DELL Technologies

Dell SafeGuard and Response

VMware Carbon Black Cloud Endpoint Advanced

Eine Plattform für den Endpunktschutz mit VMware Carbon Black Cloud Endpoint Standard und VMware Carbon Black Cloud Audit and Remediation™.

	Antiviruslösung der nächsten Generation (NGAV)	Verhaltensbasierte Endpunkterkennung und -reaktion (EDR)	IT-Hygiene	Echtzeitendpunkt-abfrage (Systemprüfung)	Endpunktkorrektur
CB Cloud Endpoint Standard	x	x			
CB Cloud Audit & Remediation			x	x	x

CB Cloud Endpoint Standard ist eine branchenführende Virenschutzlösung der nächsten Generation (NGAV) und eine Lösung für die verhaltensbasierte Endpunkterkennung und -reaktion (EDR). Die Bereitstellung erfolgt über die VMware Carbon Black Cloud. Dies ist eine Plattform zum Schutz Ihrer Endpunkte, die Endpunktsicherheit in der Cloud über einen einzigen Agent und eine einheitliche Konsole konsolidiert. Diese Lösung ist nachweislich* in der Lage, gängige Antivirenlösungen zu ersetzen, und bietet optimale Endpunktsicherheit mit möglichst geringem Verwaltungsaufwand. Sie schützt Ihre Systeme vor der gesamten Bandbreite an modernen Cyberangriffen und kann bekannte Malware und unbekannte Nicht-Malware-Angriffe erkennen, verhindern und darauf reagieren.

CB Cloud Audit & Remediation ist eine Lösung für Audit und Korrektur in Echtzeit, mit der Sie auf einfache Weise den Systemstatus von Endpunkten und Containern abrufen und ändern können. Mit dem gleichen VMware Carbon Black Cloud-Agent und der gleichen Konsole können IT-AdministratorInnen und Sicherheitsteams die IT-Hygiene aufrechterhalten, auf Incidents reagieren und Sicherheitslücken bewerten, um schnelle und souveräne Entscheidungen zur Verbesserung des Sicherheitsstatus treffen. VMware Carbon Black Cloud Audit and Remediation schließt die Lücke zwischen Sicherheit und Betrieb. Dadurch können Administratoren und Sicherheitsteams vollständige Untersuchungen durchführen und Maßnahmen ergreifen, um Endpunkte remote zu korrigieren.

Plattform für den Endpunktschutz

VMware Carbon Black Cloud vereitelt nicht nur Angriffe, sondern gibt Ihnen auch die Möglichkeit, Aktivitäten auf den Endpunkten zu analysieren, Ihre Präventionsmaßnahmen im Hinblick auf neue Bedrohungen anzupassen und manuelle Vorgänge in Ihrem gesamten Sicherheitsstack zu automatisieren. All dies erfolgt über eine einzige Konsole und einen unkomplizierten Agent, damit Ihre Endpunkte sowohl online als auch offline geschützt sind.

Lernen und Verhindern

Die zukunftsweisenden Modelle für maschinelles Lernen (ML) analysieren sämtliche Daten auf den Endpunkten, um schädliches Verhalten zu erkennen und so alle Arten von Angriffen, ob online oder offline, zu stoppen.

* https://www.carbonblack.com/products/solutions/use-case/risk-and-compliance/pcidss/

Weitere Informationen finden Sie unter DellEMC.com/endpointsecurity.

vmware Carbon Black

Erfassen und Analysieren

Die Lösung erfasst fortlaufend die Aktivitäten aller Endpunkte, um jeden Ereignis-Stream im Kontext zu analysieren und aufkommende Bedrohungen aufzuspüren, die von anderen Lösungen nicht erkannt werden.

Schnelle Reaktion

Mit den branchenführenden Erkennungs- und Reaktionsfunktionen werden Bedrohungsaktivitäten in Echtzeit erkannt, sodass Sie auf nahezu jede Art von Angriff reagieren können, sobald er identifiziert wurde. Alle Phasen des Angriffs werden mit leicht verständlichen Details zu den Angriffsketten visualisiert, damit die Ursache innerhalb von Minuten ermittelt werden kann.

On-Demand-Abfragen

Bieten Sie Ihrem Sicherheits- und IT-Betriebsteam einen genauen Einblick in den aktuellen Systemstatus aller Endpunkte, damit Sie schnelle und sichere Entscheidungen zur Risikominderung treffen können und die Möglichkeit haben, Endpunkte nach den neuesten Bedrohungsvektoren sowie Gefährdungs- und Angriffsindikatoren abzufragen.

Dell SafeBIOS-Integration

Die kombinierte Leistung von VMware Carbon Black Audit and Remediation und Dell SafeBIOS bietet modernste Sicherheit sowohl oberhalb als auch unterhalb der BS-Ebene und ermöglicht Telemetriefunktionen anhand des vom Host unabhängigen BIOS-Verifizierungsstatus für Dell PCs. Mit der integrierten Lösung können Sicherheits- und IT-Teams das Reporting des Verifizierungsstatus automatisieren und so Maßnahmen ergreifen, um durch BIOS-Manipulationen entstandene Schäden zu korrigieren. Diese Partnerschaft verstärkt die Position von Dell als Anbieter der sichersten PCs der Branche.

Sofortige Remotekorrektur

Schließt die Lücke zwischen Sicherheit und Betriebsabläufen, sodass Administratoren eine Remote-Shell direkt an Endpunkte anschließen können, um vollständige Ermittlungen und Remotekorrektur über eine einzige Cloud-basierte Plattform durchzuführen.

Vereinfachtes betriebliches Reporting

AdministratorInnen und Sicherheitsteams können Abfragen speichern und erneut ausführen, das Betriebs-Reporting zu Patch-Levels, Nutzerprivilegien, Festplattenverschlüsselungsstatus und mehr automatisieren und so Ihre sich ständig verändernde Umgebung überwachen. Sie können nutzerdefinierte Abfragen einfach erstellen und die Ergebnisse von allen Endpunkten in der Umgebung an eine einzige Cloud-basierte Konsole senden.

Konsolidieren des SecOps-Pakets

Konsolidieren Sie das Sicherheitspaket, indem Sie das einzige Echtzeitaudit- und Korrekturtool nutzen, das auf einer Cloud-basierten Plattform für Endpoint Security aufbaut.

IT-Hygiene

Damit können IT-AdministratorInnen und SecOps nachvollziehen, was sie haben, wie es verbunden und konfiguriert ist – und zwar übergreifend für Clouds, Endpunkte, APIs, Geräte und Nutzerkonten. Diese Funktion bietet auch Management für Sicherheitslücken sowie Patchen auf Firmware-, Betriebssystem- und Anwendungsebene, einschließlich Prüfungsfunktionen.

Sicherheitslückenmanagement

Sicherheitsteams werden mithilfe eines bewährten Data-Science-Ansatzes zur Risikobewertung von Sicherheitslücken unterstützt, damit sie sich auf das Patchung oder die Korrektur der kritischsten Schwachstellen in ihrer Umgebung konzentrieren können. Die Teams erhalten direkten Zugriff auf Informationen und Kontext zu Sicherheitslücken und können so sicherstellen, dass sie Sicherheitslücken mit dem höchsten Sicherheitsrisiko schneller korrigieren als solche mit geringerem Risiko.

Anwendungsbeispiele

Virenschutz der nächsten Generation | Verhaltensbasierte Endpunkterkennung und -reaktion | Aufrechterhaltung der IT-Hygiene und Nachverfolgen von Abweichungen | Bewertung von Sicherheitslücken in Echtzeit | Nachweisen und Aufrechterhalten von Compliance | Zuverlässige Reaktion auf Incidents und Sicherheitslücken in Echtzeit | Souveräne Reaktion auf Incidents

Wenden Sie sich noch heute unter endpointsecurity@dell.com an Ihren Dell Endpoint Security Specialist, um zu erfahren, wie Sie mit SafeGuard and Response-Produkten Ihren Sicherheitsstatus verbessern können.

Weitere Informationen finden Sie unter DellEMC.com/endpointsecurity.

vmware Carbon Black