VMware Carbon Black Workload

Advanced workload security that scales with your business

Powered by VMware Contexa™ cloud-delivered threat intelligence.

Use cases

- Protect cloud and on premises workloads
- Enable workload behavioral monitoring and endpoint detection and response (EDR)
- Prioritize and report on vulnerabilities
- Secure workloads in air-gapped environments
- Audit workloads for security risks and operational hygiene
- Strengthen virtual and cloud infrastructure security posture
- Replace legacy antivirus on servers
- Replace multiple security products to consolidate the IT and security stack

Benefits for security teams

- 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)
- Keep workloads insulated from Internet traffic with the Sensor Gateway
- Engage with an active user community of internal security experts and peers

As organizations accelerate their journey to distributed, multi-cloud environments and cloud native applications, they require modern security solutions that are both powerful and easy to operationalize. VMware Carbon Black Workload™ is a purpose-built, cloud native security solution that enables security teams to detect, prevent and respond to advanced threats. This innovative solution combines deep visibility and workload hardening with industry-leading prevention, detection and response capabilities to protect workloads running in on premises and cloud environments.

Carbon Black Workload collects detailed workload telemetry for multiple security use cases in a single console. This unified solution enables security, infrastructure and cloud teams to automatically secure new and existing workloads at every point in the security lifecycle, while simplifying operations and consolidating the IT and security stack.

Prevent, detect and respond to advanced attacks

Security teams often lack visibility and control in highly dynamic, virtualized and cloud environments. Carbon Black Workload protects workloads running in these environments by increasing visibility and combining foundational vulnerability assessment and workload hardening with industry-leading NGAV, workload behavioral monitoring, and EDR for workloads and containers. With advanced workload protection from VMware, security teams can analyze attacker behavior patterns over time to detect and stop malware and non-malware, ransomware, and never-seen-before attacks, including lateral movement and those manipulating known-good software. If an attacker bypasses perimeter defenses, Carbon Black Workload empowers security teams to shut down the attack before it escalates to a data breach.

Secure public cloud workloads

Carbon Black Workload protects workloads no matter where they reside, including major cloud platforms: AWS, Microsoft Azure and Google Cloud Platform (GCP). This solution provides easier account onboarding, setup and deeper visibility into your public cloud environments with the prevention, detection and response capabilities required to keep public cloud workloads secure.

This powerful solution reduces management overhead and makes account management easier with single and multiple account management modes. Carbon Black Workload provides flexible options to enable security for all public cloud workloads, including auto-generated continuous integration and continuous deployment (CI/CD) using Chef, Puppet, Ansible

Benefits for infrastructure teams

- 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

Features

- NGAV and EDR for workloads
- Easy account onboarding for public cloud workloads
- VMware vCenter® plug-in for VMware vSphere and VMware Cloud workloads
- CIS Benchmarking
- Optional Sensor Gateway for air-gapped environments
- On-demand querying of thousands of workload artifacts
- Scanless, risk-prioritized vulnerability assessment
- Workload inventory and lifecycle management
- Workload behavioral monitoring
- Consumption dashboard to track workload license usage
- Optional MDR services

and more. Security teams can't protect what they can't see, so Carbon Black Workload provides full visibility into all VMs and Amazon Elastic Compute Cloud (EC2) instances, a rich set of metadata, management of ephemeral instances, and management functions such as search and export.

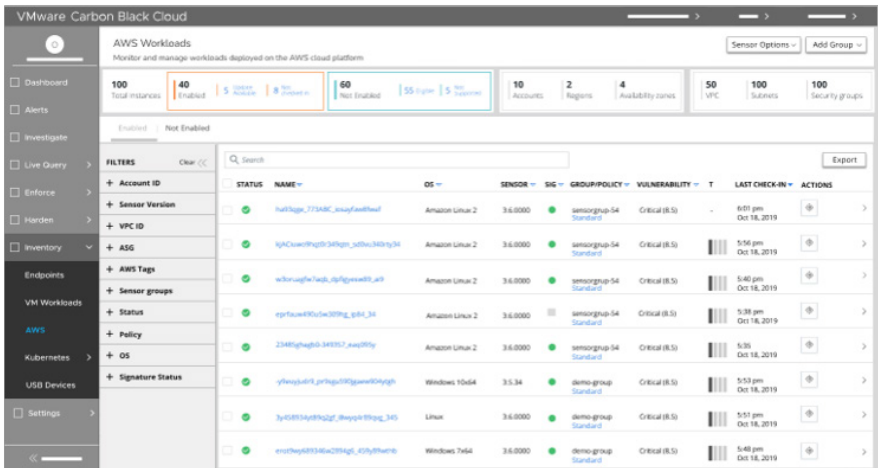

Figure 1: Unified visibility into all workloads across private, public and hybrid clouds.

Secure virtual and private cloud workloads

Security teams can take advantage of the VMware Carbon Black Cloud™ platform to extend your security program to virtualized and cloud workloads running on VMware vSphere™ and VMware Cloud™ from a single console. Security operations center (SOC) teams can prevent, detect and respond to threats targeting your organization's most critical assets with next-generation antivirus (NGAV) that is certified to replace legacy antivirus, combined with industry-leading detection and response capabilities. Managed detection and response (MDR) services for workloads are also available to help organizations scale their security program.

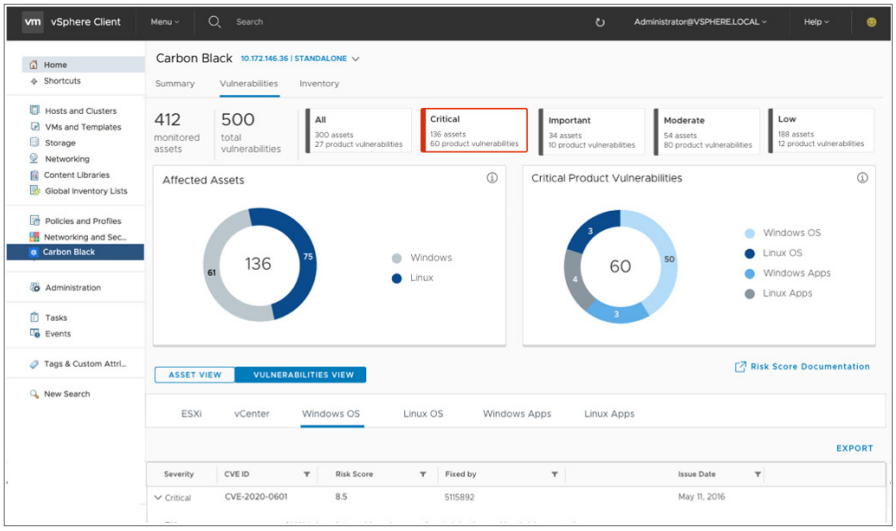

Figure 2: Scanless, risk-prioritized vulnerability reporting in the vSphere Client console.

Platforms

- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016
- Windows 2019
- Windows 2022
- RHEL/CentOS 6/7
- Ubuntu 16/18/19/20
- SLES 12/15
- Amazon Linux 2
- Microsoft Azure
- Google Cloud Platform

Minimum technical requirements

Internet connection to VMware Carbon Black Cloud

Learn more

For additional information, visit the VMware Carbon Black Workload product page.

For more information or to purchase VMware Carbon Black products, please call 855-525-2489 in the U.S., +44 118 908 2374 in EMEA.

vSphere and VMware Cloud administrators can easily activate workload protection as a feature right from the vSphere Client or VMware Cloud console, with bulk enablement and lifecycle management for virtual machine inventory. Carbon Black Workload enables deeper, unparalleled visibility into your environment to reduce risk and harden workloads, while helping streamline and operationalize security.

Manage risk and harden workloads

Carbon Black Workload helps security and infrastructure teams reduce their organization's attack surface with workload hardening, compliance reporting and vulnerability prioritization. By embedding security into the infrastructure, security teams can easily audit the current system state to track security posture and harden workloads, while enabling easier collaboration with infrastructure and cloud administrators to address critical vulnerabilities. By bringing CIS Benchmarks as a feature into Carbon Black Workload, teams can measure and report on the compliance of organizational workload assets against industry standard benchmarks published by the Center for Internet Security (CIS).

Simplify operations for security, IT and cloud 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 operation simplicity by providing a single source of truth for teams to accelerate response to critical vulnerabilities and attacks, while enabling collaboration and reducing friction. With shared visibility into critical vulnerabilities, IT hygiene and compliance reporting, infrastructure and security teams can collaborate more effectively to reduce risk and respond faster to threats. Furthering efficiency, users can access a dashboard that tracks their workload consumption across all devices and at various intervals. This allows teams to make informed decisions about their Carbon Black Workload licensing and the state of the business. Simplify and consolidate your IT and security stack by replacing multiple point security tools that compete for resources, with Carbon Black Workload.

Item No: VMware Carbon Black Workload Datasheet 8.1.23 8/23