WHITE PAPER–MARCH 2021

Cloud Workload Protection

How to secure workloads in hybrid clouds

Table of contents

Executive summary

The hybrid cloud is at the centerpiece of digital transformation. Today, more than 90 percent of enterprises report using a multi-cloud strategy, with most combining their use of public and private clouds.[1] The good news is that this approach offers the necessary flexibility and scalability to support rapid innovation. The downside is that it often adds increased complexity and risk, making security an essential component across private and public clouds.

As enterprise teams deploy and manage critical workloads across multi-cloud environments, visibility into the security posture of workloads and controlling the attack surface are critical for securing data and maintaining operations.

Many distinct teams across the enterprise, including IT Ops and SecOps, are key stakeholders in the performance, availability and security of cloud workloads. Keeping team members aligned rather than fragmented is also an essential success factor.

This white paper covers the key challenges enterprise teams have encountered in securing cloud workloads, and how to overcome them using the VMware intrinsic security approach featuring VMware Carbon Black Cloud™, VMware vSphere®, and VMware NSX®. This paper also includes a discussion of how the cloud forces a new way to think about risk—one that can bring cross-team stakeholders together rather than remain across the digital divide. A cloud workload protection platform evaluation checklist is also provided to help organizations examine key requirements when considering solutions.

Security challenges with private, public and hybrid clouds

Deploying and managing workloads and apps in private, public and hybrid clouds takes a village. What we once considered traditional IT has been replaced by a collective. IT Ops, DevOps and SecOps now team together to deliver and secure apps and services from the cloud.

[1] Flexera. “Flexera 2020 State of the Cloud Report.” April 2020.

As shown in Table 1, failing to develop cross-team coordination and plan for the unique aspects of cloud workloads can lead to increased risks.

	HYBRID CLOUD OPERATIONS	SECURITY CHALLENGES	TRADITIONAL IT OPERATIONS	GAPS IN TRADITIONAL IT SECURITY
Design architecture	Interconnected services	• No visibility into how workloads communicate and connect • Flat, non-segmented networks increase risk	Monolithic and isolated	• Traditional antivirus (AV) not built for a cloud workload context • Data center-centric monitoring lacks baseline understanding of what normal network behavior is
Operational model	Distributed ownership and management	• IT Ops is responsible for the posture, management and availability of workloads but can't see vulnerabilities within them • Technology and process silos contribute to misconfigurations, insecure configurations, and other human errors	Centralized	• The addition of point security products requires installing additional agents, slowing system performance, and complicating operations • The lack of unified visibility within workloads, and across workloads and clouds, complicates cross-team coordination
Scalability	Highly dynamic, automatic	• The lack of change control results in misconfigurations, such as unsecured data storage, excessive permissions, default credentials and configuration settings, and disabling security controls • The inability to standardize workload security policies across private and public clouds increases risk	Static, manual	• Traditional scanning is not designed to catch common cloud misconfigurations (the leading cause of cloud-based data breaches)[2] • Deploying point security solutions for each distinct cloud environment complicates managing governance and policy at scale

TABLE 1: Security challenges with hybrid cloud workloads stem from failing to recognize the key differences between cloud computing and traditional IT.

[2] Cloud Security Alliance. "Top Threats to Cloud Computing: Egregious Eleven Deep Dive." September 2020.

IT Ops, DevOps and SecOps all share the responsibility of maintaining the security and availability of critical workloads in the cloud.

Three steps for redefining risk

The best way to make the most of digital transformation is to accept how much of a paradigm shift it represents. Old risk management models no longer apply when change is a constant and there are so many cooks in the kitchen.

When securing cloud workloads, enterprise teams need to:

1. Increase visibility – Identify unknown or undetected risks in workloads.
2. Speed recovery – Accelerate risk recovery by building resilience into cloud workloads.
3. Simplify security – Unify risk mitigation across workloads, endpoints and containers.

Step One: Increase visibility – Identify unknown or undetected risks in workloads

- **Why this is a challenge** – You cannot manage risks you don't know exist. Unfortunately, most virtual machine (VM) administrators lack visibility into how the apps and workloads running on their VMs are potentially vulnerable to attacks. While an attacker only needs to identify and exploit a single vulnerability to gain unauthorized access, those protecting it need to know all the ways it can be exploited so they can close those holes. Plus, once vulnerabilities are identified, gaining consensus between IT Ops and SecOps on which vulnerabilities are the highest priority to fix, why and when, is not always straightforward.
- **Example** – Joe is a site reliability engineer (SRE) for a large healthcare services company. He's responsible for managing their private cloud infrastructure, which includes servers, workloads and apps that process sensitive healthcare data. Joe knows that he needs to identify and mitigate any vulnerabilities that may impact compliance or expose patient data. That said, service performance, availability and uptime are top priorities for Joe and the other SREs on his team. After all, patient care is mission-critical.

  Currently, Joe expects Sarah, a security analyst, to tell him when a scheduled scan detects a high severity vulnerability that requires mitigation. They often disagree on the best course of action because each uses a different toolset. Without a common system of record, reaching consensus on these critical issues remains elusive: Which vulnerabilities have the highest priority, are these compensating controls sufficient, what are attackers targeting and how, and so on.
- **What's needed: Cross-domain risk discovery** – Discover all cloud workload risks—from all angles and attack vectors—and use a common system of record to manage them. If a patch cannot be implemented due to downtime risk, gain consensus on a compensating control, or set up a watchlist to detect when the vulnerability is targeted.

Step Two: Speed recovery – Accelerate risk recovery by building resilience into cloud workloads

- **Why this is a challenge** – For most enterprises, data breaches have become not a question of if, but when. During a breach, knowing the extent or blast radius of the exposure is critical to prevent similar outbreaks in the future. Additionally, these insights are fundamental for a rapid and complete recovery. The challenge is one of competing priorities. For DevOps and IT Ops teams, their priority is to restore services as quickly as possible, even if that means destroying forensic evidence and artifacts the SecOps team needs to identify and investigate the source and full scope of the attack.
- **Example** – Recovering from a ransomware attack within your cloud environment can be costly, complicated and labor-intensive. These outbreaks can migrate from workloads to the servers hosting them to the endpoints used by employees to access these workloads. The goal is to reduce the attack surface for the ransomware attack by shutting down the early stages of the attack—code execution within the workload itself—before the toolset is fully deployed or the command and control (C2) connections are set up to exfiltrate or encrypt the data for ransom.

- **What's needed: Risk resilience** – Restoring services rapidly after a breach or malware attack and retaining the data needed to perform forensic investigations is possible in the cloud providing you have the right workload security platform. In fact, bridging this divide is a key aspect of building risk resilience into your cloud workloads. Managing workload and endpoint security from the same platform enables teams to identify risks across these control points and pursue a more resilient recovery strategy.

Step Three: Simplify security – Unify risk mitigation across workloads, endpoints and containers

- **Why this is a challenge** – Managing risk in cloud workloads using traditional point solutions leads to stovepipe processes that add operational overhead and compound risk. Using different security tools based on the public cloud provider, host OS, or type of cloud (private vs. public), puts a consistent risk mitigation strategy out of practical reach. After all, when there is no single source of truth on security, teams cannot agree on how to prevent malware outbreaks, find and fix misconfigurations, or contain fast-moving threats.
- **Example** – To optimize operational resiliency, some IT Ops teams choose to use multiple cloud providers or combine their use of private and public cloud infrastructure. Without a truly agnostic security policy that can transcend these environments, teams are left with either a patchwork set of controls or are stuck staying with a single cloud service provider or cloud architecture (private or public).
- **What's needed: Unified security** – The goal is to deploy unified security designed for the cloud and applied uniformly, regardless of where the workload is located (public vs. private cloud). Using a single lifecycle management across clouds, workloads and containers enables a consistent and extensive security policy and risk mitigation strategy. For example, using a single platform for vulnerability management, audit and remediation, and endpoint detection and response (EDR) simplifies workload security and empowers collaboration among IT Ops, SecOps and DevOps.

Intrinsic security for cloud workloads

As shown in this paper, using disparate technologies to manage cloud workloads complicates risk and simply is not scalable. At the same time, empowering each team from IT Ops to DevOps and SecOps to use their console of choice is critical. This is not to say that migrating to the cloud requires adoption of an entirely new process, new UI, or management console. After all, these teams already have enough on their plates.

With the VMware intrinsic security approach, deep monitoring and behavioral analysis are implemented at each control point: cloud, workload, endpoint, network and identity, and then unified for full contextual awareness. Like a video camera that records each move at every control point, intrinsic security enables comprehensive contextual awareness. Because there's no need to manually stitch together telemetry from disparate control points, teams can quickly track down threats from the point of entry and every step in between.

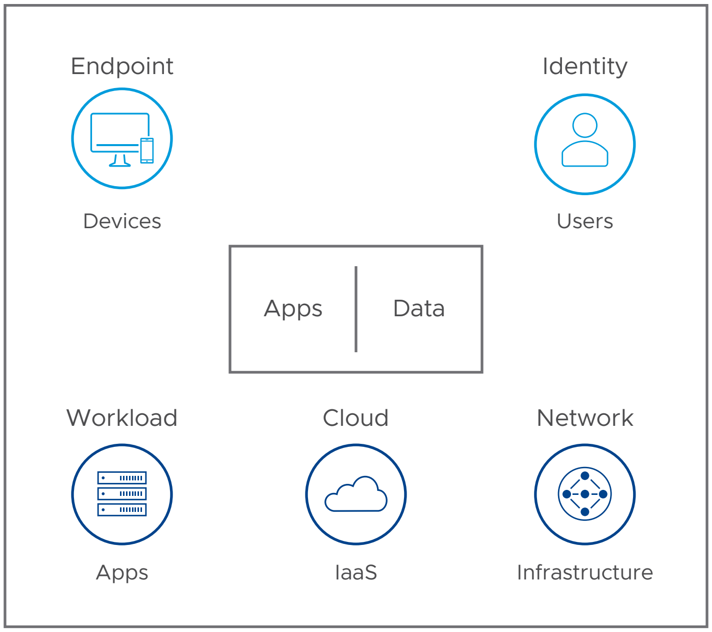

FIGURE 1: The five control points of intrinsic security.

Scalable cloud workload protection

VMware Carbon Black Cloud provides all the functionality for scalable cloud workload protection, and natively integrates with vSphere and NSX. Thanks to this tight integration, vSphere administrators and NSX administrators can access all relevant threat data within the context of their respective domains and within the same console optimized for their own roles.

In addition to providing full contextual awareness within and across clouds, workloads, endpoints, networks and identity, VMware Carbon Black Cloud provides the common system of record for IT Ops, DevOps and SecOps to prevent, detect and remediate threats impacting their critical apps and workloads.

The foundational components of intrinsic security are:

- VMware Carbon Black Cloud
- VMware vSphere
- VMware NSX

VMware Carbon Black Cloud

VMware Carbon Black Cloud is a cloud native, cloud workload protection platform that combines the intelligent system hardening and behavioral prevention needed to keep emerging threats at bay, using a single lifecycle management and an easy-to use console.

VMware vSphere

vSphere is the industry-leading compute virtualization platform, and has been rearchitected with native *Kubernetes* to allow customers to modernize workloads running on vSphere.

VMware NSX Advanced Threat Prevention™

Powered by machine learning, VMware NSX Service-defined Firewall™ delivers network traffic analysis, intrusion detection and prevention, and advance malware analysis with comprehensive network detection and response capabilities.

VMware cloud workload protection: How it works

The VMware intrinsic security approach enables enterprises to protect cloud workloads by utilizing existing infrastructure to proactively identify risks, prevent exploits and exposures, and quickly detect and respond to new and emerging threats.

The three-step process works in the following way, supported by essential security controls.

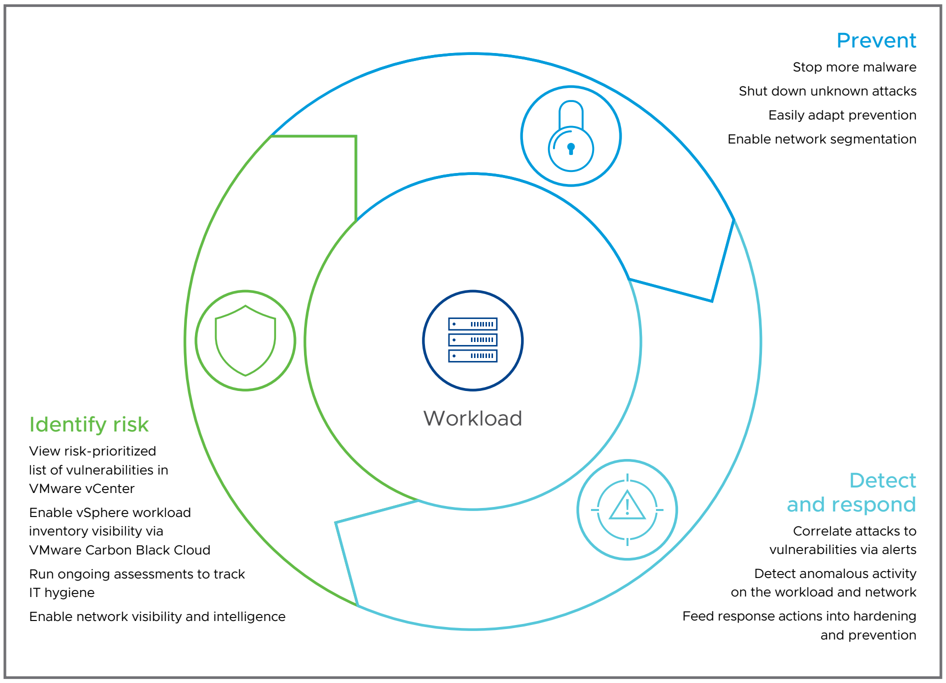
Prevent
Stop more malware
Shut down unknown attacks
Easily adapt prevention
Enable network segmentation
Workload
Identify risk
View risk-prioritized list of vulnerabilities in VMware vCenter
Enable vSphere workload inventory visibility via VMware Carbon Black Cloud
Run ongoing assessments to track IT hygiene
Enable network visibility and intelligence
Detect and respond
Correlate attacks to vulnerabilities via alerts
Detect anomalous activity on the workload and network
Feed response actions into hardening and prevention

FIGURE 2: Intrinsic security for cloud workloads provides comprehensive protection for vSphere workloads.

Step One: Identify risk

- **Initial state integrity check** – VMware Carbon Black Cloud conducts an initial state integrity check to validate the system you're installing the workload on is clean, compliant and appropriate for the type of workload. It will also collect and analyze OS patch levels, assess vulnerabilities and misconfigurations, and determine if additional hardening is required.
- **Ongoing visibility into system state** – VMware Carbon Black Cloud identifies configuration drift, the presence of unknown or unauthorized applications, vulnerabilities, and other dynamic activity that increases the environment's attack surface. For example, it will:
  - – Monitor for any changes that indicate nefarious activity (e.g., zeroing out passwords, changes in BitLocker configuration)
  - – Audit and remediate to query 1,500 artifacts for each workload and endpoint across private and public clouds
  - – Empower admins to run custom SQL queries to look out for specific malicious behavior or activity
- **Ongoing visibility into vulnerabilities and network activity** – VMware Carbon Black Cloud enables vSphere admins to view risk-prioritized workload vulnerabilities in VMware vCenter® and regularly run scan-free vulnerability assessments across workloads. NSX delivers a built-in distributed firewall, so IT Ops teams can monitor communication of workloads across private and public clouds, determine which workloads are part of an app, and determine how to segment unrelated workloads.

Step Two: Prevent risks from escalating

- **Prevent exploits on the workload** – VMware Carbon Black Cloud delivers next-generation antivirus (NGAV) for protection that transcends point-in-time indicators for malware, ransomware, zero-day, rapid variants, suspicious files, and potentially unwanted processes (PUPs) specific to workloads across private and public clouds. The VMware platform combines ransomware decoys, dynamic analysis, and machine learning to provide ongoing analysis that prevents suspicious files from executing.
- **Prevent non-malware attacks** – In addition to blocking malware attacks, VMware Carbon Black Cloud protects against the latest persistent attacks using fileless malware, memory-based, and living-off-the-land (LotL) tactics. These pernicious attacks use existing software and allowlisted apps (e.g., PowerShell), and authorized protocols to carry out malicious activities. Unlike legacy approaches that rely on known threats, the VMware platform can identify new variants and zero-day exploits by piecing together connected behaviors.
- **Prevent network-based attacks** – The NSX Service-defined Firewall protects workloads by mitigating lateral movement and blocking inbound exploits of vulnerable apps and services. With this level of visibility, you can understand how LotL attacks move across the network, identify indicators of compromise (IOCs), and lock down these network connections to isolate workloads from attackers.
- **Customize prevention** – Every environment has different and often competing operational constraints. VMware offers our customers the ability to balance security and operational risks with precise granularity. With the VMware policy engine, you can choose how to mitigate threats based on the specific type of workload, its function, criticality, and adjacency to other critical workloads. For example, to isolate a mission-critical workload, a sysadmin can prevent PowerShell from scraping the memory of another process or invoking an untrusted application.

Step Three: Detect and respond to ongoing risks

- **Know when and where to start an investigation (zoom in)** – Use VMware out-of-the-box automated threat detection via updated threat intelligence from the VMware Threat Analysis Unit™ to pinpoint affected systems and isolate them for remediation. VMware APIs allow you to integrate your own third-party feeds and watchlists, and round out collaborative threat sharing information from VMware's robust user exchange.
- **See the full scope and time frame of the attack (zoom out)** – The VMware platform allows investigators to rewind the tape to understand how an attack unfolded, which systems were affected, and how the attack progressed over time. Because VMware captures all the data (e.g., detailed process activity, process-to-process interaction, parent-child process relationships, etc.), building a detailed timeline without blind spots—well after the fact—empowers incident response and forensic teams to get to the truth.
- **Rapid detect-to-prevent workflow** – In three easy steps, VMware Carbon Black Cloud enables you to translate threat detection into standardized prevention policy across your workloads. First, apply automated policies based on previous detections customized for your workloads. Second, instantly preview the downstream effects of the prevention policy before it's implemented. Third, with a single click, roll out the updated policy across workloads on any environment.

Protecting cloud workloads against a wide variety of threats requires a multipronged approach, one with granular yet unified visibility into all aspects of the computing environment. IT Ops, DevOps and SecOps must work in accord to share the responsibility for securing critical workloads in the cloud. Enterprises that attempt to use traditional approaches to securing hybrid clouds face many challenges, including a lack of visibility into how workloads connect, fragmented processes, and misconfigurations. As discussed in this paper, increasing visibility, speeding recovery, and simplifying security are three key strategies enterprise teams must put into action to mitigate risks.

VMware is uniquely positioned to protect workloads in hybrid clouds. Specifically, VMware solutions enable teams to accurately identify emerging risks to workloads, prevent these risks from escalating further, and quickly contain outbreaks without disrupting operations. While other endpoint and workload security products only collect a dataset related to known bad actors, VMware Carbon Black Cloud continuously collects comprehensive workload, endpoint and network data, and analyzes attackers' behavior patterns to proactively stop attacks before impact. This level of increased operational visibility simplifies security and accelerates system recovery.

While there are many cloud workload protection vendors in the marketplace, not all solutions are the same. Enterprises must consider key requirements, such as design architecture, operational models, and scalability, and ask the right questions to determine how well the platform matches their needs. Use the checklist in Table 2 when considering cloud workload protection platforms. With 100 points to allocate, assign points to each key question as it relates to your organization. The total value of the weighted value column should equal 100. By completing this checklist, you can get a better sense of your key priorities and considerations.

Cloud workload protection platform evaluation checklist

	KEY REQUIREMENT	KEY QUESTIONS	WEIGHTED VALUE
Design architecture	Describe how the cloud workload protection platform visualizes communications and connections between workloads.	Can it consolidate telemetry data across clouds, workloads, networks and endpoints?	
		Does it support every application regardless of OS, configuration and cloud, or is it reliant on any of the above?	
		Can it recognize what constitutes normal behavior within a workload or across workloads?	
		What behavioral models does it deploy to detect malware and non-malware (fileless) attacks within workloads and between workloads?	
Operational model	Describe how the cloud workload protection platform supports alignment and frictionless coordination between IT Ops, DevOps and SecOps to reduce risk, simplify compliance, and increase resilience.	How many agents are required to install on each workload, container and OS?	
		Can IT Ops, DevOps and SecOps leverage the same dataset when monitoring and responding to incidents?	
		Which governance frameworks does your platform support (e.g., NIST 800-53)?	
		How would a typical workflow operate among IT Ops, DevOps and SecOps once a threat, vulnerability or misconfiguration has been identified?	
Scalability	Describe how the cloud workload protection platform supports secure yet rapid change control programs to increase security policy standardization, and reduce misconfiguration risk and other human errors at scale.	What is the average CPU consumption per each cloud workload protection agent?	
		Can it consolidate multiple security capabilities, such as EDR, NGAV, and vulnerability management, into a single agent and management console?	
		Can the cloud workload protection platform enforce and report on a standardized, consistent security policy across private, public and hybrid cloud environments?	
		How does it conduct regular vulnerability scanning without impacting availability and performance?	

TABLE 2: Cloud workload protection evaluation checklist.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com