VMware Carbon Black Workload

Advanced cloud native workload security that scales with your business

Powered by VMware Contexa™ cloud-delivered threat intelligence.

Use cases

- Protect cloud workloads
- Enable workload behavioral monitoring and endpoint detection and response (EDR)
- Prioritize and report on vulnerabilities
- 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)
- Remove barriers between security analysis and IT operations
- 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 strengthens security posture and reduces risk. This innovative solution combines prioritized vulnerability reporting and workload hardening with industry-leading prevention, detection and response capabilities to protect workloads running in private, public and hybrid cloud environments.

VMware 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.

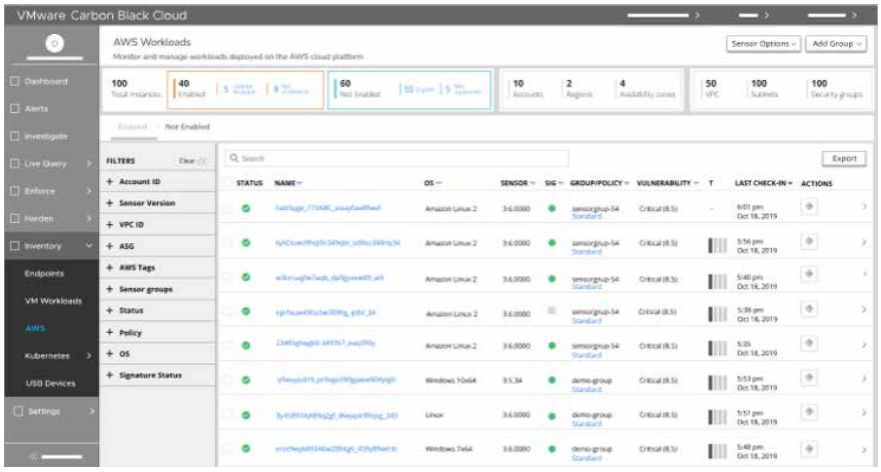

Figure 1: Unified visibility into all workloads across private, public and hybrid clouds.

Secure public cloud workloads

VMware Carbon Black Workload provides easier onboarding, setup and deeper visibility into your AWS environment 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. VMware Carbon Black Workload provides flexible options to enable security for AWS workloads, including auto-generated continuous integration and continuous deployment (CI/CD) using Chef, Puppet, Ansible and more.

Benefits for infrastructure teams

- Assess application and OS vulnerabilities in near real time from the VMware vSphere® Client™ or VMware Cloud™ console
- 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

- Powered by VMware Contexa cloud-delivered threat intelligence
- Scanless, risk-prioritized vulnerability assessment
- Workload inventory and lifecycle management
- VMware vCenter® plug-in for vSphere and VMware Cloud workloads
- Easy AWS account onboarding for public cloud workloads
- Workload behavioral monitoring
- Implementation of ongoing assessments to track IT hygiene over time
- On-demand querying of thousands of workload artifacts
- Optional NGAV
- Optional EDR and threat hunting for workloads
- Optional MDR services

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

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's 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.

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. VMware Carbon Black Workload enables deeper, unparalleled visibility into your environment to reduce risk and harden workloads, while helping streamline and operationalize security.

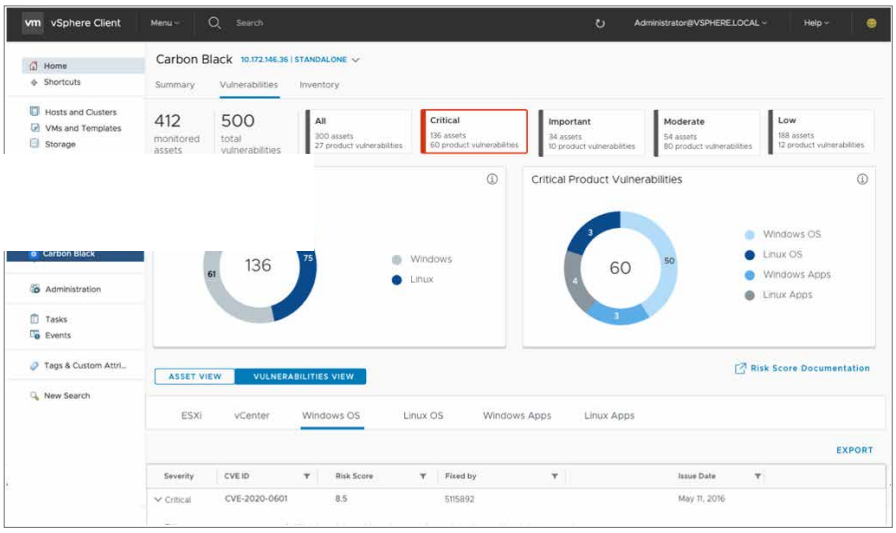

Figure 2: Scanless, risk-prioritized vulnerability reporting in the vSphere Client console.

Manage risk and harden workloads

VMware 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.

Platforms

- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016
- Windows 2019
- RHEL/CentOS 6/7
- Ubuntu 16/18/19/20
- SLES 12/15
- Amazon Linux 2

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.

With VMware Carbon Black Workload, infrastructure and cloud teams can focus on the most high-risk vulnerabilities and common exploits across their environments because it's not about finding the most vulnerabilities—it's about finding the right ones. Increase patching efficiency and focus on the most critical vulnerabilities with best-in-class prioritization using a combination of the Common Vulnerability Scoring System (CVSS), real-life exploitability, and frequency of attack. Powerful audit and remediation capabilities also allow security and IT teams to query thousands of workload artifacts on demand and generate compliance reports to establish proactive IT hygiene practices and prevent breaches.

Prevent, detect and respond to advanced attacks

Security teams often lack visibility and control in highly dynamic, virtualized and cloud environments. VMware 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. 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, VMware Carbon Black Workload empowers security teams to shut down the attack before it escalates to a data breach.

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 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. 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. Simplify and consolidate your IT and security stack by replacing multiple point security tools that compete for resources with VMware Carbon Black Workload.

Powered by VMware Contexa

VMware Contexa demystifies machine learning with the use of the VMware Carbon Black® dynamic rules engine that scales and supports rapid innovation, enabling future-ready security. As new adversarial techniques emerge, VMware Contexa recursively identifies historic triggers, builds detection and prevention logic based on your environment, and deploys enforcement without the need for any administrative action, which accelerates resolution when you encounter indicators of compromise. VMware Contexa currently identifies active network exploits at a daily rate of 80,000 exploits, including Log4Shell and other moderate to critical exploits. Each day, nearly 2 million files are further analyzed, resulting in more than 1 million ransomware attack preventions every 90 days.