VMware Cloud Foundation 9

# VCF 9.1 and Project Glasswing

## Defending Against Frontier AI Threats

July 8, 2026

vmware by Broadcom

# Disclaimer

Certain information in this presentation may outline Broadcom's general product direction.

This presentation shall not serve to (i) affect the rights and/or obligations of Broadcom or its licensees under any existing or future license agreement or services agreement relating to any Broadcom software product; or (ii) amend any product documentation or specifications for any Broadcom software product.

This presentation is based on current information and resource allocations and is subject to change or withdrawal by Broadcom at any time without notice.

The development, release and timing of any features or functionality described in this presentation remain at Broadcom's sole discretion.

Notwithstanding anything in this presentation to the contrary, upon the general availability of any future Broadcom product release referenced in this presentation, Broadcom may make such release available to new licensees in the form of a regularly scheduled major product release.

Such release may be made available to licensees of the product who are active subscribers to Broadcom maintenance and support, on a when and if-available basis.

The information in this presentation is not deemed to be incorporated into any contract.

# Disclaimer

This document is intended to provide general guidance for organizations that are considering Broadcom solutions. The information contained in this document is for educational and informational purposes only.

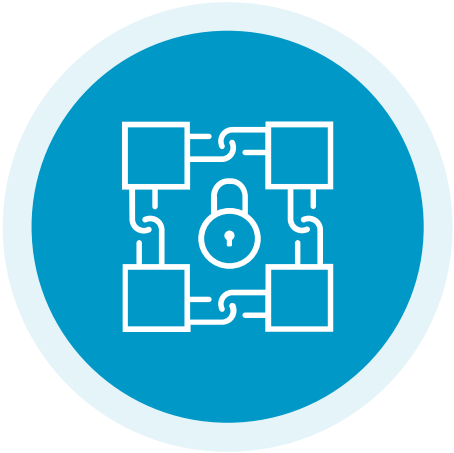
This document is not intended to provide advice and is provided “AS IS.”

Broadcom makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained herein.

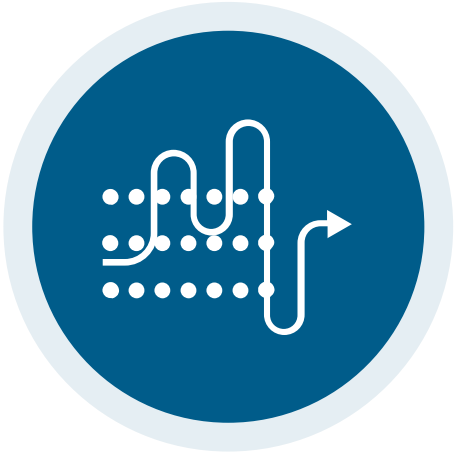
Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of requirements and effectiveness of implementations.

# Why Folks Are Worried About AI

Finds & Exploits Vulnerabilities



Chains Vulnerabilities

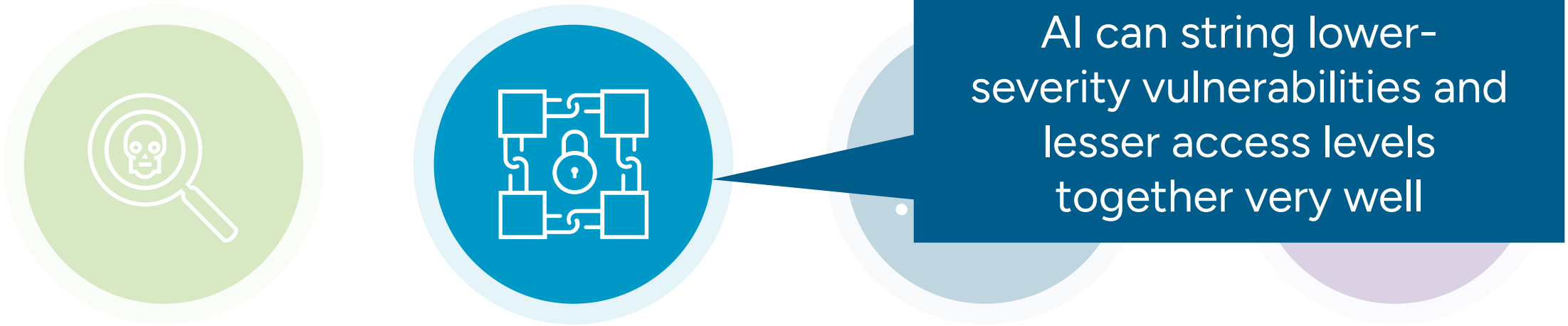


Customizes Malware

Conducts Attacks

# Why Folks Are Worried About AI

# Why Folks Are Worried About AI




Finds & Exploits Vulnerabilities

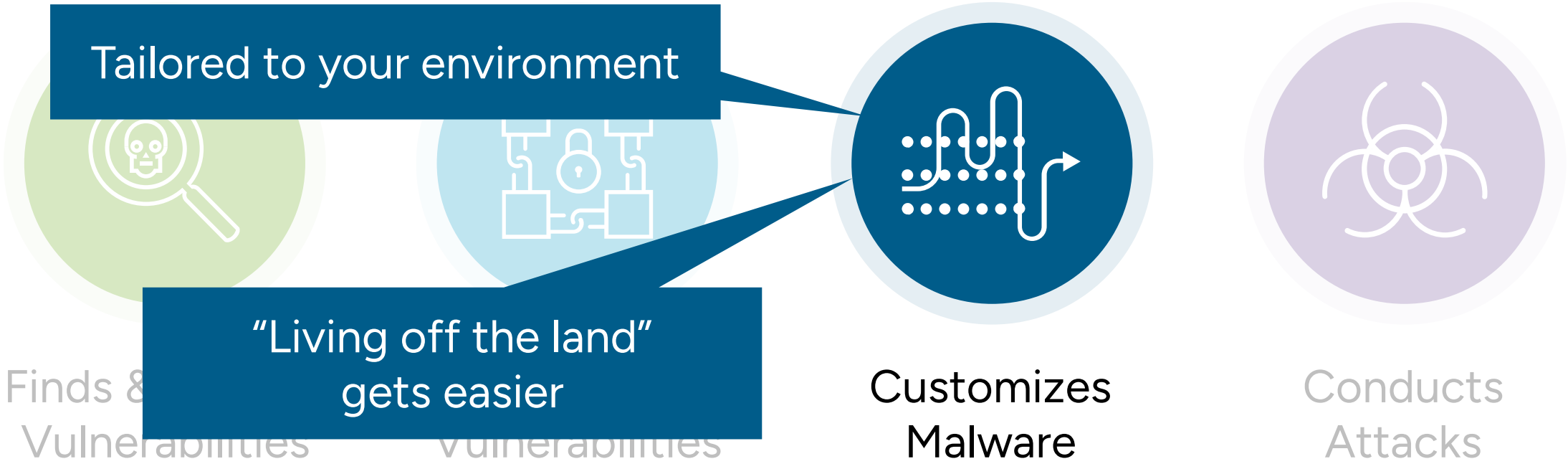
Chains Vulnerabilities

Customizes Malware

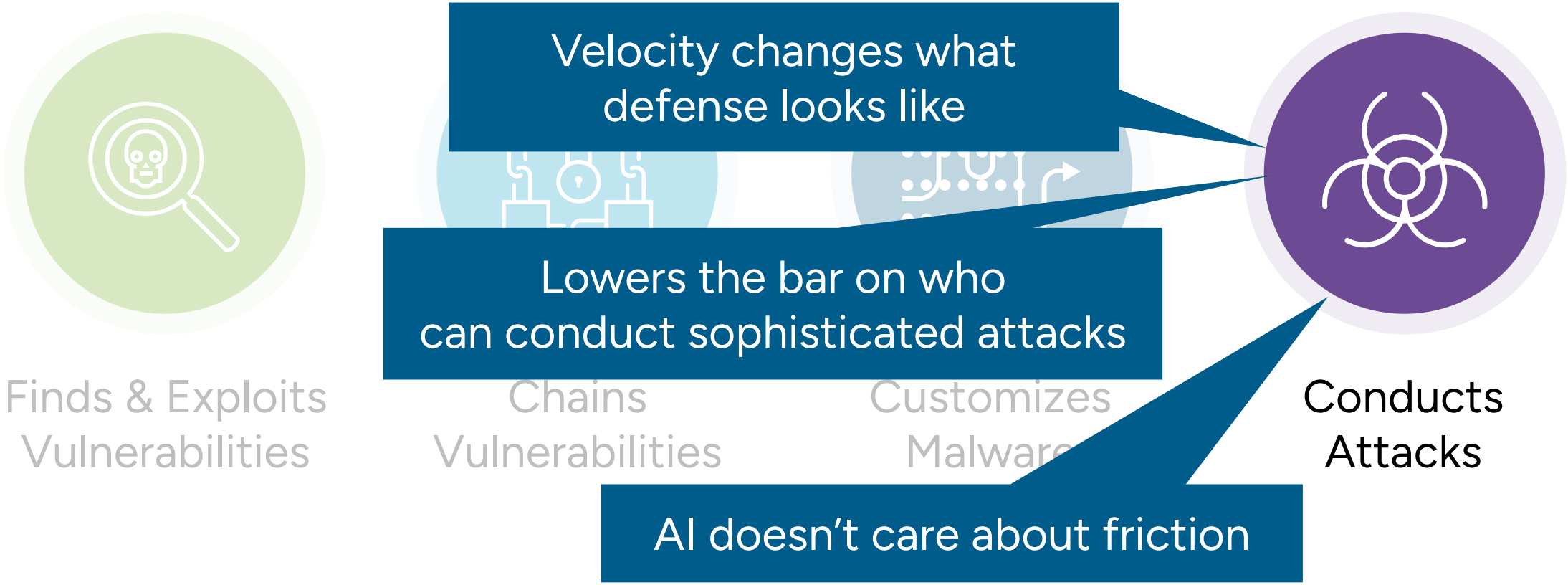
Conducts Attacks

vmware by Broadcom

# Why Folks Are Worried About AI



# Why Folks Are Worried About AI



# Organizations Need To Think Differently

## Security Always

The perils AI brings to us turn many things into actual operational risk. Actual architectural zero-trust security practices need to be prioritized.

## Patching Is One Piece

Patching is essential, but it is one piece among many. Identity, segmentation, logging, and recovery create resilience and defense-in-depth.

## Survivorship Bias

A clean record is easily mistaken for a strong defense. Perhaps the test has not come, or an attacker is already inside, unnoticed.

# Not Just Broadcom Saying These Things

Different Audiences, Same Ideas

## Cloud Security Alliance

Segmentation between systems

Identity isolation and phishing-resistant MFA

Deception and tripwires inside the network

Pre-authorized containment that runs at machine speed

## FS-ISAC

Treat vulnerability backlogs as operational risk, not compliance debt

Shift from vulnerability management to exploit prevention

Move beyond CVSS-only prioritization

Replace end-of-life software, stay within two major versions

## Anthropic

Patch internet-facing systems within 24 hours

Design for breach: hard barriers, not friction

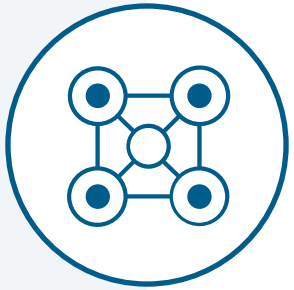
Manual approval cycles are now a security risk

Identity as primary control, segmentation as backstop

# What can be done?

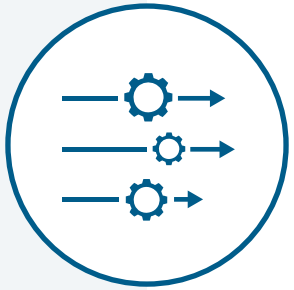
## Defend Holistically

Most intrusions exploit trust relationships between systems. Actual zero trust, plus strong identity and access controls help close gaps.



## Limit Lateral Movement

Perimeter and endpoint defenses will fail eventually. Segmentation and least privilege turn a compromise into a contained problem.



## De-Risk Patching

Snapshots, backups, canaries, and staged rollouts improve overall resilience (not just patching!)
All features that are in or available for VCF.

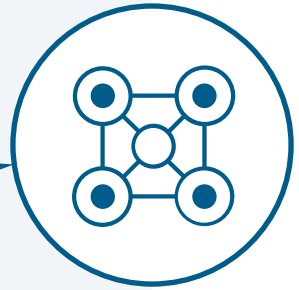
W
be

SSO & Federation!
RBAC! Avi!
Log Management!

## Defend Holistically

Most intrusions exploit trust relationships between systems. Actual zero trust, plus strong identity and access controls help close gaps.

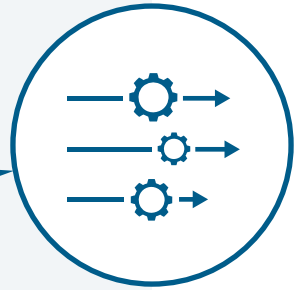
vDefend!
VLANs! VPCs!
Distributed Switch!



## Limit Lateral Movement

Perimeter and endpoint defenses will fail eventually. Segmentation and least privilege turn a compromise into a contained problem.

Protection & Recovery!
Replication! Avi!
Snapshots! Clones!



## De-Risk Patching

Snapshots, backups, canaries, and staged rollouts improve overall resilience (not just patching!)
All features that are in or available for VCF.

# Defense in Depth with VMware Cloud Foundation

## Cyber-Resilient Recovery

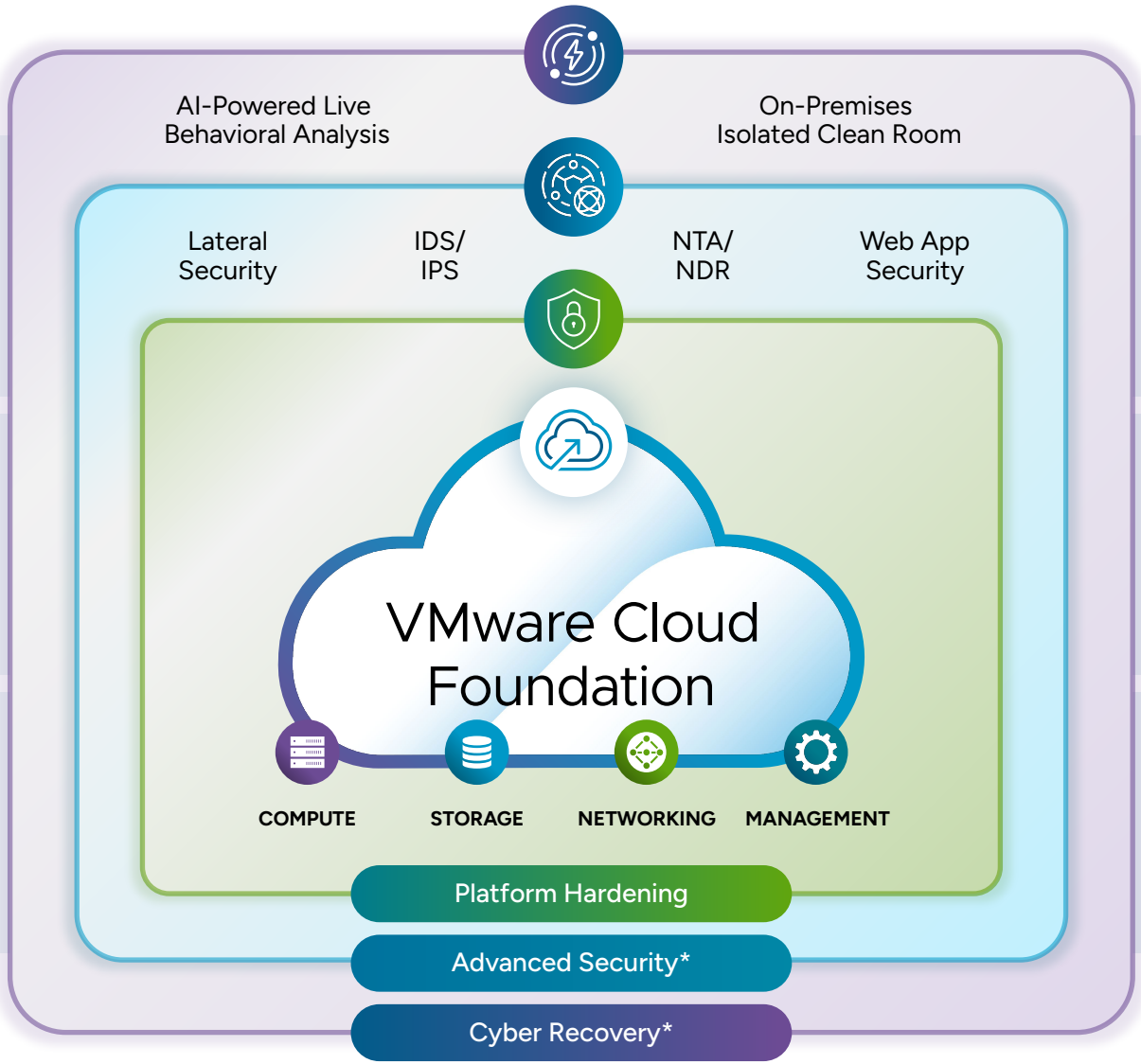
- Continuous replication with rollback points
- Automated testing in isolated networks
- Choice of detection vendor
- **Faster recovery, verified clean**

## Strong Lateral Security

- Visibility into every workload and flow
- Signature- and behavior-based detection
- Automated response and policy tuning
- **Reduce blast radius and dwell time**

## Hardened Infrastructure

- Compliance enforcement and drift detection
- Patching while workloads stay running
- High performance, secure storage
- **Resilient from hardware to workload**




vmware by Broadcom

* Capabilities mentioned here may require additional licensing

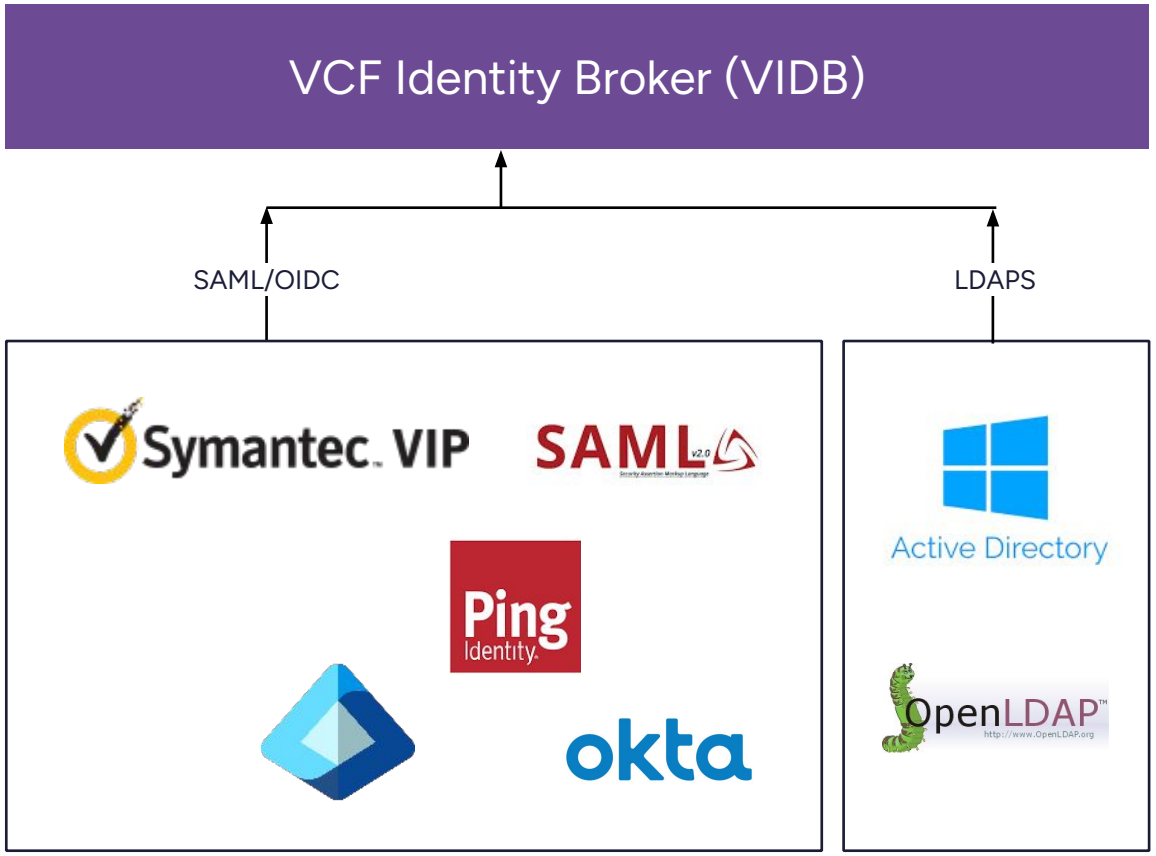
# Make Identity Hard To Compromise

## Authentication & Authorization

vmware by Broadcom

# Unified Identity: One Broker for All VCF Components

## VMware Cloud Foundation SSO




Embedded (in vCenter), standalone, and clustered appliance deployment models

Automatic configuration for vCenter, NSX, Operations, and Automation

One IdP configuration for VCF management components, but Automation has multitenancy

**Supports any SAML, OIDC, and AD/LDAPS-based IdP**

# Isolate Identity From Compromise

## Authentication & Authorization with VMware Cloud Foundation 9

1. **Use VCF SSO to federate VCF management with an isolated, infrastructure-only IdP.**
2. **Enable phishing-resistant MFA, number matching, and conditional access.**
3. **Do not connect HR, user provisioning, password reset, or configuration management systems to the infrastructure IdP.** Do not connect centralized monitoring systems to infrastructure in a way that lets them execute commands or push configurations.
4. **Help Desk must not be able to reset administrator authenticators, including for remote staff. Reset in person for all privileged accounts. This is a common threat actor tactic now.**
5. **Lower authentication token lifetimes.**
6. **Reduce permissions for service accounts to the minimum needed**.
7. Audit infrastructure IdPs against published best practices (disable SSPR, Seamless SSO).

"We cannot become what we want **by remaining what we are.**"

- Max De Pree

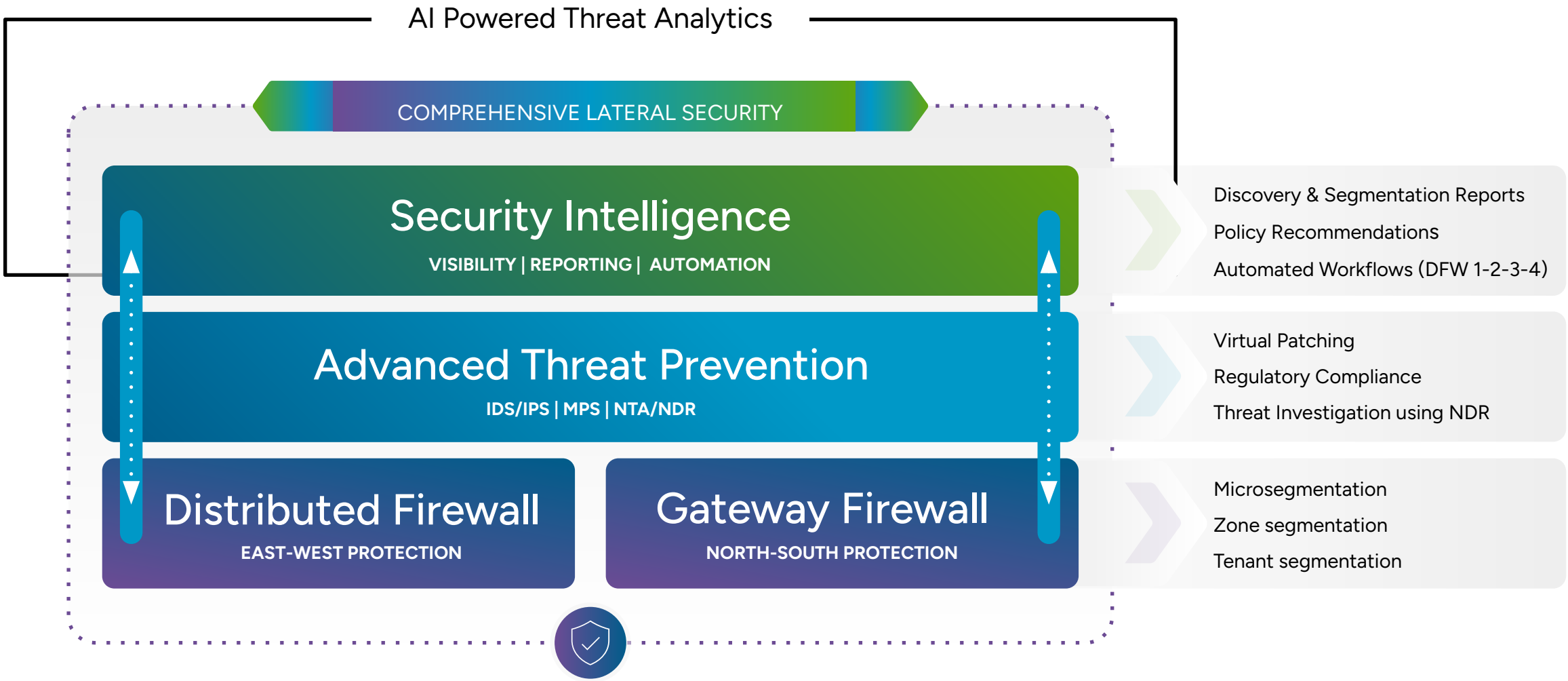
# Limit Lateral Movement of Attackers

## Network Access Control

vmware by Broadcom

# Lateral Security, Deep Visibility, and Automated Workflows

## VMware vDefend




vmware by Broadcom

# Limit Lateral Movement of Attackers

## Network Access Control with VMware Cloud Foundation 9

1. Add layers to public applications and websites with Avi and vDefend IDS/IPS/NTA.
2. **Egress rules, including DNS filtering and outbound inspection using vDefend Firewall.**
3. Identity-based microsegmentation between workloads with vDefend.
4. **Strict controls between infrastructure management interfaces and the rest of the organization. Consider privileged access workstations and out-of-band management.**
5. **Severely restrict access to ESX. Drive all access through vCenter & RBAC model.**
6. Canaries, honeypots, and tripwires on the network.
7. **Let vDefend automatically block problems when they are detected.**

# See What Attackers Are Doing

## Logging & Detection

vmware by Broadcom

# Logs

ANALYZE LOGS | COMPARE LOGS

LOG SOURCES

Choose Saved Query | Search logs for text containing

PARTITION: All Partitions

5M 1H 6H 24H 7D CUSTOM

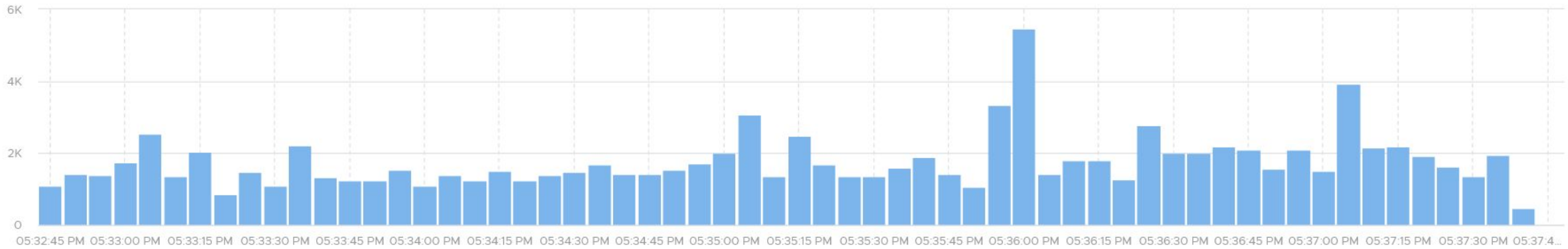
4/30/26 5:32 PM - 4/30/26 5:37 PM

ADD FILTER

COMPARE SAVE QUERY

COUNT OF EVENTS | OVER TIME | APPLY | RESET

CHART TYPE | 5 seconds




Stream | Event Types | Event Trends

EXPORT

Sorting By: Newest First

1 - 50 of 105.91K items | 1 / 400

| Timestamp | Log |
|---|---|
| 2026-04-30 17:37:41 -05:00 | 2026-04-30T22:37:38.312Z INFO blueprint-service-app [host='tango-blueprint-service-app-5c4c75bc98-ks5zj' thread='generalScheduler-1' user='' org='' trace=''][bp='' proj='' dep='' req='' flow='' task='' tile='' res='' op=''] c.v.t.b.telemetry.LogMetricsConfig - threadPoolTaskExecutor executor stats: poolSize=0 active=0 corePoolSize=15 max=2147483647 prefix=tasks- |
| 2026-04-30 17:37:41 | 2026-04-30T22:37:38.312Z INFO blueprint-service-app [host='tango-blueprint-service-app-5c4c75bc98-ks5zj' thread='generalScheduler-1' user='' |

Fields

FIELDS LIBRARY

Search Fields

app

cluster

component

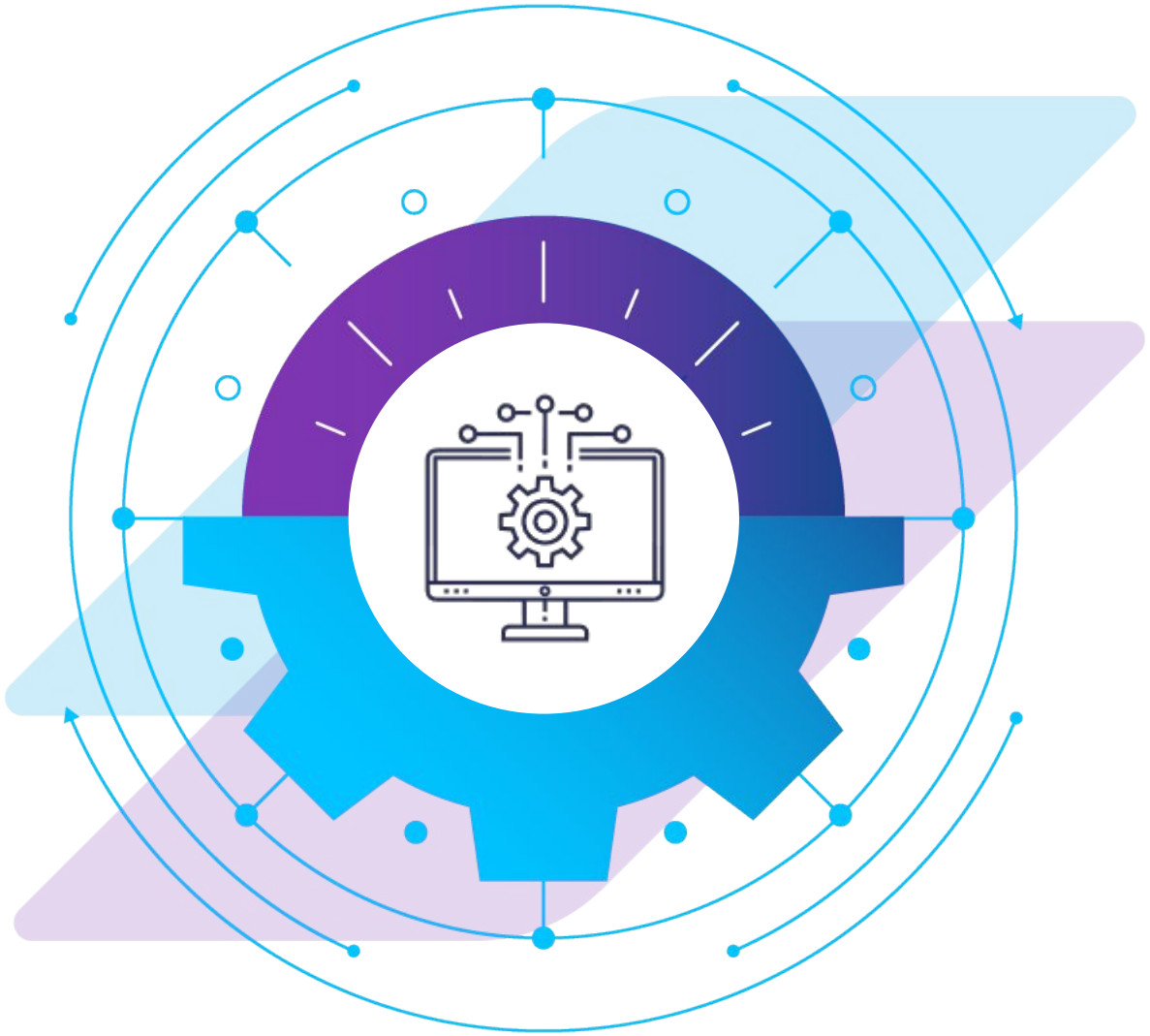
# See What Attackers Are Doing

## Logging & Detection with VMware Cloud Foundation 9

1. Follow the VMware VCF Security Configuration Guide to enable audit logging everywhere.
2. Attackers are often using stolen credentials and have administrator access to the breached systems. Use VCF Log Management to aggregate, filter, and forward logs to your SIEM, out of reach from the attackers who might have access to the systems generating the data.
3. Retain logs long enough to investigate a breach that started three years ago. This includes access logs for your IdP (isolated IdP has a much lower volume of logs!)
4. Watch for legitimate operations performed by the wrong thing. Cloning by something that does not clone. Snapshots outside backup windows. Exports from accounts that do not export. See the VMware guidance on defending against BRICKSTORM for more info.
5. Watch for changes to logging and audit configuration itself.

# Patch Everything, Survive Anything

## De-Risk Patching



vmware by Broadcom

# Reworking The VCF Roadmap To Protect Customers

VCF continues to be the most trustworthy platform for workloads

VCF 9.1 is the beginning of this journey

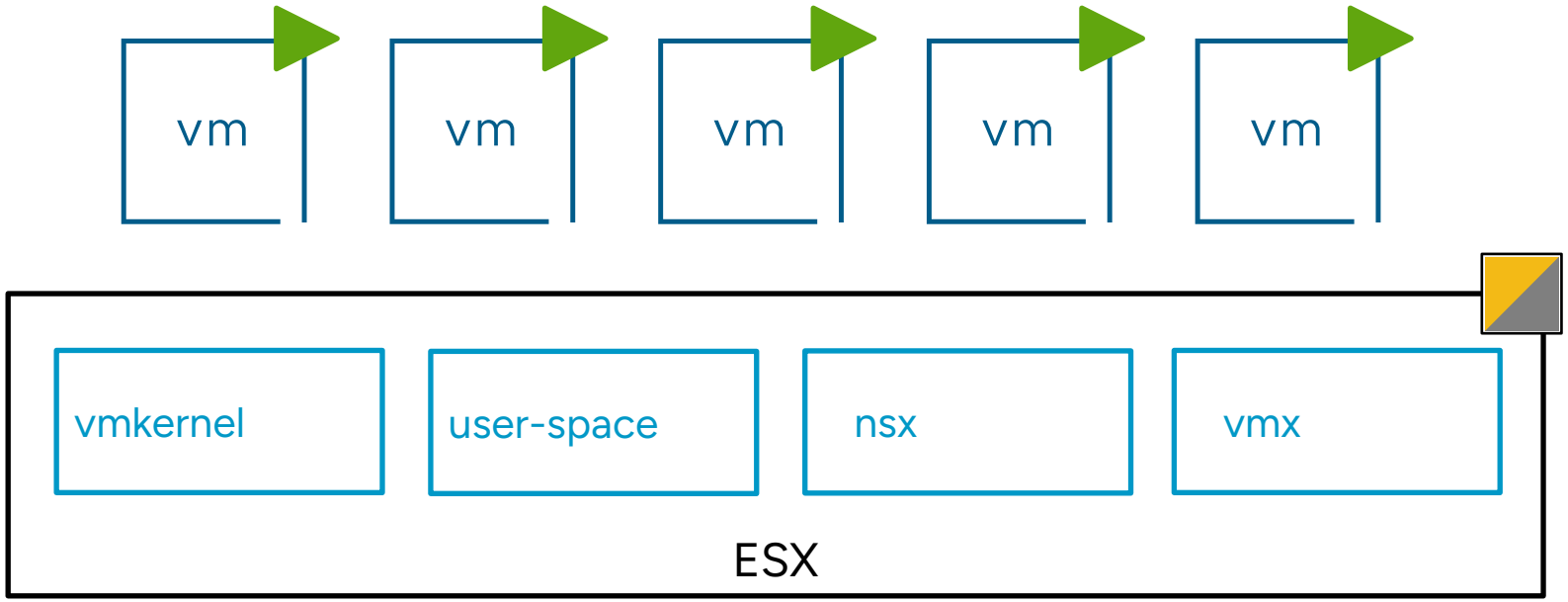
New monthly VCF 9.1.0.x patches

Quarterly 9.1.x releases may add security capabilities

Controlled VCF architectural changes

# Zero Downtime Updates At The Core of VCF

Live Patch of ESX vmkernel, VM runtime, NSX, vSAN, system daemons, and vCenter!




**Most critical patching intended to incur minimal to no disruption**

**TPM-enabled hosts now fully supported for live patching**

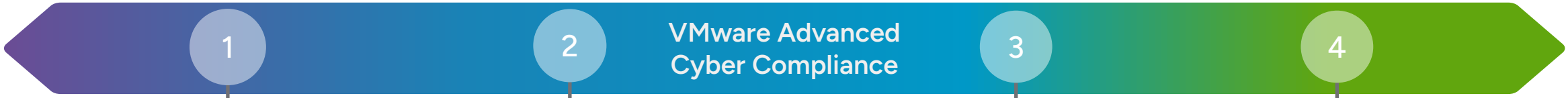
Some limitations apply: Confidential Computing, PodVM, skipping versions, big updates.

# Purpose-Built Cyber Recovery With End-to-End Automation

DR and immutable backups are **not enough** for cyber recovery

AI-powered cyberattacks have **redefined cyber recovery requirements**

AI threats **exploit gaps** created by **fragmented operations**




**ISOLATED CLEAN ROOM**

Safe environment to power on workloads for validation before restore to production

**VM NETWORK ISOLATION**

Isolation of workloads during validation to prevent malware spread and reinfection

**AI/ML-POWERED VALIDATION**

Detection of malware-free, "living-off-the-land" attacks that remain undetected with traditional antivirus

**END-TO-END CYBER RECOVERY WORKFLOW**

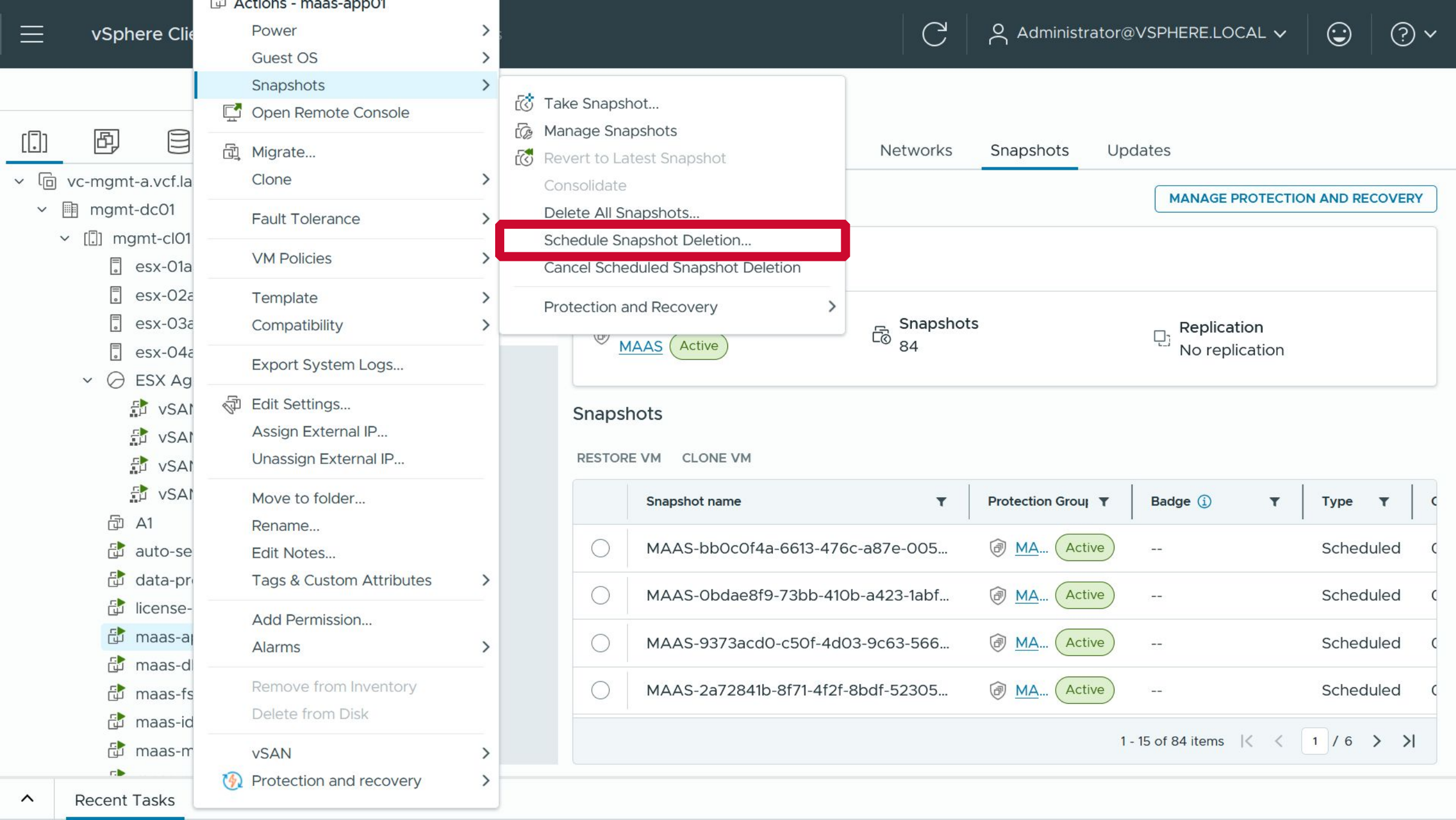
Fully-integrated cyber recovery to on-premises VCF sites with guided workflow automation

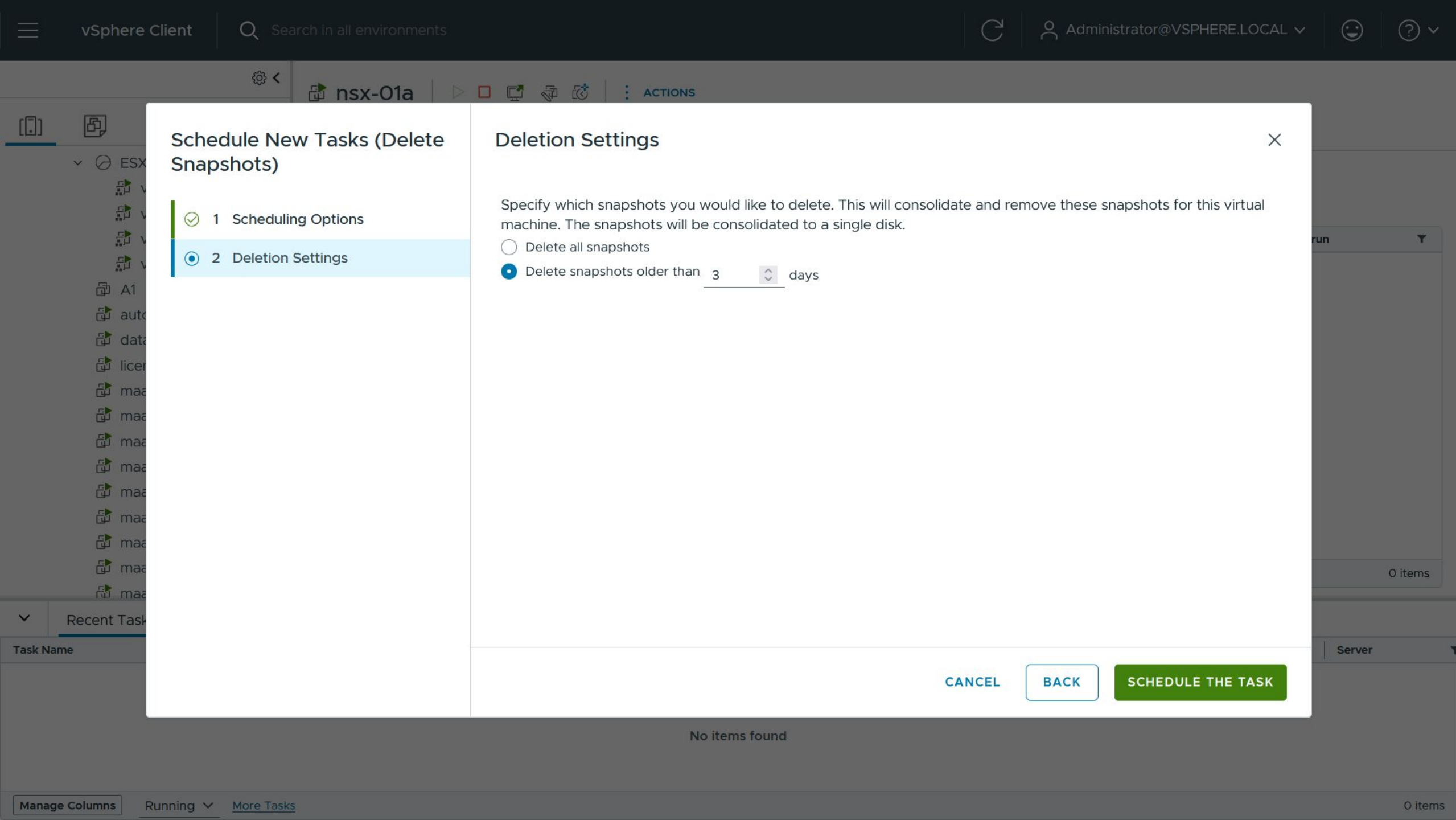
vmware by Broadcom

# Make Rollback Easy Enough to Patch Anything

## Workload Protection with VMware Cloud Foundation 9

1. Software updates sometimes introduce unexpected change. **The fix is a pipeline that catches them early, not a process that patches slowly.**
2. **Snapshot before patching.** Automated through API, with automatic cleanup after a defined window (schedule snapshot cleanup).
3. Snapshots capture VM virtual hardware configuration, too (including compatibility levels).
4. **Deploy and use the vSAN Data Protection appliance for automated, continuous, workload-level point-in-time/tactical recovery options.** This is not a backup, though.
5. **Use Avi & rolling updates to keep services up during patching.** “Too important to be down” is now “too important to leave unsecured.” Service availability has robust solutions.
6. **Replicate critical workloads with VCF Cyber Recovery**. Use the testing tools to practice the recovery regularly so you know how it will work, and that it will work.
7. **Make workloads start automatically when their VMs start**.

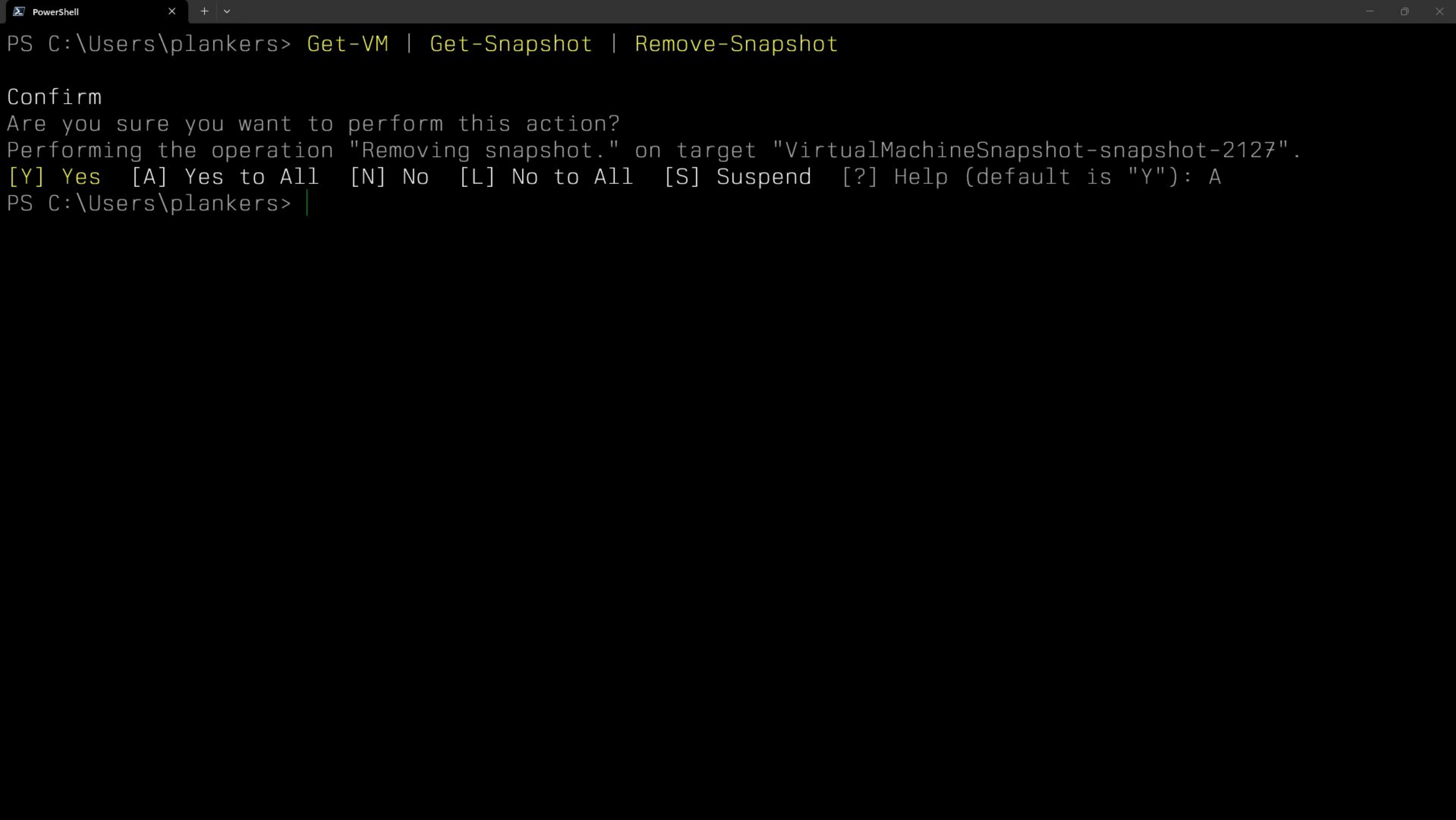

vSphere Clie
Administrator@VSPHERE.LOCAL
Actions - maas-app01
Power
Guest OS
Snapshots
Open Remote Console
Migrate...
Clone
Fault Tolerance
VM Policies
Template
Compatibility
Export System Logs...
Edit Settings...
Assign External IP...
Unassign External IP...
Move to folder...
Rename...
Edit Notes...
Tags & Custom Attributes
Add Permission...
Alarms
Remove from Inventory
Delete from Disk
vSAN
Protection and recovery
Take Snapshot...
Manage Snapshots
Revert to Latest Snapshot
Consolidate
Delete All Snapshots...
Schedule Snapshot Deletion...
Cancel Scheduled Snapshot Deletion
Protection and Recovery
vc-mgmt-a.vcf.la
mgmt-dc01
mgmt-cl01
esx-01a
esx-02a
esx-03a
esx-04a
ESX Ag
A1
Networks
Snapshots
Updates
MANAGE PROTECTION AND RECOVERY
MAAS
Active
Snapshots
84
Replication
No replication
Snapshots
RESTORE VM
CLONE VM
Snapshot name
Protection Grou
Badge
Type
MAAS-bb0c0f4a-6613-476c-a87e-005...
MAAS-0bdae8f9-73bb-410b-a423-1abf...
MAAS-9373acd0-c50f-4d03-9c63-566...
MAAS-2a72841b-8f71-4f2f-8bdf-52305...
Active
Scheduled
1 - 15 of 84 items
1 / 6
Recent Tasks


vSphere Client
Search in all environments
Administrator@VSPHERE.LOCAL
nsx-01a
ACTIONS
Schedule New Tasks (Delete Snapshots)
1 Scheduling Options
2 Deletion Settings
Deletion Settings
Specify which snapshots you would like to delete. This will consolidate and remove these snapshots for this virtual machine. The snapshots will be consolidated to a single disk.
Delete all snapshots
Delete snapshots older than 3 days
CANCEL
BACK
SCHEDULE THE TASK
Recent Tasks
Task Name
Server
No items found
Manage Columns
Running
More Tasks
0 items

PowerShell

```
PS C:\Users\plankers> Get-VM | New-Snapshot -Name PrePatch

Name                 Description                    PowerState
----                 -----------                    ----------
PrePatch                                            PoweredOff
PrePatch                                            PoweredOff
PrePatch                                            PoweredOff
PrePatch                                            PoweredOff
PrePatch                                            PoweredOff
PrePatch                                            PoweredOff
PrePatch                                            PoweredOff
PrePatch                                            PoweredOff
PrePatch                                            PoweredOff
PrePatch                                            PoweredOff
New-Snapshot: 6/8/2026 4:51:31 PM      New-Snapshot           The operation for the entity "nsx-01a" f
ailed with the following message: "An error occurred while saving the snapshot: Exceeded the maximum num
ber of permitted snapshots.". An error occurred while saving the snapshot: Exceeded the maximum number o
f permitted snapshots. An error occurred while taking a snapshot: Exceeded the maximum number of permitt
ed snapshots.
New-Snapshot: 6/8/2026 4:51:31 PM      New-Snapshot           The operation for the entity "platform-s
ervices-a-hng7n" failed with the following message: "An error occurred while saving the snapshot: Exceed
ed the maximum number of permitted snapshots.". An error occurred while saving the snapshot: Exceeded th
e maximum number of permitted snapshots. An error occurred while taking a snapshot: Exceeded the maximum
 number of permitted snapshots.
PrePatch                                            PoweredOff
PrePatch                                            PoweredOff
PrePatch                                            PoweredOff
PrePatch                                            PoweredOff
PrePatch                                            PoweredOff
```


PowerShell
PS C:\Users\plankers> Get-VM | Get-Snapshot | Remove-Snapshot
Confirm
Are you sure you want to perform this action?
Performing the operation "Removing snapshot." on target "VirtualMachineSnapshot-snapshot-2127".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): A
PS C:\Users\plankers>

# maas-app01

ACTIONS

Summary | Monitor | Configure | Permissions | Datastores | Networks | Snapshots | Updates

- Snapshot Management
- Snapshot Deletion
- Protection and Recovery
  - Snapshot Management

## Protection and Recovery

MANAGE PROTECTION AND RECOVERY

### Overview

**Protection Groups**
MAAS Active

**Snapshots**
84

**Replication**
No replication

### Snapshots

RESTORE VM | CLONE VM

| Snapshot name | Protection Group | Badge | Type | Created At | Expires At |
|---|---|---|---|---|---|
| MAAS-bb0c0f4a-6613-476c-a87e-005... | MAAS Active | -- | Scheduled | 06/08/2026, 3:13:35 PM | 06/15/2026, 3:13:35 PM |
| MAAS-0bdae8f9-73bb-410b-a423-1abf... | MAAS Active | -- | Scheduled | 06/08/2026, 1:13:35 PM | 06/15/2026, 1:13:35 PM |
| MAAS-9373acd0-c50f-4d03-9c63-566... | MAAS Active | -- | Scheduled | 06/08/2026, 11:13:35 AM | 06/15/2026, 11:13:35 AM |
| MAAS-2a72841b-8f71-4f2f-8bdf-52305... | MAAS Active | -- | Scheduled | 06/08/2026, 9:13:35 AM | 06/15/2026, 9:13:35 AM |
| MAAS-54a12676-3e7c-424c-8d82-2a8... | MAAS Active | -- | Scheduled | 06/08/2026, 7:13:35 AM | 06/15/2026, 7:13:35 AM |
| MAAS-9bf66cf3-a368-480c-979e-b441... | MAAS Active | -- | Scheduled | 06/08/2026, 5:13:35 AM | 06/15/2026, 5:13:35 AM |
| MAAS-c43771ce-7848-4fd5-8fc3-bb78... | MAAS Active | -- | Scheduled | 06/08/2026, 3:13:35 AM | 06/15/2026, 3:13:35 AM |
| MAAS-cd7be1e6-3f8d-49df-837f-0d56... | MAAS Active | -- | Scheduled | 06/08/2026, 1:13:35 AM | 06/15/2026, 1:13:35 AM |

1 - 15 of 84 items 1 / 6

# mgmt-cl01

ACTIONS

Summary | Monitor | Configure | Permissions | Hosts | VMs | Datastores | Networks | Updates


- Services
  - vSphere DRS
  - vSphere Availability
- Configuration
  - Quickstart
  - General
  - Key Provider
  - VMware EVC
  - VM/Host Groups
  - VM/Host Rules
  - VM Overrides
  - I/O Filters
  - Host Options
  - Host Profile
- Licensing
- Alarm Definitions
- Scheduled Tasks
- Desired State
  - Configuration
- vSAN


## Protection and Recovery

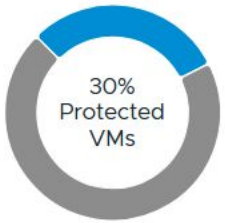
Use Protection and Recovery to protect your VMs with local and remote vSAN snapshots against disasters, outages, and cyber threats.

SUMMARY | PROTECTION GROUPS | VMS | REPLICATION

### Overview

Protection groups
1

Active 1




Protected VMs
12 (out of 40)

VMs with local protection 12 (30%)
Not protected VMs 28 (70%)

### vSAN Snapshot Space Usage

939.99 GB (18.56%) Free usable capacity 4.03 TB

Used capacity 939.99 GB (18.56%) Used by vSAN snapshots 25.22 GB (0.49%)

Scheduled snapshots will not be taken if the datastore's capacity exceeds 70% threshold.

VIEW VSAN CAPACITY

The investments in process improvement that make patching safe also make **ransomware recovery, hardware failure, application upgrades, human error, and AI coding tools dropping your databases survivable.**

# Security Hardening & Compliance Resources

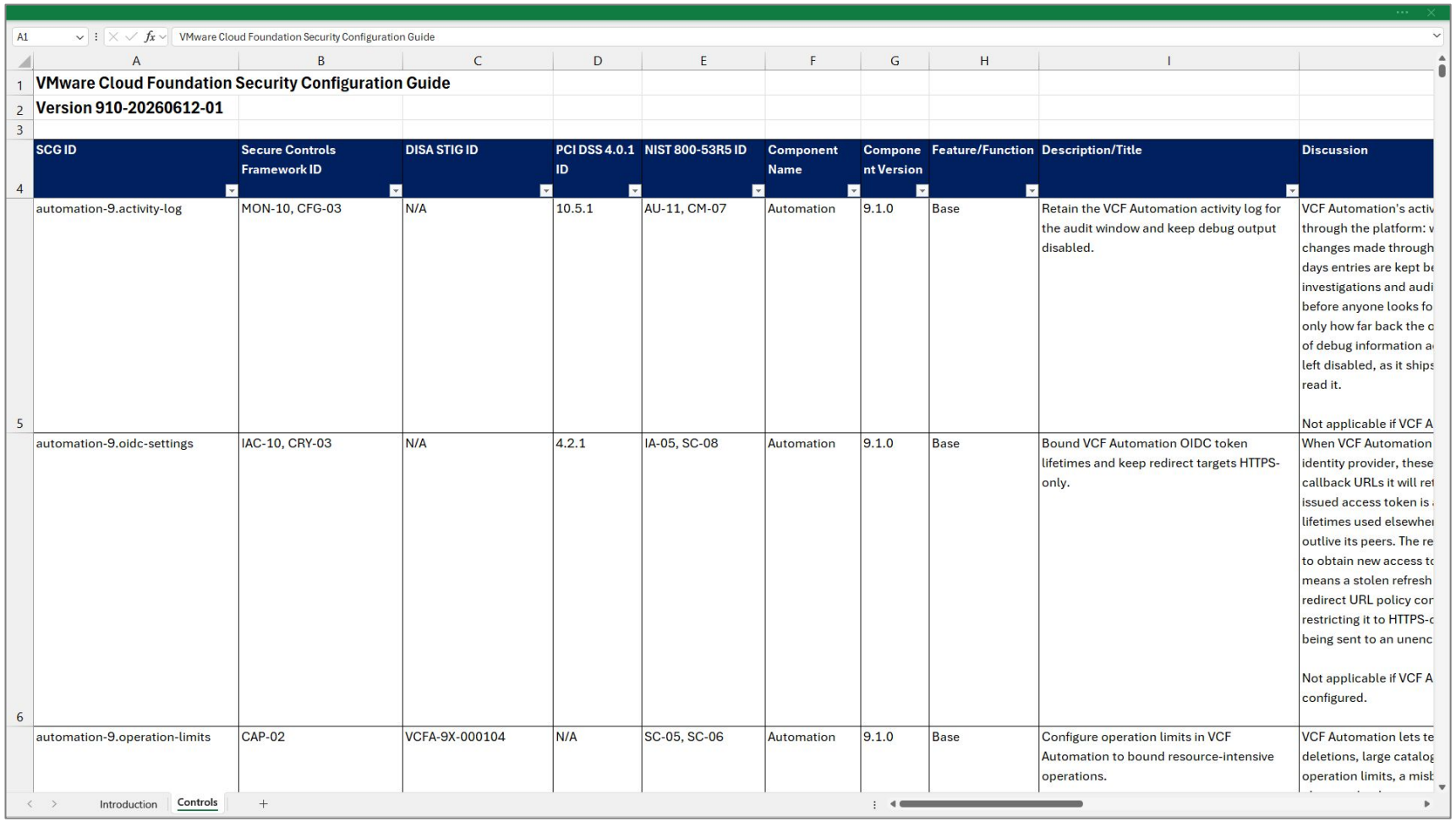
https://brcm.tech/vcf-security

https://github.com/vmware/vcf-security-and-compliance-guidelines/

vmware by Broadcom

# Baseline Hardening Made Easy Across All VCF Components

## VCF 9.1 Security Configuration Guide at https://brcm.tech/vcf-security



VMware Cloud Foundation Security Configuration Guide

**VMware Cloud Foundation Security Configuration Guide**

**Version 910-20260612-01**

| SCG ID | Secure Controls Framework ID | DISA STIG ID | PCI DSS 4.0.1 ID | NIST 800-53R5 ID | Component Name | Component Version | Feature/Function | Description/Title | Discussion |
|---|---|---|---|---|---|---|---|---|---|
| automation-9.activity-log | MON-10, CFG-03 | N/A | 10.5.1 | AU-11, CM-07 | Automation | 9.1.0 | Base | Retain the VCF Automation activity log for the audit window and keep debug output disabled. | VCF Automation's activ through the platform: v changes made through days entries are kept be investigations and audi before anyone looks fo only how far back the c of debug information a left disabled, as it ships read it.<br><br>Not applicable if VCF A |
| automation-9.oidc-settings | IAC-10, CRY-03 | N/A | 4.2.1 | IA-05, SC-08 | Automation | 9.1.0 | Base | Bound VCF Automation OIDC token lifetimes and keep redirect targets HTTPS-only. | When VCF Automation identity provider, these callback URLs it will ret issued access token is lifetimes used elsewher outlive its peers. The re to obtain new access to means a stolen refresh redirect URL policy con restricting it to HTTPS-c being sent to an unenc<br><br>Not applicable if VCF A configured. |
| automation-9.operation-limits | CAP-02 | VCFA-9X-000104 | N/A | SC-05, SC-06 | Automation | 9.1.0 | Base | Configure operation limits in VCF Automation to bound resource-intensive operations. | VCF Automation lets te deletions, large catalog operation limits, a misb |

Introduction | Controls

- Filterable based on component, feature, version, and risk
- Standardizes checks across components
- Maps additional regulations and differences
- **Guidance that is easy to use and understand for VCF components**

vmware by Broadcom

# Understand How VCF Features Meet Regulatory Requirements

VCF Regulatory Compliance Library at https://brcm.tech/vcf-security


27 standards + the Secure Controls Framework itself

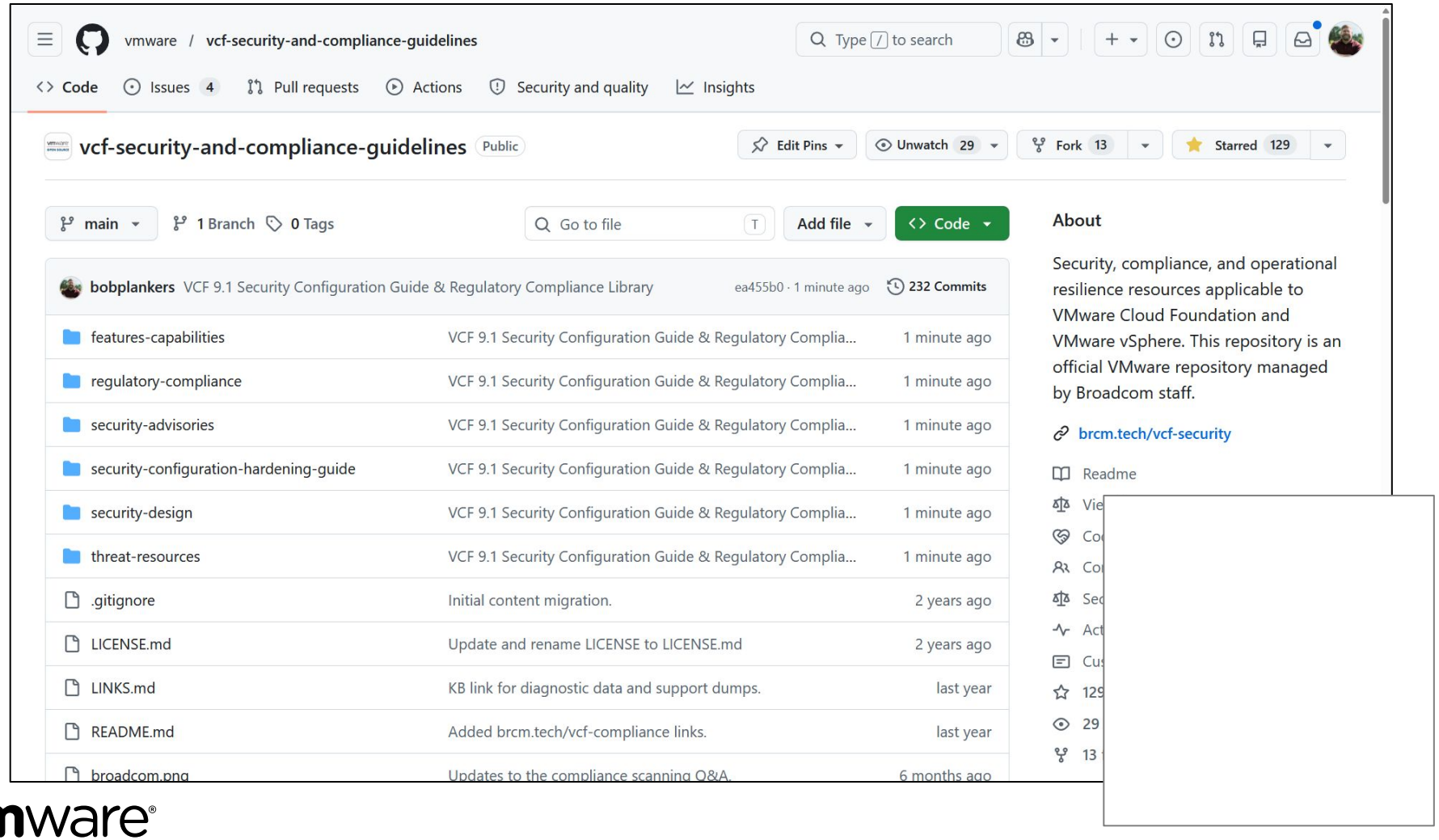
XLSX, CSV, Markdown, PDF

Know which VCF features apply to a specific regulatory requirement.

**Aids auditor understanding of VCF features.**

# Security & Compliance Repository: brcm.tech/vcf-security

https://github.com/vmware/vcf-security-and-compliance-guidelines




- SCG & sample code for automation
- Regulatory compliance library
- Whitepapers on standards and design
- Q&A for product capabilities
- “One-stop shop” for platform security

vmware by Broadcom

VMware Cloud Foundation 9

# Thank You