

## VMware Carbon Black Cloud

# Managed Detection

## Monitoring and Alert Triage

### USE CASES

- Support for handling security alerts
- Extra set of eyes on your environment
- Security experts supplementing your team

### BENEFITS

- More efficient and proactive security operations
- More actionable alerts, reducing alert fatigue
- Notifications provide analysts with the information needed to keep their leadership aware of threats and mitigations.
- Reduced time spent investigating root cause
- Alleviation of staffing pressures with 24x7 support
- Clearer view of security trends to help guide policy

### MANAGED DETECTION AND THE CARBON BLACK CLOUD

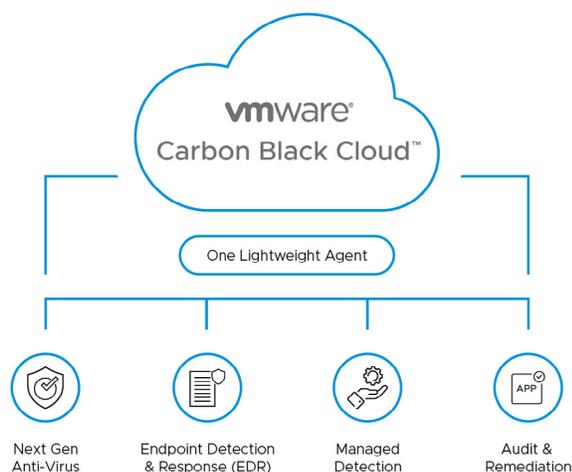
- Human analysts use the Carbon Black Cloud's unfiltered data to hunt evasive threats
- Global threat intel allows us to see attack trends before they hit you
- Monthly reports provide additional insights about your environment

As enterprises face a shortage of skilled security professionals, 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 into the history of the event.

Carbon Black Cloud Managed Detection provides a much needed view into attacks with recommendations for the policy changes needed to remediate the threat. Managed Detection Analysts notify service subscribers via email of threats and provide specific policy changes to address the threat in Carbon Black Cloud Next Gen AV and Behavioral EDR. Built directly on the Carbon Black Cloud platform, CB Managed Detection is staffed by a world-class team of security experts who monitor and analyze the data in the Carbon Black Cloud using advanced machine learning and algorithmic tool sets.

Offered as a managed service, Managed Detection provides a world-class team of Carbon Black security experts who with your organization to validate and prioritize alerts, uncover new threats and accelerate investigations.

### Cloud-Native Endpoint Protection Program



“Another kudo for Carbon Black. I follow Carbon Black Managed Detection’s recommendations immediately and it is already working. [They are] a superior team.”

– CHUCK BALDWIN, IT ADMINISTRATOR, INTEGRA TECHNOLOGIES

### FEATURES

- Threat validation
- Email alerts
- Root cause analysis
- Threat advisories
- Monthly reports

### PLATFORMS

Carbon Black Managed Detection is an add-on service to Carbon Black NGAV and Behavioral EDR, which supports:

Windows:	Windows 7/8/10
Mac OS X:	10.6.8+
Server:	Windows 2008 Windows 2012 Windows 2016

### LEARN MORE

To set up a personalized demo or try it free in your organization, visit [CarbonBlack.com/trial](https://CarbonBlack.com/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](mailto:Contact@CarbonBlack.com) or visit [CarbonBlack.com/epp-cloud](https://CarbonBlack.com/epp-cloud)

### 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. Carbon Black's security experts proactively validate alerts and send email notifications, helping to assure that your team doesn't miss the alerts that matter.

#### Roadmap to Root Cause

Carbon Black Managed Detection provides additional, human-generated context to Carbon Black NGAV and Behavioral EDR alerts, such as connecting alerts caused by the same root cause, to help you streamline investigations and resolve security issues.

#### Outbreak Advisories

Carbon Black's 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 Carbon Black 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.

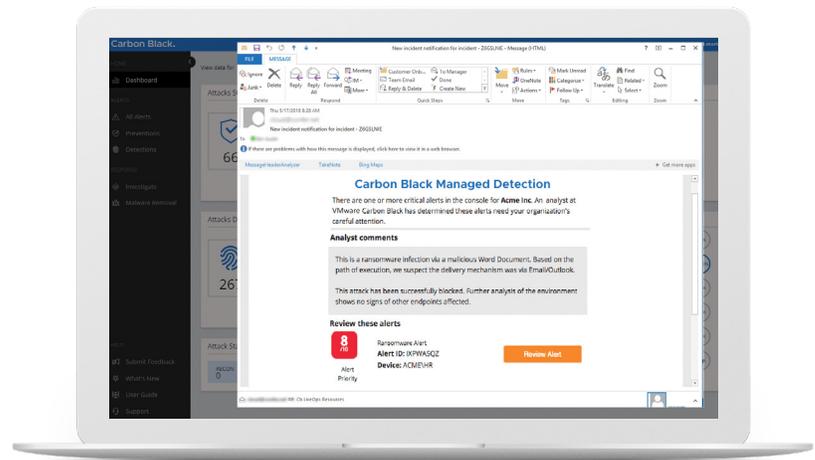


FIGURE 2: When the Managed Detection team validates a true threat, they immediately notify your administrators and provide additional context to help streamline investigations and resolve issues faster.