Dell SafeGuard and Response

VMware Carbon Black Cloud Endpoint Enterprise Eine Plattform für den Endpunktschutz mit

VMware Carbon Black Cloud Endpoint Standard, Audit & Remediation und Enterprise EDR

	Antiviru-slösung der nächsten Generation (NGAV)	Verhaltens-basierte Endpoint Detection and Response (EDR)	IT-Hygiene	Echtzeitend-punktabfrage (System-prüfung)	Endpunkt-korrektur	Enterprise Endpoint Detection and Response (EDR)	Erweiterte Ereignisa-nalyse (Threat Hunting)
CB Cloud Endpoint Standard	x	x					
CB Cloud Audit & Remediation			x	x	x		
CB Cloud Enterprise EDR						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.

Die Lösung, die nachweislich* in der Lage ist, gängige Antivirenlösungen zu ersetzen, 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 Echtzeitaudit- und Korrekturlösung, die Sicherheitsteams schnelleren, einfacheren Zugriff auf Audits und Änderung des Systemzustands von Endpunkten und Containern bietet – mit dem gleichen VMware Carbon Black Cloud Agent und der gleichen Konsole können IT-Administratoren und Sicherheitsteams die IT-Hygiene aufrecht erhalten, auf Vorfälle reagieren und Sicherheitslücken bewerten, um schnelle, selbstbewusste Entscheidungen zur Verbesserung ihrer Sicherheitsstrategie zu treffen. VMware Carbon Black Audit & Remediation schließt die Lücke zwischen Sicherheit und Betrieb. Dadurch können Administratoren und Sicherheitsteams vollständige Untersuchungen durchführen und Maßnahmen ergreifen, um Endpunkte remote zu korrigieren.

CB Cloud Enterprise EDR ist eine Endpunkterkennung und -reaktionslösung für eine kontinuierliche Sichtbarkeit für Security Operations Center (SOC) und IR-Teams (Incident Response). Enterprise EDR reduziert langwierige Ermittlungen von Tagen auf Minuten, ermöglicht Teams die proaktive Suche nach Bedrohungen und gibt ihnen die Möglichkeit, in Echtzeit zu reagieren und zu korrigieren.

Plattform für den Endgeräteschutz

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

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

Weitere Informationen unter DellEMC.com/de-de/endpointsecurity

vmware Carbon Black

Lernen und verhindern

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

Erfassen und analysieren

Die Lösung erfasst fortlaufend alle Aktivitäten von allen Endpunkten, um jeden Ereignis-Stream im jeweiligen Kontext zu analysieren und aufkommende Bedrohungen aufzuspüren, die von anderen Lösungen unentdeckt bleiben.

Schnelle Reaktion

Mit den branchenführenden Erkennungs- und Reaktionsfunktionen werden Bedrohungsaktivitäten in Echtzeit erkannt, sodass Sie auf 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

Bietet Ihrem Sicherheits- und IT-Betriebsteam Einblick in den präzisesten aktuellen Systemstatus aller Endpunkte, sodass Sie schnell und souverän Entscheidungen treffen können, um Risiken zu reduzieren. Abfrage von Endpunkten für die neuesten Bedrohungsvektoren, Indikatoren für die Gefährdung und Indikatoren für Angriffe.

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

Administratoren und Sicherheitsteams können Abfragen speichern und erneut ausführen, um das Betriebs-Reporting zu Patch-Levels, Benutzerprivilegien, Festplattenverschlüsselungsstatus und mehr zu automatisieren und so ihre sich ständig verändernde Umgebung zu überwachen. Die Möglichkeit, benutzerdefinierte Abfragen einfach zu erstellen und Ergebnisse von allen Endpunkten in ihrer Umgebung an eine einzige Cloud-basierte Konsole zu senden.

Konsolidieren Sie Ihren SecOps-Stack

Konsolidieren Sie Ihr Sicherheitspaket, indem Sie das einzige Echtzeitaudit- und Korrekturtool nutzen, das auf einer Cloud-basierten Endpunktsicherheitsplattform aufbaut.

IT-Hygiene

Erfahren Sie, was vorhanden ist, wie es verbunden ist, wie es über Ihre Cloud, Endpunkte, APIs, Geräte und Benutzerkonten konfiguriert wird. Sicherheitslückenmanagement und Patching: Firmware-, Betriebssystem- und Anwendungsebene, einschließlich Prüfung der oben genannten.

Kontinuierliche Ereigniserfassung

Untersuchungen, die in der Regel Tage oder Wochen dauern, können in nur wenigen Minuten erledigt werden. CB Cloud Enterprise EDR korreliert und visualisiert umfassende Informationen zu Endpunktereignissen, sodass Sicherheitsexperten einen besseren Einblick in ihre Umgebung erhalten.

Anwendungsfälle

Virenschutz der nächsten Generation | Verhaltensbasierte Endpunkterkennung und -reaktion | Incident-Reaktion | Aufrechterhaltung des IT-Hygiene-rack-Drift | Bewertung von Sicherheitslücken in Echtzeit | Nachweisen und Aufrechterhalten von Compliance

Wenden Sie sich an den für Sie zuständigen Dell Endpoint Security Experten unter endpointsecurity@dell.com, um Informationen zu den SafeGuard and Response-Produkten zu erhalten, mit denen Sie Ihre Sicherheitsstrategie verbessern können.

Weitere Informationen unter DellEMC.com/de-de/endpointsecurity

vmware Carbon Black