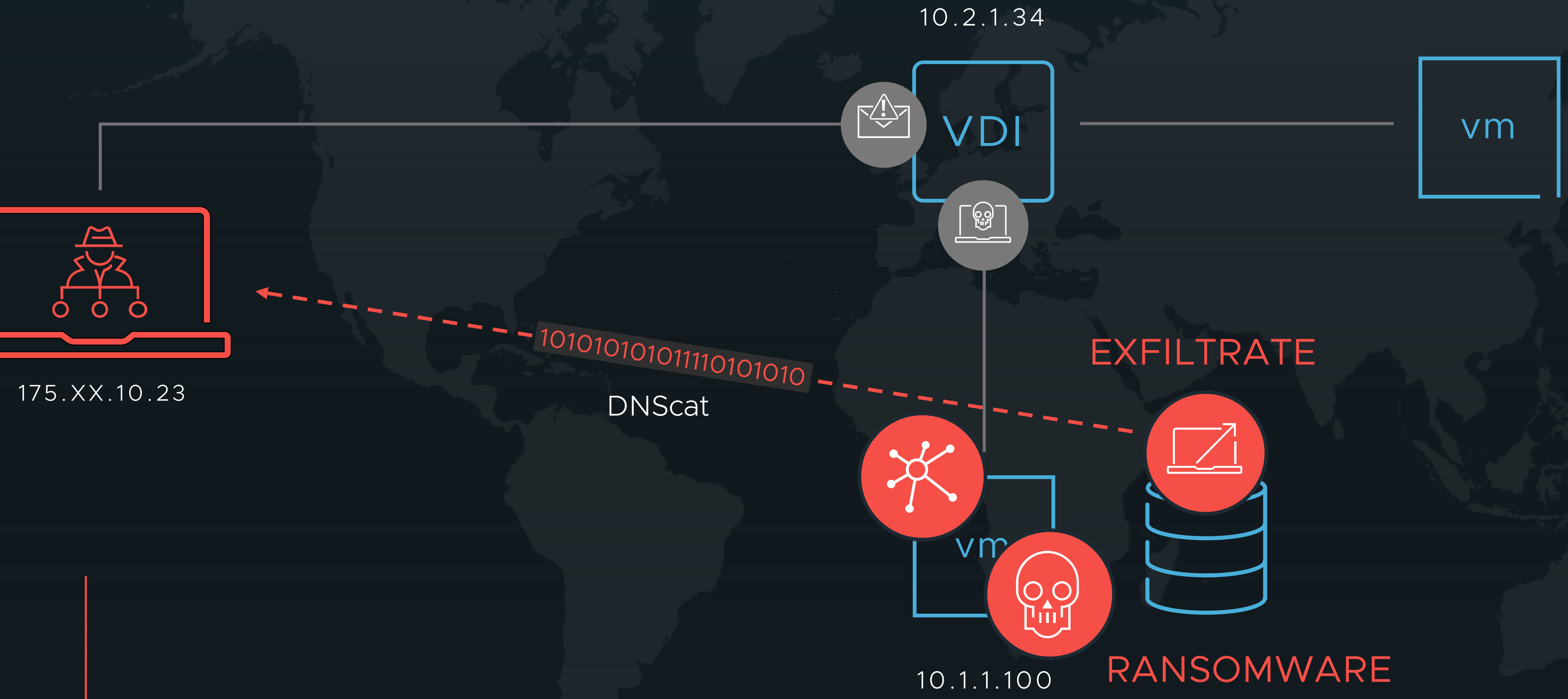
vmware®

ATTACK SEQUENCE

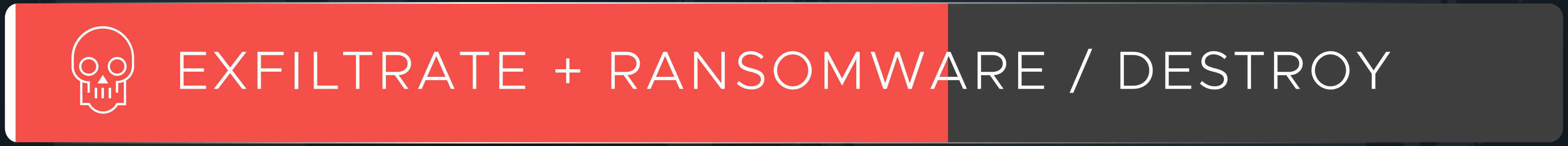
- INITIAL ACCESS/ESTABLISH PERSISTENCE
- COMMAND AND CONTROL
- LATERAL MOVEMENT
- EXFILTRATE + RANSOMWARE / DESTROY

- INITIAL ACCESS
- COMMAND AND CONTROL
- LATERAL MOVEMENT
- EXFILTRATE / RANSOMWARE / DESTROY

12:02 AM
Feb 14th



vmware®



EXFILTRATE + RANSOMWARE / DESTROY

59%

DOUBLE EXTORTION

Source: IBM X-Force Threat Intelligence Index 2021

vmware®

Challenges Implementing a Holistic Solution

Ransomware risk mitigation

Lack of a ransomware avoidance strategy

Lack of integration between DR and ransomware detection solutions

Weak implementation of network and endpoint security policies

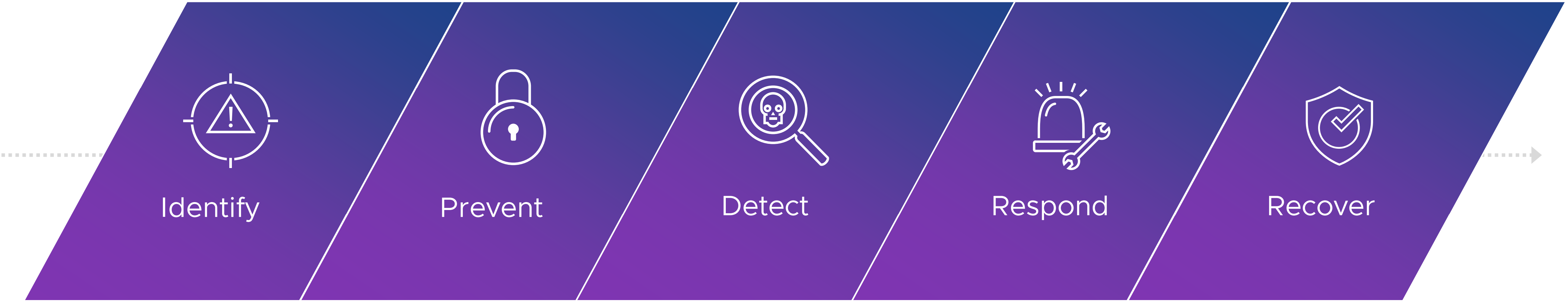
Poor visibility into application complexities and dependencies

Insufficient staff and time

Lack of security awareness and containment experience and skills

The Ransomware Protection Cycle

VMware ransomware solutions



Manage risk across systems, people, assets, data and capabilities

Limit or contain the impact of an attack

Define activities to identify the occurrence of an attack

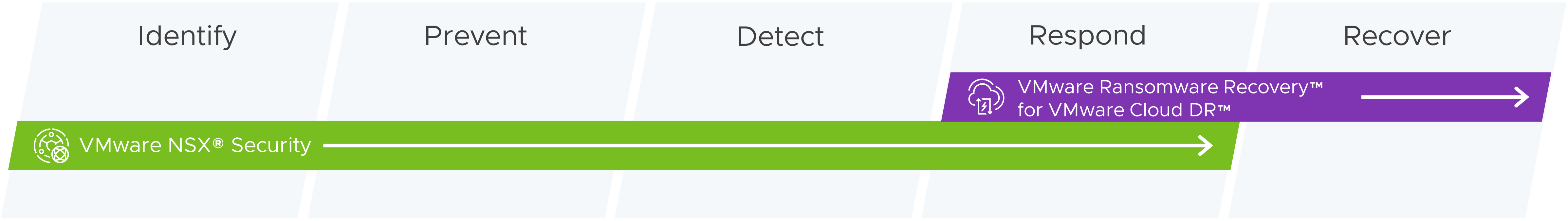
Contain the impact of a potential attack

Restore normal operations to reduce the impact of an attack

Source: NIST

Full Coverage of the Ransomware Protection Cycle

VMware ransomware solutions



Identify

- 🟩 Baseline Network Environment
- 🟩 High Value Assets Tagging
- 🟩 Flow Visualization
- 🟪 DR Plan Config, Test, Check
- 🟪 Application Dependency Mapping

Prevent

- 🟩 Network Segmentations
- 🟩 IDS/IPS/Deep Packet Inspection
- 🟩 Attack Surface Reduction
- 🟩 Micro-segmentation
- 🟩 Malware Prevention

Detect

- 🟩 Signature-based & behavior-based detection (Network)
- 🟩 Signal Correlation Across Detectors
- 🟩 Sandbox/Malware Detection
- 🟩 Network Anomaly

Respond

- 🟩 Network Quarantine
- 🟩 Network Resets
- 🟩 Allow/Deny
- 🟪 Failover to Isolated Recovery Environment
- 🟪 Identify Restore Point candidates

Recover

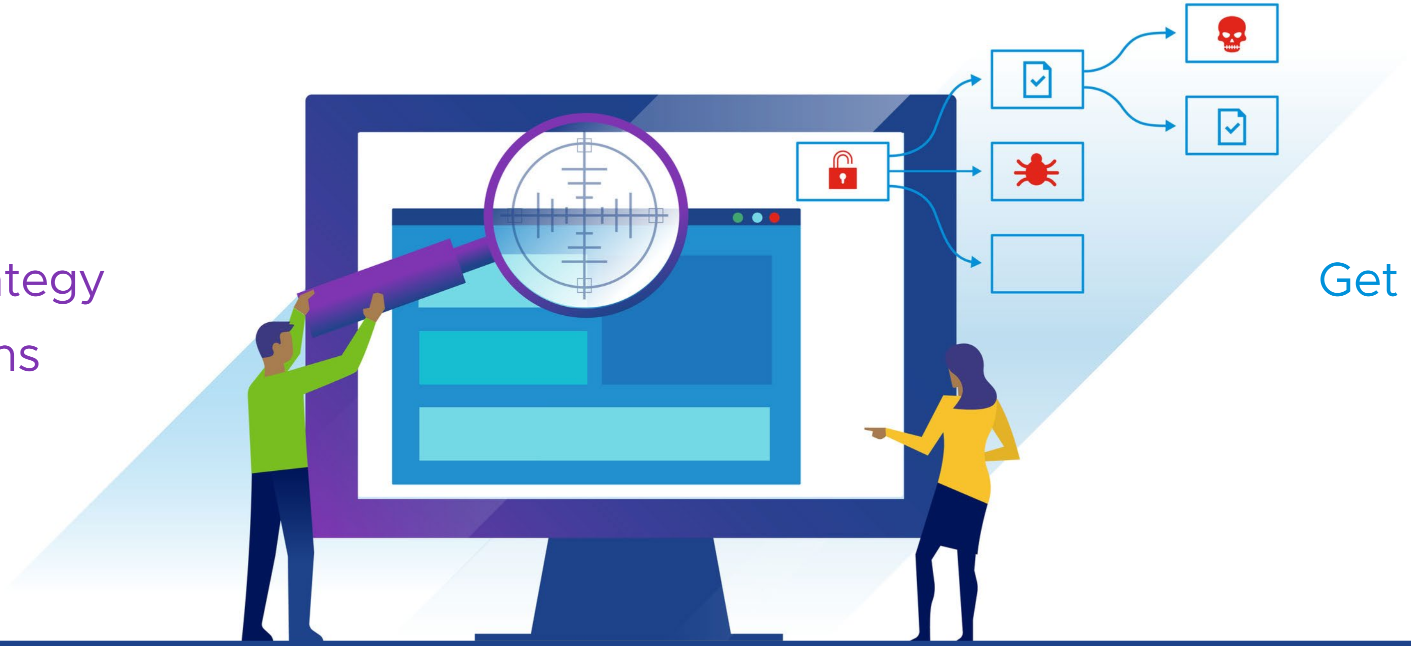
- 🟪 Validation of recovery points
- 🟪 File and folder-level recovery
- 🟪 Delta-based Failback
- 🟪 Review, Audit & Remediate

🟩 NSX Security　🟪 VMware Cloud DR

Ransomware Risk Mitigation Implementation Methodology

An end-to-end holistic approach

Define the strategy and integrations



Get started operating the environment

Implement and integrate the solutions

Endpoint Protection

Network Protection

Data Protection

Define the Strategy and Integrations

Define the Strategy and Integrations

Leverage an agile approach for a faster path to security

Optimize your security posture with an **assessment and strategy roadmap**

Secure your endpoints and workloads

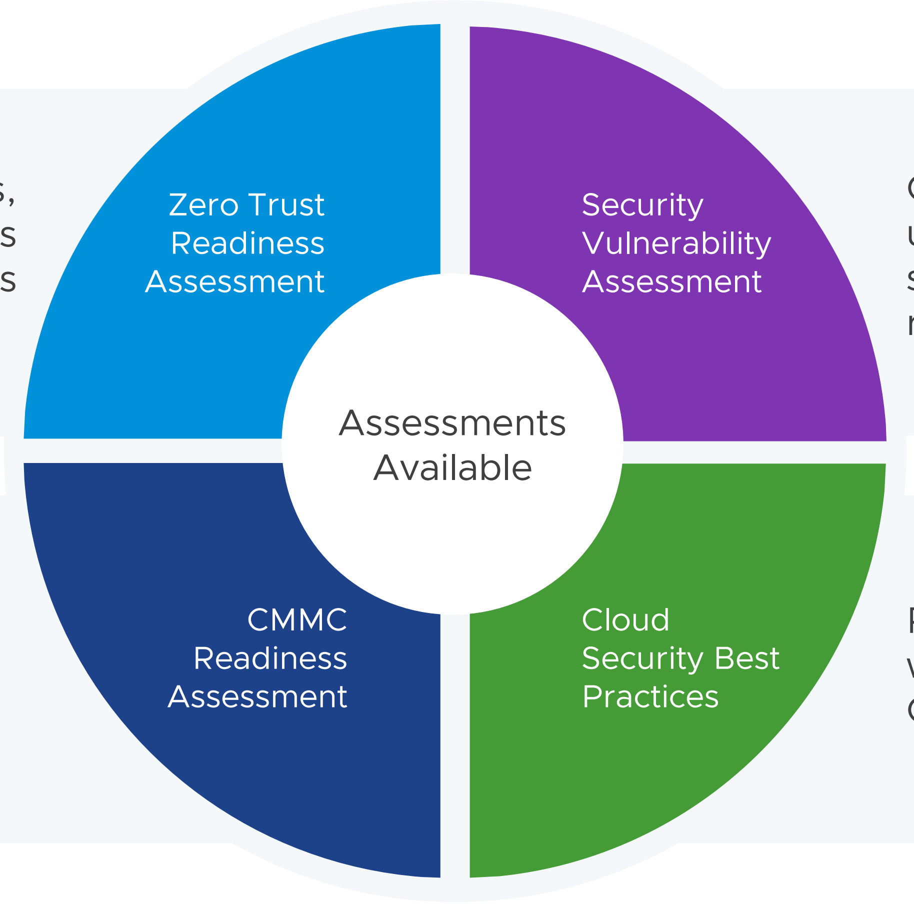
Reduce the number of vulnerable attack surfaces with **network protection**

Safeguard your business and customer information with **data protection**

Get the support you need to mitigate ransomware risk with four flexible integration options that work in any combination

Assess the Security Posture to Identify Vulnerabilities

A crucial step to implement the most appropriate countermeasures



Assessments Available

Zero Trust Readiness Assessment

Assess people, processes, and VMware technologies based on NIST standards

Security Vulnerability Assessment

Gain a deep understanding of security posture to remediate as needed

CMMC Readiness Assessment

Gain insights on requirements for all Department of Defense suppliers

Cloud Security Best Practices

Reduce risks within VMware Cloud architecture

Integrate Security Strategy for Endpoints

Requirements, assumptions, constraints, and risks

- Data flows and communications
- Permission, blocking, and isolation rules
- Policies and notifications
- Response procedures
- Exceptions list

Integrate Security Strategy for Networks

Requirements, assumptions, constraints, and risks

Allowed and blocked communications flows

Level of protection to pursue

Integration with external identity manager

Logging integration

Exceptions list

Implement Data Protection

Disaster Recovery: Proper Preparation Prevents Poor Performance

Protect your datacenter to the cloud with VMware Cloud Disaster Recovery

Plan

Map applications

Select SLAs

Organize Site(s)

Define

Build site(s)

Define policies

Begin data copy

Configure

Deploy cloud site

Align sites

Define DR plans

Test

Test failovers

Measure results

Adjust plans

Operate

Review runbooks

Monitor sites

Report & Audit

Discover VMs and dependency mapping

Discover

Virtual workloads
Applications
Infrastructure

Analyze

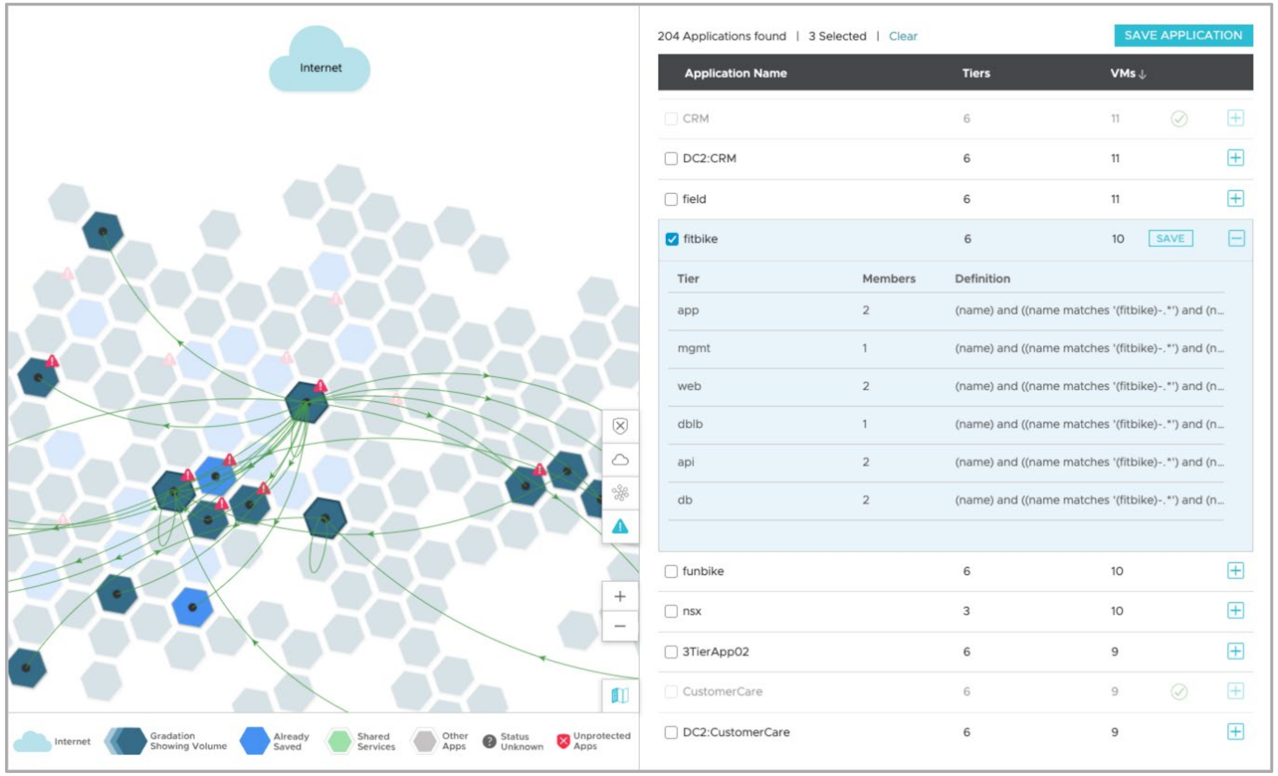
Packet flows
Compliance requirements
Security requirements

Map

Application dependencies

Define

Protection groups
Replication timing and snapshot frequency



204 Applications found | 3 Selected | Clear

SAVE APPLICATION

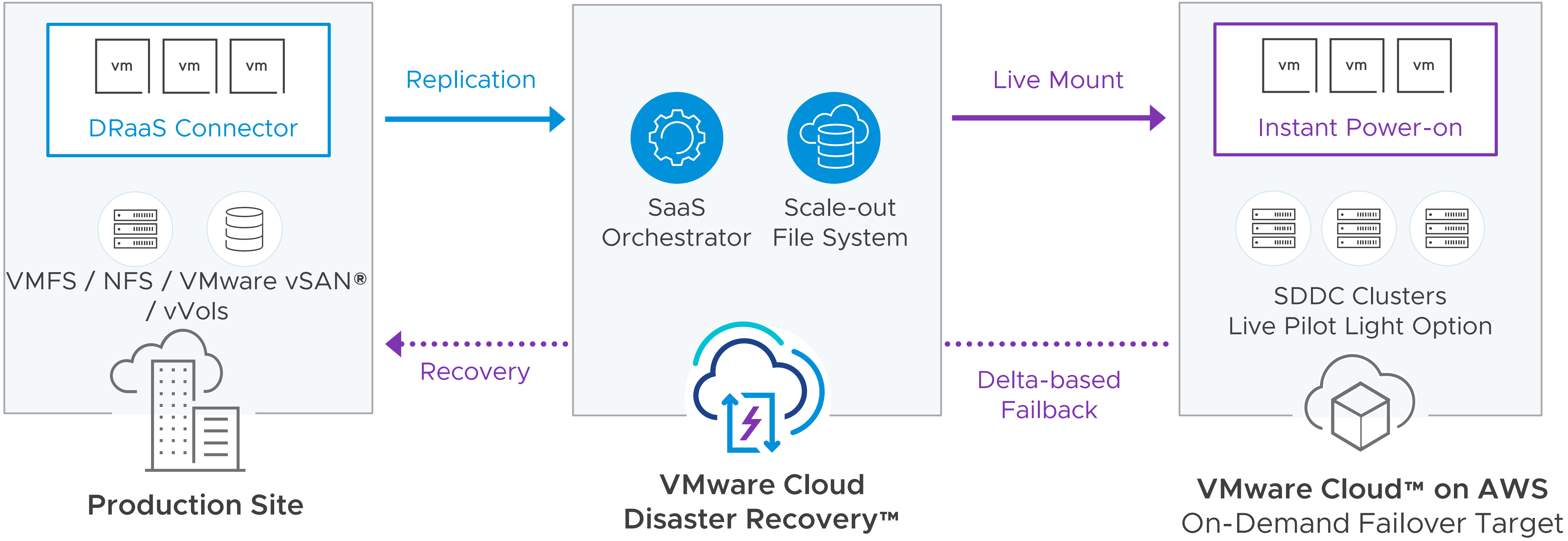
Application Name	Tiers	VMs ↓		
□ CRM	6	11	✓	+
□ DC2:CRM	6	11		+
□ field	6	11		+
☑ fitbike	6	10	SAVE	−

Tier	Members	Definition
app	2	(name) and ((name matches '(fitbike)-.*') and (n...
mgmt	1	(name) and ((name matches '(fitbike)-.*') and (n...
web	2	(name) and ((name matches '(fitbike)-.*') and (n...
dblb	1	(name) and ((name matches '(fitbike)-.*') and (n...
api	2	(name) and ((name matches '(fitbike)-.*') and (n...
db	2	(name) and ((name matches '(fitbike)-.*') and (n...

Application Name	Tiers	VMs ↓		
□ funbike	6	10		+
□ nsx	3	10		+
□ 3TierApp02	6	9		+
□ CustomerCare	6	9	✓	+
□ DC2:CustomerCare	6	9		+

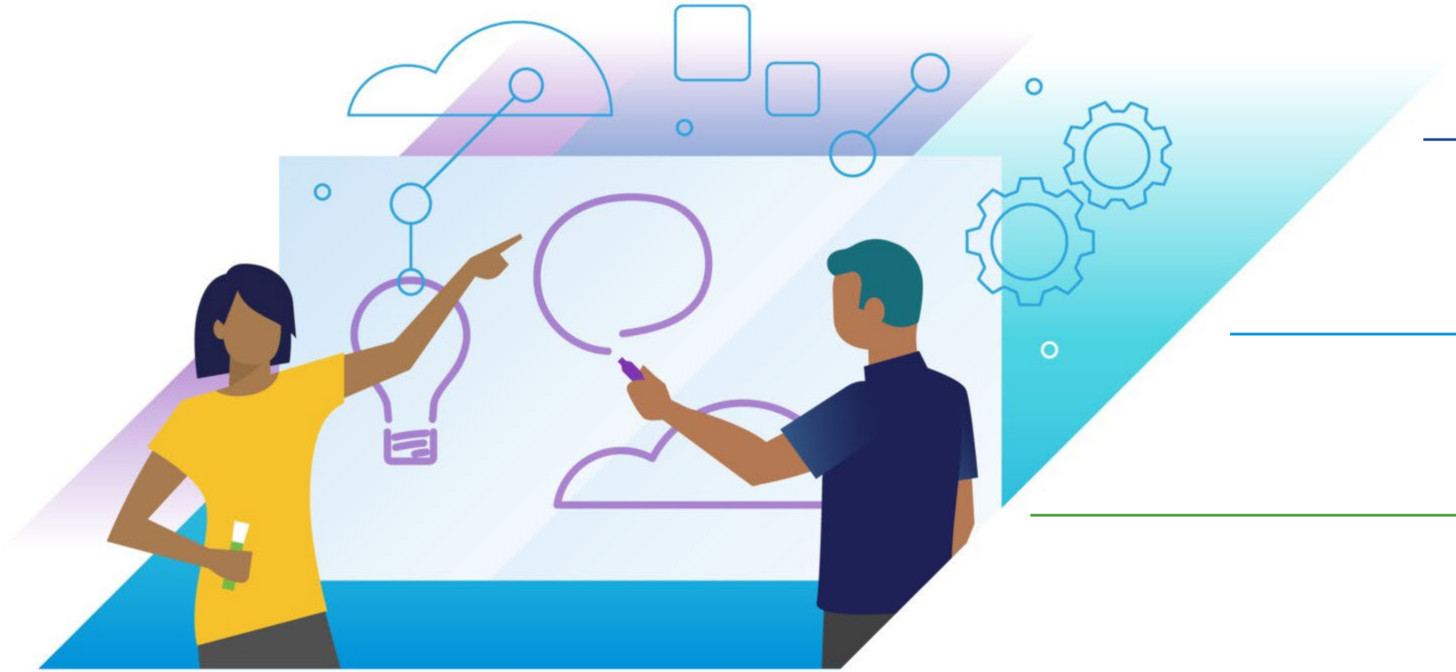
VMware Cloud Disaster Recovery

On-demand disaster recovery, delivered as an easy-to-use SaaS solution, with cloud economics



Blue: Steady-state operations | **Purple:** Activated for tests, failovers, failbacks

Create a Detailed Disaster Recovery Plan



Define scope of DR plan(s)

Design and configure the target DR site

Define recovery steps and sequence

Define custom scripts

Integrate details into broader DR plan

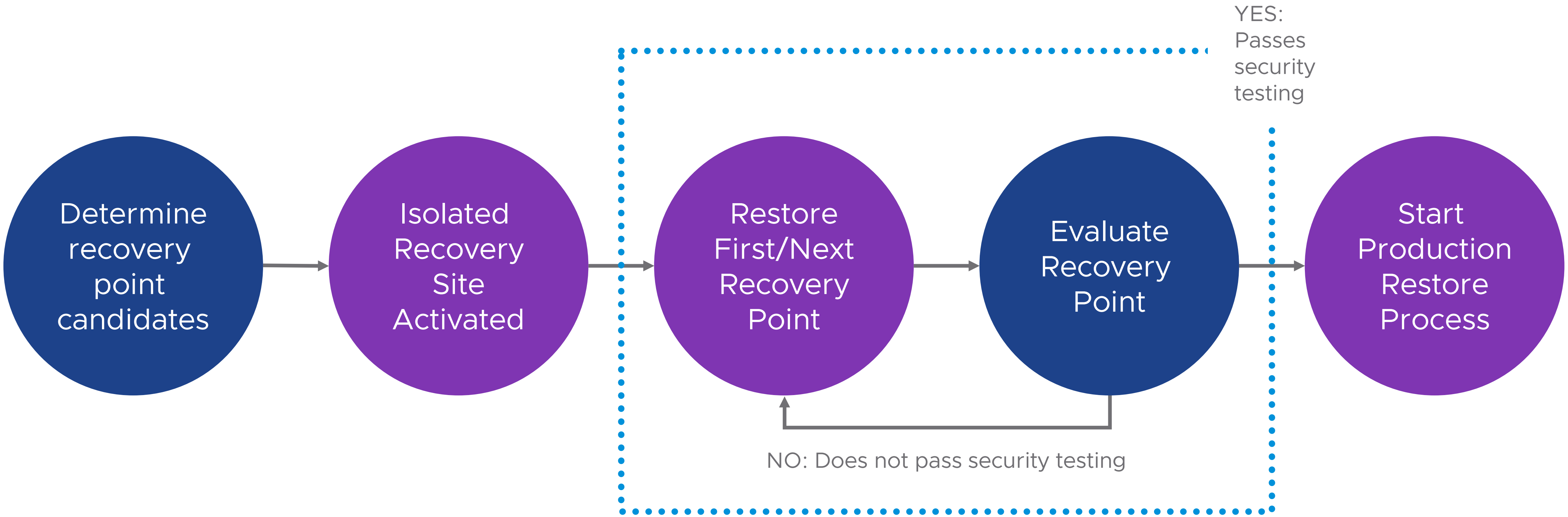
Integrate Security Strategy

- Threat scan frequency
- Image snapshot frequency and retention
- RPOs
- RTOs

Ensure threat detection and disaster recovery works together

VMware Cloud DR: Identifying a Clean Recovery Point

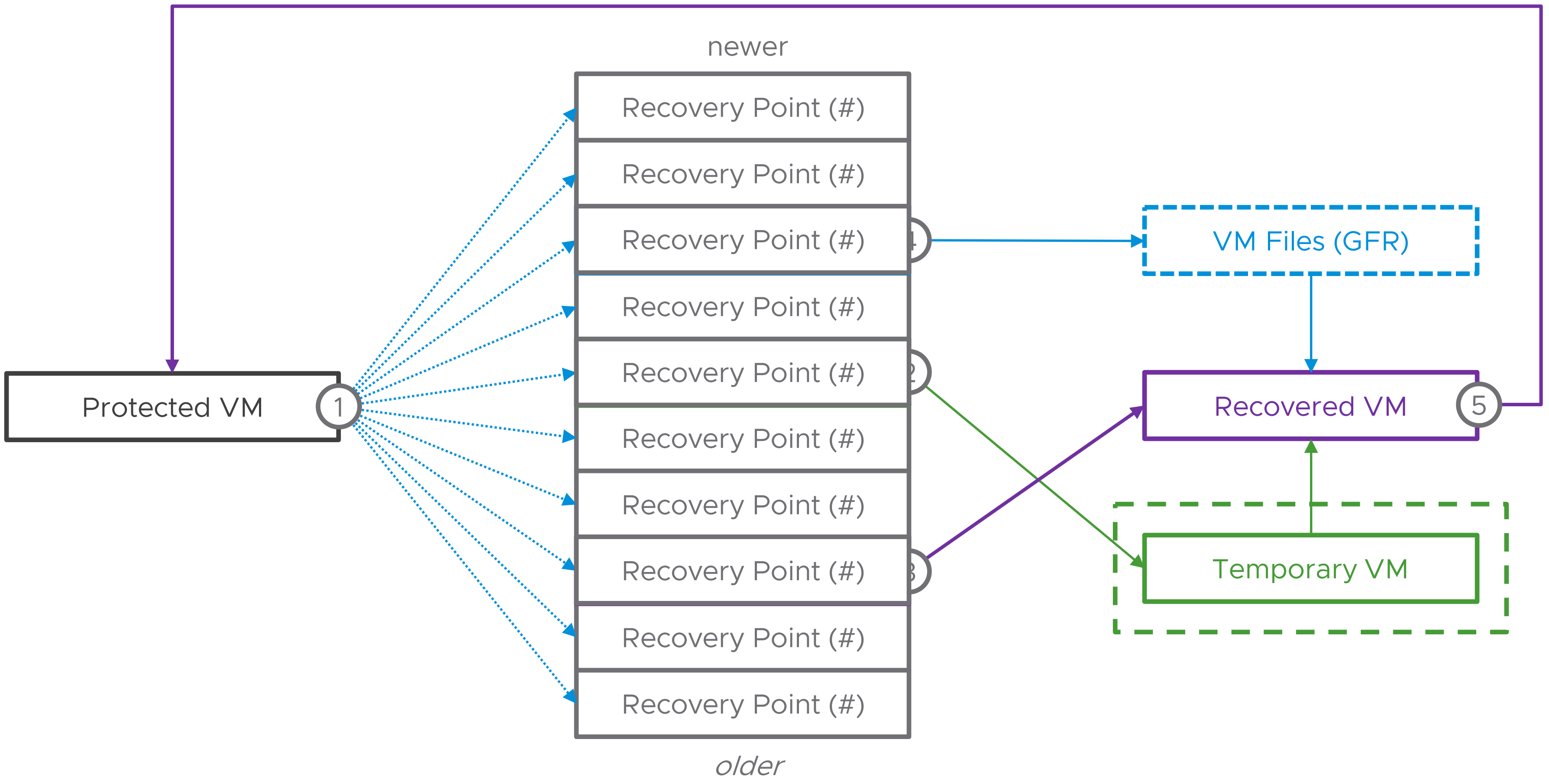
An iterative process that must be done as quickly as possible


YES: Passes security testing
Determine recovery point candidates
Isolated Recovery Site Activated
Restore First/Next Recovery Point
Evaluate Recovery Point
Start Production Restore Process
NO: Does not pass security testing

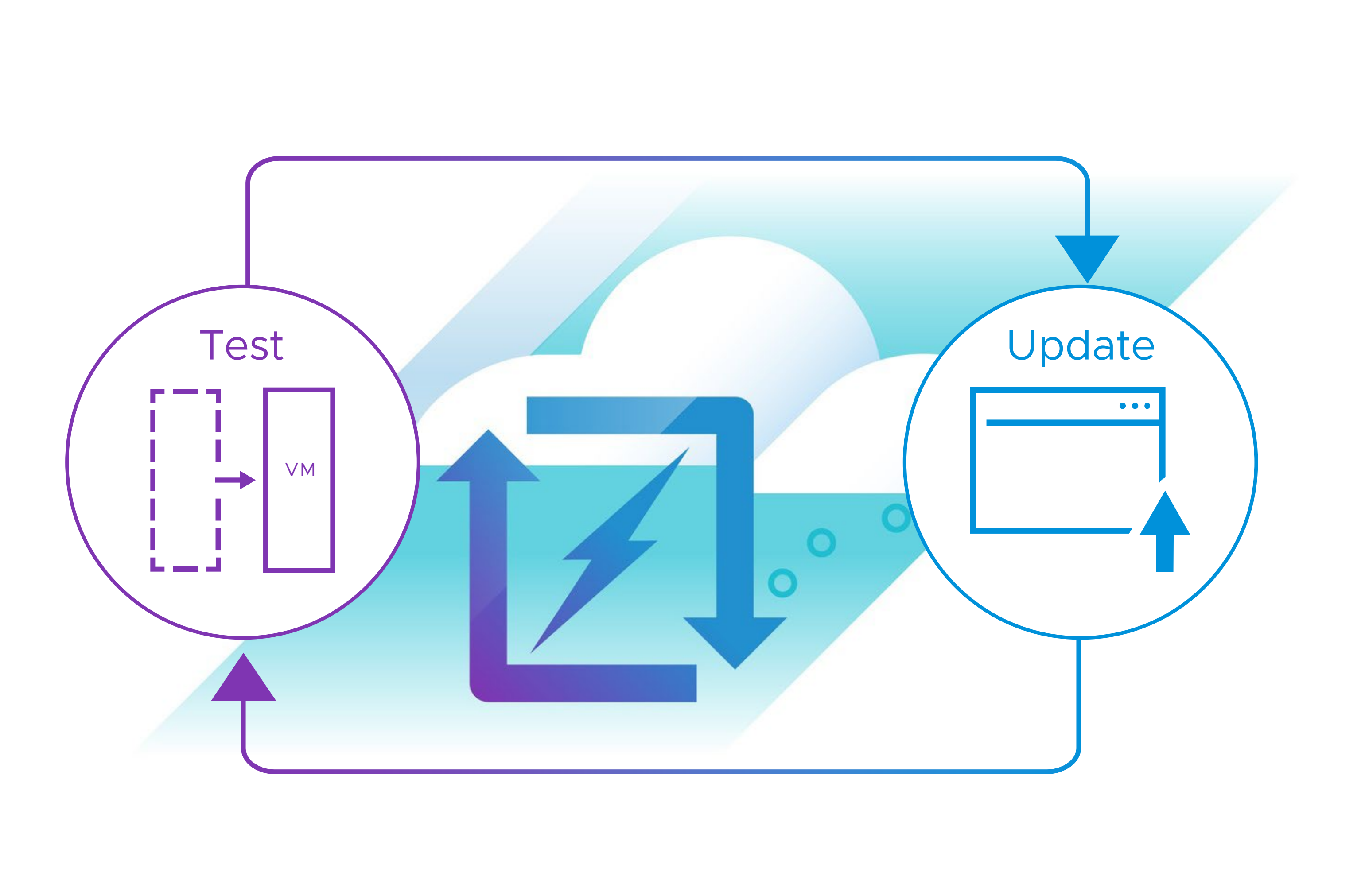
CRITICAL: Must **rapidly** do this iterative process

Merged VM Recovery Process

Combining more than one recovery point into the recovered VM



Test and Validate Scenarios

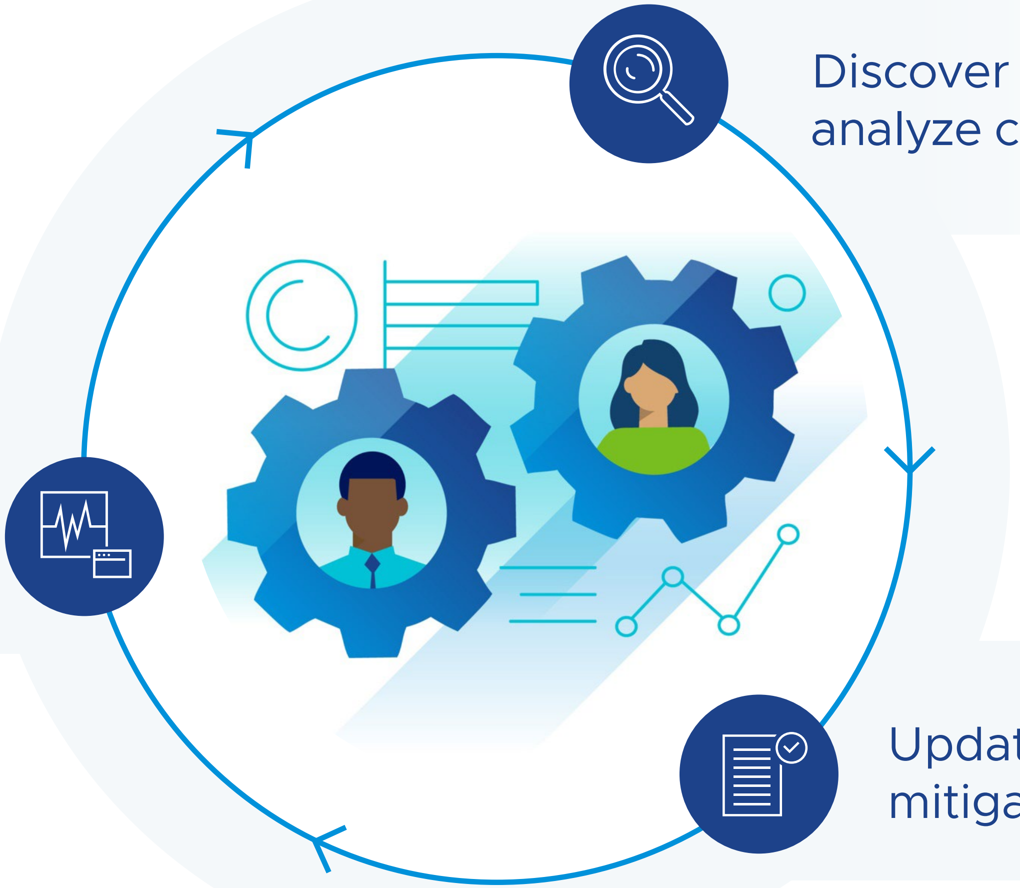


Validate failover with non-disruptive testing

- Activate VMs on the target site
- Power-on VMs on the test network
- Validate applications, sequence, scripts, and timing

Continuously Mitigate Risks

Monitor, manage, and test



Discover and analyze changes

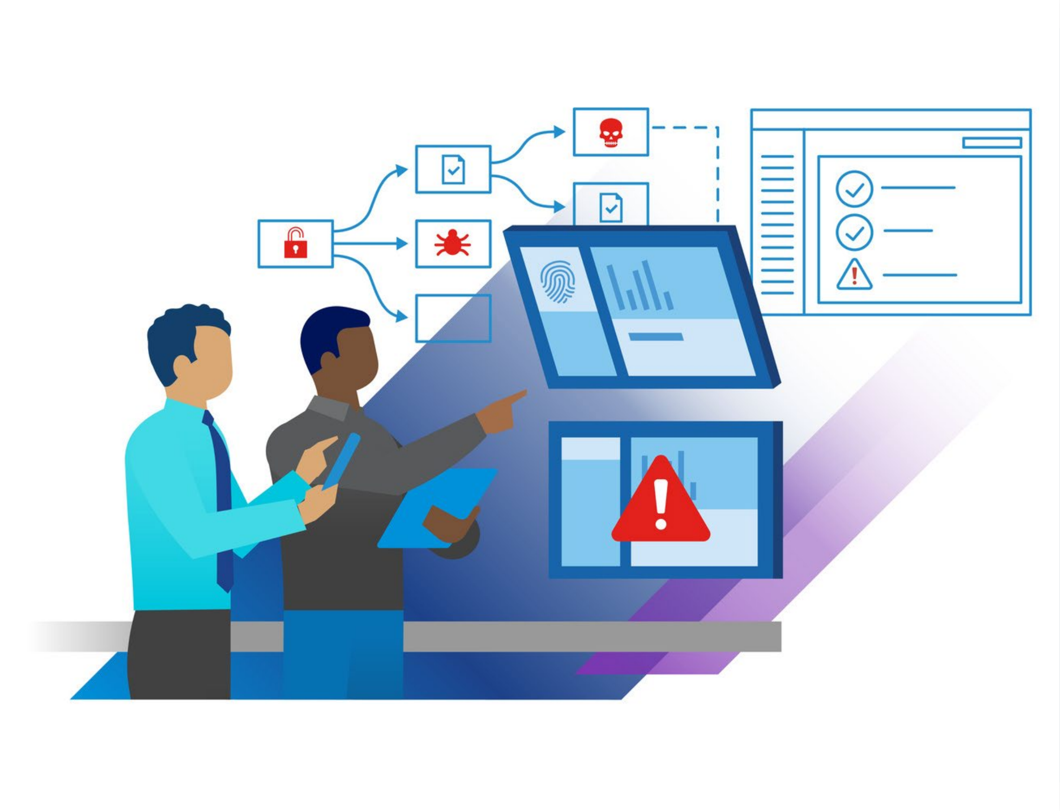
Update the mitigation plans

Keep testing, validate recovery points

Update Operations

Infrastructure Best Practices and Standard Operating Procedures

- Service Request Management
- Network and Firewall Configuration
- Capacity Management
- Virtual Machine Management
- Monitoring
- Patching and Upgrades



Security Operations Center (SOC) Procedures

- Security Posture Awareness
- Endpoint Security
- Threat Hunting
- Alert Triaging
- Threat Response
- Remediation and Recovery

Manufacturing Industry

Disaster recovery

IT / Business Problem

- Business critical applications do not have data protection
- Limited budget available for IT services
- Insufficient disaster recover strategy or plan
- Lack of staff and time to deploy disaster recovery sites
- Poor visibility into application complexities and dependencies

Solution

- Automated discovery of applications using VMware Aria Operations™ for Networks to analyze application groping to protect
- VMware Cloud Disaster Recovery on-demand solution leveraged to optimize cost
- Protection policies created based application RPO and RTO

Outcomes

Protected workloads to cloud successfully using VMware Cloud Disaster Recovery without any additional hardware

Protection grouping based on application dependency mapping

On-demand recovery for ransomware protection

Simplified and streamlined protection and recovery methodology using VMware Cloud Disaster Recovery

Highly satisfied customer with protection and recovery services

Product and Services Industry

Disaster recovery

IT / Business Problem

- Can't afford to take the time needed to research, implement and fully test disaster recovery plans
- Application availability needed incase of natural disasters such as hurricanes, floods, wildfires and earthquakes
- Protection from ransomware and cyber attacks
- Inefficient use of resources with current DR solutions
- Significant complexity and manual effort

Solution

- VMware Cloud Disaster Recovery solution provided with upfront SDDC deployment to cater customer RPO and RTO requirements
- Customized protection and recovery plans based on each application requirement
- Application dependency mapping using VMware Aria Operations for Networks
- Isolated recovery environment (IRE), so the ransomware can be fully remediated before migrating any virtual machines back into a production environment.

Outcomes

Cost effective on-demand DR solution which is scalable, flexible and easy to manage

Store a deep history of immutable snapshots in an isolated, offsite and encrypted cloud file system with daily data integrity checks

Non-disruptively test DR plans

Streamlined DR orchestration and reporting vmware® EXPLORE

Please take your survey.

vmware® EXPLORE

Thank You