VMware Carbon Black Workload and Cloud Configuration

Powered by VMware Contexa™ cloud-delivered threat intelligence

Use cases

- Next-generation antivirus (NGAV) and endpoint detection and response (EDR) for workloads
- Cloud security posture management
- Kubernetes security posture management
- Vulnerability assessment
- Center for Internet Security (CIS) benchmarking
- Continuous compliance
- Threat correlation

Security designed for cloud native architecture

As organizations continue to migrate workloads to public clouds, modernize their applications, and adopt cloud native practices at a rapid pace, the attack surface grows exponentially. Yet, traditional security tools and practices are not effective in complex, cloud native environments. To reduce misconfigurations, detect malicious activity, and prevent unauthorized access, organizations need a unified, cloud-smart solution that provides consistent visibility, control and security across clouds.

VMware Carbon Black® Workload and Cloud Configuration™ combines real-time cloud security posture management (CSPM), entitlement visibility, Kubernetes security, threat prevention (NGAV), and advanced detection and response capabilities for workloads (EDR) to deliver a more integrated approach to cloud security. This comprehensive solution enables cloud security teams to identify and reduce risk through configuration and posture management, prevent breaches, and respond to attacks faster to keep cloud workloads and resources secure.

Cloud configuration security and compliance

VMware Aria Automation™ for Secure Clouds is a real-time, contextual cloud configuration security platform that enables IT and developer teams to reduce misconfiguration risk across public cloud and Kubernetes infrastructure. The solution enables you to prioritize and investigate security violations with near real-time graph search, allowing visualization of resource relationships. Advanced rules help correlate risk due to resource relationships and entitlements with misconfigurations and threat activity. As your cloud footprint grows, you can operationalize security at scale by automating actions, such as alerts, suppressions and remediation, based on predefined criteria.

Foundational to VMware Aria Automation for Secure Clouds is an interconnected cloud security model (see Figure 1), an intermediate data layer that leverages cloud APIs, change events, and native threat data to help organizations model an entire multi-cloud environment in a single place. To this data layer, the service applies predefined security and compliance benchmarks as well as organization-specific custom rules to surface violations that increase risk.

Solution benefits

- Achieve unprecedented visibility into cloud resources and workloads to proactively reduce attack surface
- Gain a comprehensive understanding of security and compliance posture with support for more than 350 cloud resources, 1,100 rules, and 20 compliance frameworks across Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and Kubernetes
- Find risks that others overlook by visualizing and correlating resource relationships with misconfigurations, entitlements and threats
- Speed investigation and response to security threats, and identify excessive privileges across cloud infrastructure
- Detect 95 percent of security violations in less than 6 seconds of a change notification and automate remediation securely
- Protect cloud and Kubernetes resources at scale with fewer false positives and automated workflows
- Benchmark compliance across ephemeral cloud resources with predefined industry standards or organization-specific custom frameworks
- Auto-remediate clouds without elevated permissions granted to the service
- Integrate security and compliance earlier in the development lifecycle

This data model enables information security, operations and application teams to quickly visualize misconfigured resources, connected cloud assets, excessive permissions, and historical changes to get a better understanding of overall risk. As objects, data and relationships change, the service intelligently detects new violations and threats in near real time.

IT administrators can distribute security and compliance insights across application owners at real-time speed. Application teams get easy access to security findings with contextual alerts and initiate actions via the cloud provider console, automated remediations, or security verification during continuous integration and continuous deployment (CI/CD) pipelines.

With VMware Aria Automation for Secure Clouds, you can:

- Reduce security investigation time from days to minutes with real-time graph search that enables you to visualize resource relationships.
- Mitigate cloud risk with real-time misconfiguration detection, infrastructure context, and automated actions. Secure managed and self-managed Kubernetes infrastructure, including insight into access to sensitive cloud credentials.
- Benchmark compliance across ephemeral cloud resources with predefined industry standards or organization-specific custom frameworks.
- Gain visibility into principals and their entitlements to cloud resources to identify sensitive access conditions.
- Prioritize response to critical threats by correlating anomalies with risky misconfigurations.
- Integrate security and compliance best practices within CI/CD pipelines to proactively identify and remediate violations before a deployment hits production.

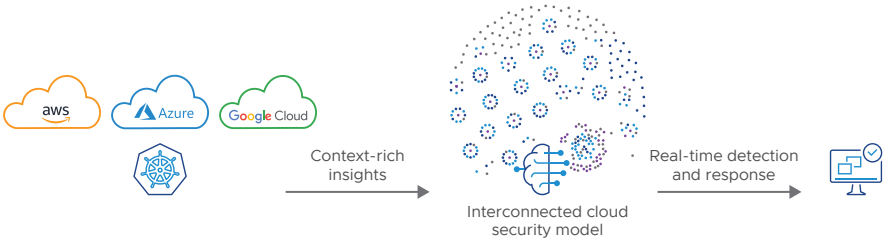

Figure 1: The interconnected cloud security model of VMware Aria Automation for Secure Clouds.

Features

- Near real-time public cloud inventory and cloud posture detection
- Stop malware, fileless, ransomware, and living-off-the-land attacks
- Out-of-the-box customizable prevention policies
- Visibility into entire attack chain for easy investigation
- Threat detection and response
- Workload behavioral monitoring
- Cloud-delivered threat intelligence
- CIS benchmark compliance
- Automated and prioritized vulnerability assessment
- Auto-generated CI/CD

Supported 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
- Google Cloud Platform
- Microsoft Azure
- Kubernetes (managed and self-managed)
- Amazon Web Services

Advanced cloud workload protection

Security teams can't protect what they can't see, yet they often lack visibility and control in highly dynamic cloud environments. VMware Carbon Black Workload™ protects cloud workloads by combining industry-leading prevention (NGAV) and detection and response (EDR) with deep visibility and workload hardening to detect, prevent and respond to threats faster. Security teams can analyze attacker behavior patterns over time to detect and stop 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 prevent the attack before it escalates to a data breach.

VMware Carbon Black Workload enables 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. This reduces operational overhead and makes account management easier with single and multiple account management modes. VMware Carbon Black Workload also provides flexible deployment options aligned with cloud native and DevOps standards to make it easy to enable security for cloud workloads, including auto-generated CI/CD using Chef, Puppet, Ansible and more.

With VMware Carbon Black Workload, you can:

- Block known and unknown attacks, including malware, ransomware, and living-off-the-land attacks.
- Stop more malware by combining exploit prevention, machine learning, and file reputation, and access lifecycle context to ensure effective protection.
- Detect anomalous activity with threat intelligence and frequency analysis, and feed response actions directly back into hardening and prevention.
- Leverage industry-leading detection and response capabilities, and enhance visibility with highlighted suspicious workload events.
- Easily investigate security incidents and visualize attack chains in real time to speed response.
- Proactively reduce the attack surface with automated compliance reporting and prioritization of vulnerabilities and misconfigurations.
- Enforce compliance and industry best practices.

VMware Carbon Black Workload provides the advanced prevention, detection and response capabilities required to keep cloud workloads secure, with easy onboarding, setup and deep visibility into cloud environments.

Minimal technical requirements

- Read-only cloud account role for all accounts managed using VMware Aria Automation for Secure Clouds
- Access to VMware Carbon Black Cloud™

Learn more

For more information or to purchase VMware products, call 877-4-VMWARE (outside North America, +1-650-427-5000).

Read our customer stories to learn how others are using VMware solutions.

Visit the VMware Carbon Black Workload product page.

Visit the VMware Aria Automation for Secure Clouds product page.

Read posts on the VMware Security Blog.

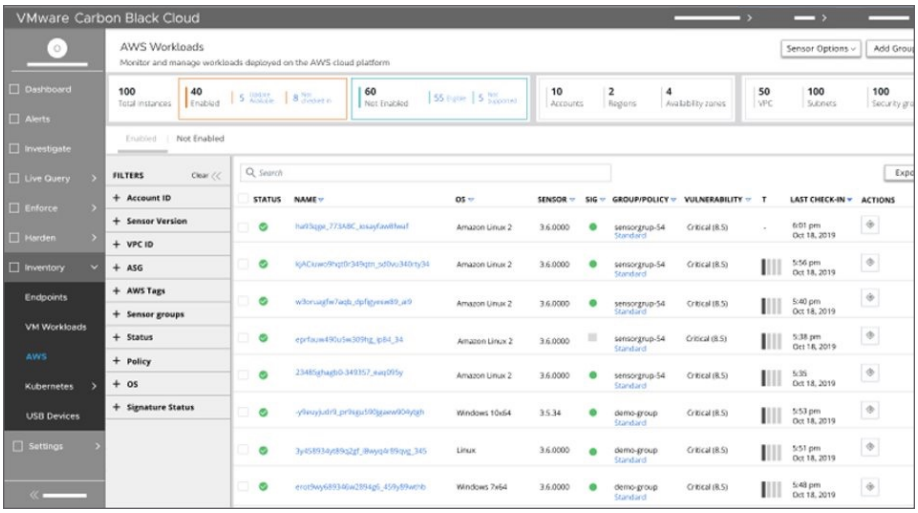

Figure 2: Unified visibility and actionable insights into all cloud workloads.

The future of cloud security with VMware Carbon Black Workload and Cloud Configuration

Securing cloud workloads and resource configurations is challenging for security and cloud teams in dynamic multi-cloud environments. 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. Take a proactive stance against lateral movement and privilege escalation in the cloud with VMware's cloud workload protection and cloud posture solutions, and enable your cloud native applications to be secure throughout their lifecycle, inside and out.

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.

Item No: 1913634aq-so-crbn-black-wkld-cld-config-uslet 3/23