VMware Carbon Black Cloud Workload for VMware Cloud on AWS

Advanced workload protection for the public cloud

USE CASES

- Cloud workload protection
- Vulnerability management
- Workload auditing for security risks and operational hygiene
- Cloud workload security posture strengthening
- Legacy antivirus replacement on workloads
- Workload behavioral monitoring and endpoint detection and response (EDR)

FEATURES

- Scanless, risk-prioritized vulnerability assessment
- Workload inventory and lifecycle management
- VMware vCenter® plug-in
- Workload behavioral monitoring
- On-demand querying of thousands of workload artifacts
- Next-generation antivirus (NGAV)
- EDR for workloads
- Implementation of ongoing assessments to track IT hygiene over time

As organizations continue their journey toward cloud transformation and application modernization, they require modern security solutions that are both powerful and easy to operationalize. VMware Carbon Black Cloud Workload™ delivers advanced protection purpose-built for securing modern workloads to reduce the attack surface and strengthen security posture both on-premises and in VMware Cloud™ on AWS. This innovative solution combines prioritized vulnerability reporting and foundational workload hardening with industry-leading prevention, detection and response capabilities to protect workloads running in public cloud environments.

Tightly integrated with VMware vSphere running at the core of VMware Cloud on AWS, VMware Carbon Black Cloud Workload provides agentless security that alleviates installation and management overhead, and consolidates the collection of telemetry for multiple workload security use cases.

This unified solution enables security and infrastructure teams to automatically secure new and existing workloads in any environment and at every point in the security lifecycle, while simplifying operations and consolidating the IT and security stack.

Securing workloads in VMware Cloud on AWS

VMware Cloud on AWS is built on the proven security posture of the VMware compute, network and storage stack coupled with the leading public cloud infrastructure provider, Amazon Web Services.

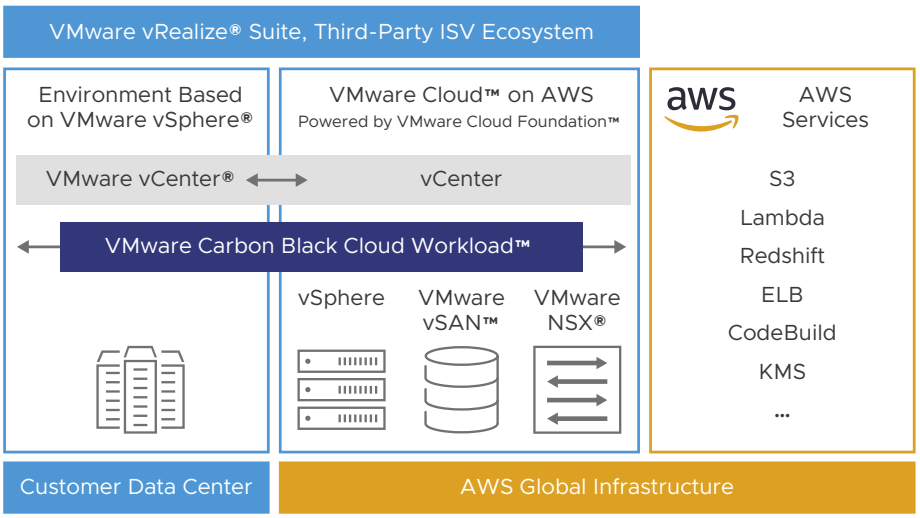

FIGURE 1: Carbon Black Cloud Workload provides agentless security across the VMware Cloud on AWS environment.

BENEFITS FOR INFRASTRUCTURE TEAMS

- Assess vulnerabilities in real time from VMware vSphere® Client™
- Increase patching efficiency with best-in-class prioritization
- Leverage security that's built into your existing infrastructure
- Establish proactive IT hygiene to prevent breaches
- Reduce overhead; no additional infrastructure or heavy scans required
- Replace legacy antivirus on servers to regain compute cycles
- Build consistency into operational reporting and auditing processes

BENEFITS FOR SECURITY TEAMS

- Reduce your organization's attack surface
- Protect workloads from known and unknown attacks
- Reduce complexity by consolidating security tools
- Easily investigate security incidents
- Access lifecycle context to ensure effective protection
- Visualize attack chains in real time
- Speed up mean time to resolution (MTTR)
- Remove barriers between security analysis and IT operations
- Engage with an active user community of internal security experts and peers

While VMware Cloud on AWS already provides consistent operations and security capabilities both on premises and in the cloud, and you can further extend those security capabilities with Carbon Black Cloud Workload. Achieve an additional layer of modern protection and attack surface reduction across your infrastructure.

Identify risk and harden workloads

Carbon Black Cloud Workload helps security and infrastructure teams focus on the most high-risk vulnerabilities and common exploits across all their environments. It's not about finding the most vulnerabilities—it's about finding the right ones. Prioritize vulnerabilities based on a combination of the Common Vulnerability Scoring System (CVSS), real-life exploitability, and real-life frequency of attack. Increase patching efficiency with best-in-class prioritization and take immediate action right from the vSphere Client.

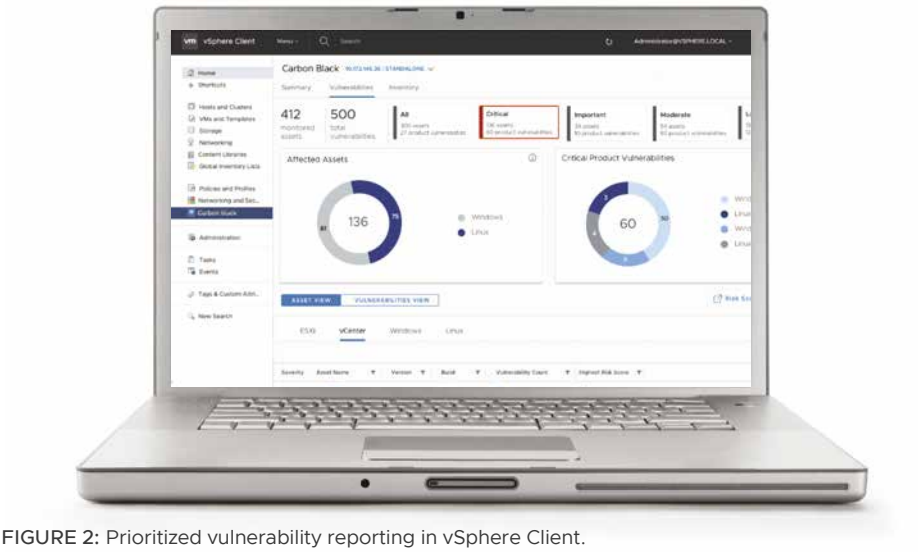

FIGURE 2: Prioritized vulnerability reporting in vSphere Client.

The real-time vulnerability assessment helps security and infrastructure teams understand vulnerability context with risk scores and links to the National Vulnerability Database. It eliminates the need for resource-heavy scans, with no additional administrative overhead or setup. Carbon Black Cloud Workload also provides visibility into operations hygiene; indicators of compromise (IOCs); malicious tactics, techniques and procedures (TTPs); and ordinary events that occur on the system.

vSphere administrators can easily activate workload protection as a feature right from the vSphere Client, with bulk enablement and lifecycle management for virtual machine inventory. The vSphere dashboard provides visibility into appliance health, inventory status, and install workflow, and allows the infrastructure team to see a risk-prioritized list of operating system and application vulnerabilities found across the environment. Carbon Black Cloud Workload enables deeper, unparalleled visibility into your environment to reduce risk and harden workloads, while helping to streamline and operationalize security.

PLATFORMS

- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016
- Windows 2019
- Red Hat 6/7
- CentOS 6/7
- Ubuntu 16/18/19/20
- SLES 12/15

MINIMUM TECHNICAL REQUIREMENTS

- 1- or 3-year subscription to VMware Cloud on AWS
- Internet connection to the VMware Carbon Black Cloud™ platform

LEARN MORE

To set up a personalized demo or for more information, email *contact@carbonblack.com* or visit *carbonblack.com/workload*.

FOR MORE INFORMATION OR TO PURCHASE VMWARE CARBON BLACK PRODUCTS

Call 855-525-2489 in the U.S., or +44 118 908 2374 in EMEA.

Prevent, detect and respond to advanced attacks

Security teams often lack visibility and control in highly dynamic, virtualized data center environments. Carbon Black Cloud Workload protects workloads running in these environments by combining foundational vulnerability assessment and workload hardening with industry-leading NGAV, workload behavioral monitoring, and EDR for workloads.

With advanced workload protection from VMware, security teams can analyze attacker behavior patterns over time to detect and stop never-seen-before attacks, including those manipulating known-good software. If an attacker bypasses perimeter defenses, Carbon Black Cloud Workload empowers security teams to shut down the attack before it escalates to a data breach. By embedding security into the infrastructure, you can easily audit the current system state to track security posture and harden workloads, while enabling easier collaboration with vSphere administrators to address known vulnerabilities.

Simplify operations for IT and security teams

At VMware, we take an intrinsic approach to delivering security—building it into the infrastructure everywhere workloads are deployed. Through this unique approach, we can eliminate the trade-off between security and operational simplicity by providing a single source of truth for infrastructure and security teams to accelerate response to critical vulnerabilities and attacks, while enabling collaboration and reducing friction. Simplify and consolidate your IT and security stack by replacing multiple point security tools that compete for resources with VMware Carbon Black Cloud Workload.

vmware®

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