Mware Carbon Black Cloud Audit and Remediation

Real-Time Device Assessment & Remediation

Even the most effective security teams are often forced to play catch up during emergency situations due to limited time and resources to perform regular, proactive analysis and evaluate potential risks.

Any delays during the investigation prolongs downtime and leaves the organization open to increased risk. Once the scope of an attack is understood, dispersed processes and tool sets can cause bottlenecks that delay the remediation of problematic endpoints.

VMware Carbon Black Audit and Remediation is a real-time assessment and remediation solution that gives teams faster, easier access to audit and change the system state of endpoints across their organization.

By providing administrators with real-time query capabilities from a cloud-native endpoint protection platform, Audit and Remediation enables teams to make quick, confident decisions to harden systems and improve security posture. Audit and Remediation closes the gap between security and operations, allowing administrators to perform full investigations and take action to remotely remediate endpoints all from a single solution.

"Carbon Black enables our incident response team to acquire key forensic artifacts that normally would require additional collection and offline parsing. It allows our teams to scale out our response from one to hundreds of systems."

TIM STILLER, SENIOR INCIDENT RESPONSE CONSULTANT, RAPID7



USE CASES

- Maintain IT Hygiene & Track Drift
- \cdot Assess Vulnerabilities in Real Time
- Prove & Maintain Compliance
- Confidently Respond to Incidents
- Audit & Protect Production Workloads

BENEFITS

- Execute abroad range of operational activities quickly and confidently
- Establish proactive IT hygiene to prevent attacks
- Build consistency into operational reporting and auditing processes
- Remove barriers between security analysis and IT operations
- Extend existing investigation and remediation capabilities
- Replace adhoc scripts and manual tasks with a structured security platform
- Automate operational reporting
 with scheduled queries

AUDIT AND REMEDIATION

- Leverages the same agenta nd console as NGAV, EDR and threat hunting platform
- · Cloud-based storage of all query results
- Easy access to unified data across Security and IT teams

VMWare[®] Carbon Black

FEATURES

- Pre-Built Recommended Queries
- SQL query (open text field)
- · Query Scheduler
- · Copy & Re-run Queries
- \cdot Save and favorite queries
- Email notifications
- Filter and group results
- \cdot Data export
- · Secure shell for remote remediation
- Two-way API

PLATFORMS

- \cdot Windows 7 and above
- Windows Server 2008 R2 and above
- MacOS 10.10 and above
- \cdot RedHat 6 and above
- \cdot CentOS 6 and above
- Ubuntu 16.04 and above
- · SUSE 12 and above
- OpenS USE 15 & 42
- Amazon Linux 2

LEARN MORE

To set up a personalized demo or try it free in your organization, visit *CarbonBlack/trial*

For more information or to purchase VMware Carbon Black Products please call: (855) 525-2489 in the US, (44) 118 908 2374 in EMEA

For more information, email Contact@CarbonBlack.com or visit CarbonBlack.com/epp-cloud

Key Capabilities

Single Agent, Cloud Platform

Audit and Remediation is built on the PSC, a cloud-native endpoint protection platform that offers converged prevention, detection, and response with additional services that can be activated as you need them, using the same converged agent, without any additional deployment or infrastructure.

On-Demand Queries

Audit and Remediation gives your Security & IT Operations team visibility into even the most precise about the current system state of all endpoints, enabling you to make quick, confident decisions to reduce risk.

Immediate Remote Remediation

Audit and Remediation closes the gap between security and operations, giving administrators a remote shell directly into endpoints to perform full investigations and remote remediations all from a single cloud-based platform.

Simplified Operational Reporting

Audit and Remediation allows you to schedule daily, weekly, or monthly queries to automate operational reporting on patch levels, user privileges, disk encryption status and more to track & maintain the desired state of your ever-changing environment.

all DASHBOARD	Recommended 50, Query Visit the Query Data
▲ ALERTS ♦ INVESTIGATE	Al If Ngleer University Management (14)
C IVE QUERY >	🛃 Engli me a sum any of query results. 🛛 🔿
G ENLORCE +	Queries non against all endpoints by default. However, you can select a specific policy or endpoints,
D ENDPOINTS	COMPLANCE
⊜ settines →	Authorized SSH Keys
	Designs The Adverse (App, the th this a stack for the canonic which wave an ing transit in years. Image: The Adverse (App, the th this a stack for the strapt system). Designs The Adverse (App, the th this a stack for the strapt system). Designs The Adverse (App, the this a stack for the strapt system).
	IT INSIDE
	AWS EC2 Instance Tags
	Designer Net ARAD C2 relative figure pay of law stream. € Read: Unit binary stream. € Read: A stream. €
	17 MIGM
	AWS EC2 Metadata Information
	Dennjem i mater endela delago je ka negl po z vonig (12 histore. Intera: Unite Al Constante interante anyor Lina wane. Au: A vendel €
	COMPLIANCE
	BitLocker Cenfiguration Details
	Derrights - Malan to Million face. It derright ynar val val de la Derrights - Derlan en Nalan en Nalan face face erget ynan it de la dere B. Generale erstytter webel. Aus - Besty Besty

FIGURE 1: Audit and Remediation gives administrators across the SecOps team the ability to easily create custom queries and return results from across all endpoints in their environment to a single cloud- based console.

VMWare[®] Carbon Black

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Copyright © 2020 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware and Carbon Black are registered trademarks or trademarks of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.