DELL Technologies

Dell SafeGuard and Response

VMware Carbon Black Cloud Managed Detection and Response™

BENEFITS

- Efficient and proactive security operations without adding direct staff
- Identify the most important alerts, reducing alert fatigue
- Notifications provide analysts with information needed to keep leadership aware of threats, policy changes, and mitigations
- Reduced time spent investigating root cause
- Alleviate staffing pressures with 24x7 support
- Monthly reports provide analysts with insight into threats to inform leadership
- Clearer view of security trends to help guide policy
- Interactive communication with security analysts during incident response
- Threat containment

FEATURES

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

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 you to see attack trends before they impact your organization
- Monthly reports provide additional insights about your environment

Monitoring, Detection, Alert Triage and Response

Even with the continuing shortage of skilled security professionals, security teams often spend too much time monitoring and validating alerts, which limits their ability to address more important security needs. What's more concerning is that when attacks occur, many security analysts are limited by the tools and data available for analysis in their environment. This is compounded by lack of visibility and context into the history of the event.

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

Leveraging the VMware Carbon Black Cloud platform, these experts monitor and analyze the data in VMware Carbon Black Cloud using advanced machine learning (ML) and algorithmic toolsets. This analysis is used to provide critical insight into attacks with recommendations for the policy changes (playbook) needed to remediate the threat. Subscribers are notified via email of threats and are provided with specific policy changes to address the threat in VMware Carbon Black Cloud™ NGAV and EDR. Additionally, analysts are available to provide incident remediation guidance as well as threat containment should an incident occur.

Learn more at www.Dell.com/endpoint-security

vmware Carbon Black

DELL Technologies

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 to assure that your team doesn't miss the alerts that matter.

Roadmap to Root Cause

Carbon Black 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, the VMware team sends out advisories that include indicators of compromise, giving your team a jump start on assessing risk and closing gaps.

Monthly Reporting

The VMware managed detection experts provide monthly reports summarizing 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 simplify your internal reporting. Monthly reports provide analysts with information needed to keep leadership aware of threats, policy changes, and mitigations.

Incident Response Communication with Analysts

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

Threat Containment

VMware 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.

Contact your dedicated Dell Endpoint Security Specialist today at endpointsecurity@dell.com, for more information about the Dell solutions to help improve your security posture

Learn more at www.Dell.com/endpoint-security

vmware Carbon Black