VMware Carbon Black Cloud Managed Detection and Response

Use cases

- Support for handling security alerts
- An extra set of eyes on your environment
- Security experts supplement your team
- Security incident support

Benefits

- More efficient and proactive security operations
- More actionable alerts, reducing alert fatigue
- Notifications provide analysts with valuable threat intelligence and the policy changes needed to mitigate threats
- Reduced time spent investigating root cause
- Alleviation of staffing pressures with 24x7 support
- Monthly reports provide analysts with insight into threats in their environment to inform leadership
- Clearer view of security trends to help guide policy
- Interactive communication with security analysts during incident response
- Threat containment

As enterprises face a shortage of skilled security professionals, your security teams often spend too much time monitoring and validating alerts, which limits their ability to address other security needs. Even more concerning, when attacks occur, many security analysts are limited by the tools and data available for analysis in their own environment. This is compounded by lack of visibility and context into the history of the event.

VMware Carbon Black Cloud Managed Detection and Response™ provides critical insight into attacks with recommendations for the policy changes you need to remediate the threat. Managed detection and response analysts notify you via email of threats and provide specific policy changes to address the threat in VMware Carbon Black Cloud™. In addition, analysts are available to provide you with incident remediation guidance as well as threat containment during an incident.

Built directly on the VMware Carbon Black Cloud platform, Carbon Black Cloud Managed Detection and Response is supported by a world-class team of security experts who monitor and analyze the data in VMware Carbon Black Cloud using advanced machine learning (ML) and algorithmic tool sets.

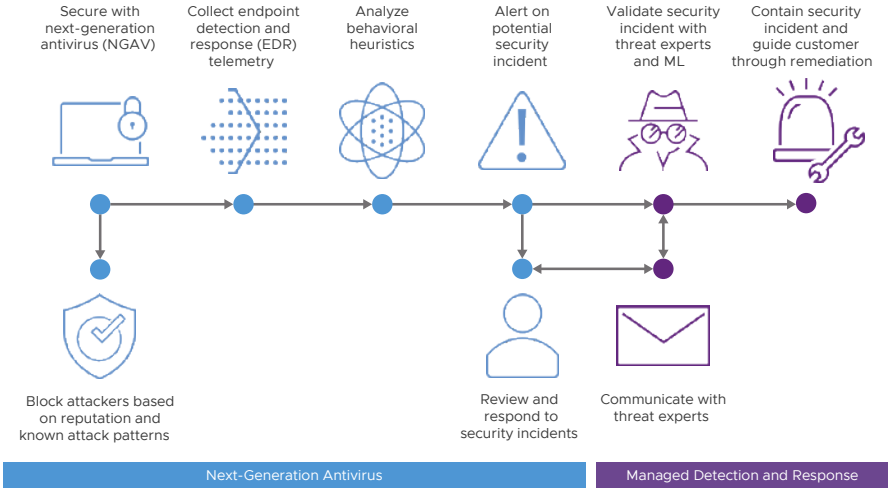

Figure 1: Carbon Black Cloud Managed Detection and Response process flow.

"Another kudo for VMware Carbon Black. I follow the Carbon Black Cloud Managed Detection recommendations immediately, and it is already working. [They are] a superior team."

Chuck Baldwin
IT Administrator
Integra Technologies

Managed detection and response and VMware Carbon Black Cloud

- Human analysts use the unfiltered data from VMware Carbon Black Cloud to hunt evasive threats
- Global threat intel allows us to see attack trends before they hit you
- Monthly reports provide additional insights about your environment

Features

- Threat validation
- Email alerts
- Root cause analysis
- Threat advisories
- Monthly reports
- Incident response communication with analysts
- Threat containment

Protect endpoints with VMware Carbon Black Cloud

Transform your endpoint security with intelligent protection that adapts to your needs. Our cloud native protection platform combines the intelligent system hardening and behavioral prevention needed to keep emerging threats at bay, using a single, easy-to-use console. By analyzing more than 1 trillion security events per day, VMware Carbon Black Cloud proactively uncovers attackers' behavior patterns and empowers defenders to detect and stop emerging attacks.

Most of today's cyberattacks now encompass tactics such as lateral movement, island hopping, and destructive attacks. Advanced hacking capabilities and services for sale on the dark web compound the issue. These realities pose a tremendous risk to targets with decentralized systems protecting high-value assets, including money, intellectual property, and state secrets.

Legacy approaches to prevention leave organizations exposed. Cybercriminals constantly update tactics and obscure their actions within common tools and processes. You need an endpoint protection platform that helps you spot the minor fluctuations that hide malicious attacks and adapt prevention in response.

While other security products only collect a dataset related to known bads, we continuously collect activity data because attackers intentionally try to look normal to hide their attacks. We analyze attackers' behavior patterns to detect and stop never-seen-before attacks.

Protect workloads with VMware Carbon Black Cloud

As organizations continue their journey toward cloud transformation and application modernization, they require modern security solutions that are 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.

This innovative solution combines prioritized vulnerability reporting and foundational workload hardening with industry-leading prevention, detection and response capabilities to protect workloads running in virtualized, private and hybrid cloud environments. Reduce your attack surface and protect critical assets with purpose-built workload protection for the modern data center.

Tightly integrated with VMware vSphere®, Carbon Black Cloud Workload provides a seamless lifecycle management experience leveraging VMware Tools™. This 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 at every point in the security lifecycle, while simplifying operations and consolidating the IT and security stack.

Replace multiple security tools and agents, and simplify operations across IT and security teams with workload protection built for today's needs. With advanced workload protection from VMware, you can block both known and unknown advanced attacks, including malware, fileless and living-off-the-land attacks, while providing a single source of truth to enable collaboration, reduce friction, and accelerate incident response.

Key capabilities

Threat validation and insight

With 24x7x365 coverage, your team can have true peace of mind knowing that nothing will slip through the cracks. VMware's security experts proactively validate alerts and send email notifications, helping assure that your team doesn't miss the alerts that matter.

Roadmap to root cause

Carbon Black Cloud Managed Detection and Response provides additional, analyst insight to VMware Carbon Black Cloud Endpoint™ Standard and Carbon Black Cloud Workload alerts, such as connecting alerts caused by the same root cause to help you streamline investigations and resolve security issues.

Outbreak advisories

The VMware Threat Analysis Unit™ constantly monitors threat trends across the globe. When widespread and newsworthy outbreaks occur, our team sends out advisories that include indicators of compromise, giving your team a jump-start on assessing risk and closing gaps.

Monthly reporting

Our managed detection experts provide monthly reports that summarize activity across your environment, including the most common suspicious events and most targeted machines. These reports provide a starting point for refining policies, help your team see big-picture trends, and make reporting effortless.

Incident response communication with analysts

In the event of a security incident, you are not alone. Our security analysts are available 24x7 to guide customers' security and IT teams through their incident remediation with two-way communication via email.

Threat containment

Our analysts use the powerful tools available in VMware Carbon Black Cloud to quickly stop threats from escalating by updating reputations of hashes, modifying behavioral prevention rules, and quarantining the device on the network.

For more information or to purchase VMware products

Call 877-4-VMWARE (outside North America, +1-650-427-5000), visit vmware.com/products, or search online for an authorized reseller. For detailed product specifications and system requirements, refer to the VMware Carbon Black Cloud Managed Detection documentation.

Get started

VMware Carbon Black Cloud Managed Detection and Response is available for any current Carbon Black Cloud Endpoint or Carbon Black Cloud Workload customer.

Related products

For more information on VMware Carbon Black Cloud, please visit vmware.com/products/carbon-black-cloud.

For more information on VMware Carbon Black Cloud Endpoint, please visit vmware.com/products/carbon-black-cloud-endpoint.

For more information on VMware Carbon Black Cloud Workload, please visit vmware.com/products/carbon-black-cloud-workload.

Item No: 1153675aq-ds-crbn-black-mngd-dtcn-rspn-a4 11/21