DELL Technologies

Dell SafeGuard and Response

VMware Carbon Black Cloud Endpoint Advanced

Une plate-forme de protection des points de terminaison dotée de la solution VMware Carbon Black Cloud Endpoint Standard et de la solution VMware Carbon Black Cloud Audit & Remediation™

	Antivirus de nouvelle génération (NGAV)	Behavioral Endpoint Detection and Response (EDR)	Hygiène IT	Interrogation des points de terminaison en temps réel (audit système)	Correction du point de terminaison
CB Cloud Endpoint Standard	x	x			
CB Cloud Audit & Remediation			x	x	x

CB Cloud Endpoint Standard est une solution leader sur le marché regroupant un antivirus de nouvelle génération (NGAV) et la fonctionnalité Behavioral Endpoint Detection and Response (EDR). Elle repose sur VMware Carbon Black Cloud, une plate-forme de protection des points de terminaison qui renforce la sécurité des points de terminaison dans le Cloud en utilisant un seul agent et une seule console. Solution de remplacement certifiée* pour un antivirus standard, elle est conçue pour offrir la meilleure sécurité au niveau des points de terminaison avec le moins de travail d'administration possible. Elle offre une protection contre toute la gamme des cyberattaques modernes, et intègre notamment la capacité de détecter, de prévenir et de contrer les attaques de logiciels malveillants connus et les attaques de logiciels non malveillants inconnus.

CB Cloud Audit & Remediation est une solution d'audit et de mesure corrective en temps réel qui permet aux équipes de sécurité d'accéder plus facilement et rapidement à l'audit, ainsi que de modifier l'état du système des points de terminaison et des conteneurs. L'utilisation du même agent et de la même console VMware Carbon Black Cloud pour permettre aux équipes IT, aux administrateurs et aux équipes de sécurité, de maintenir l'hygiène IT, de répondre aux incidents et d'évaluer les failles de sécurité, ainsi que de prendre des décisions rapides et sûres pour améliorer leur posture de sécurité. La solution VMware Carbon Black Cloud Audit & Remediation comble le fossé entre la sécurité et les opérations. Cette solution permet aux administrateurs et aux équipes de sécurité d'effectuer des enquêtes complètes et de prendre des mesures correctives à distance pour les points de terminaison.

Plate-forme de protection des points de terminaison

La plate-forme VMware Carbon Black Cloud fait plus qu'interrompre le comportement des pirates en vous donnant la possibilité d'analyser l'activité des points de terminaison, d'adapter la prévention des menaces émergentes et d'automatiser les efforts manuels sur l'ensemble de votre pile de sécurité. Le tout à partir d'une seule console et d'un seul agent léger pour sécuriser vos points de terminaison en ligne et hors ligne.

Apprendre et prévenir

Les modèles d'apprentissage automatique avancés analysent l'ensemble des données de points de terminaison pour identifier les comportements malveillants afin d'arrêter tous les types d'attaques, en ligne et hors ligne.

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

Pour en savoir plus, consultez le site DellEMC.com/endpointsecurity

vmware Carbon Black

Capturer et analyser
Capture en continu les activités de tous les points de terminaison, afin d'analyser chaque flux d'événements dans le contexte et d'identifier les attaques émergentes que d'autres solutions ne détecteraient pas.

Réagir rapidement
Des fonctionnalités de détection et de réponse à la pointe du secteur identifient l'activité des menaces en temps réel, afin que vous puissiez répondre à presque tout type d'attaque dès son identification. Chaque étape de l'attaque est visualisée avec des informations sur la chaîne d'attaque faciles à suivre afin de découvrir la cause première en quelques minutes.

Requêtes à la demande
Fournissez à vos équipes des opérations IT et de sécurité une visibilité sur l'état du système actuel le plus précis de tous les points de terminaison, ce qui vous permet de prendre des décisions rapides et sûres afin de réduire les risques et les capacités d'interroger les points de terminaison sur les derniers vecteurs de menaces et les indicateurs de corruption et d'attaque.

Intégration de la solution Dell SafeBIOS
La puissance combinée de VMware Carbon Black Cloud Audit & Remediation et de la solution Dell SafeBIOS offre une sécurité de pointe à la fois au-dessus et au-dessous du système d'exploitation et permet la télémétrie à partir de la vérification de l'état du BIOS hors hôte sur l'offre d'ordinateurs professionnels Dell. La solution intégrée permet aux équipes IT et de sécurité d'automatiser la création de rapports sur l'état de la vérification afin qu'elles puissent prendre des mesures pour corriger les failles résultant de l'altération du BIOS. Ce partenariat renforce la position de Dell en tant que fournisseur d'ordinateurs professionnels les plus sécurisés du marché.

Correction immédiate à distance
Comble les failles entre sécurité et opérations, ce qui permet aux administrateurs d'accéder aux points de terminaison via un shell distant pour réaliser des enquêtes complètes et prendre des mesures correctives à distance, le tout à partir d'une seule plate-forme basée sur le Cloud.

Création de rapports opérationnels simplifiée
Permet aux administrateurs et aux équipes de sécurité d'enregistrer et de relancer les requêtes, automatiser la création de rapports opérationnels sur les niveaux de correctif, les privilèges utilisateur, l'état du chiffrement des disques, etc., pour rester au fait de l'environnement en constante évolution. Donne la possibilité de créer facilement des requêtes personnalisées et de renvoyer les résultats de tous les points de terminaison sur une seule console basée sur le Cloud.

Consolidation de la pile SecOps
Consolidez la pile de sécurité en tirant profit du seul outil d'audit et de résolution des problèmes en temps réel reposant sur une plate-forme de sécurité des points de terminaison basée sur le Cloud.

Hygiène IT
Cette fonctionnalité aide les administrateurs IT et l'équipe SecOps à comprendre l'environnement dont ils disposent et comment tout est connecté et configuré entre le Cloud, les points de terminaison, les API, les appareils et les comptes d'utilisateur. Elle permet également de gérer les failles de sécurité, d'appliquer des correctifs au niveau du firmware, du système d'exploitation et des applications, y compris les fonctionnalités d'audit.

Gestion des failles de sécurité
Utilise une approche éprouvée de la science des données pour l'évaluation des risques de faille de sécurité. Les équipes de sécurité peuvent ainsi se concentrer sur les correctifs ou l'application de mesures correctives liés aux failles de sécurité les plus stratégiques dans leur environnement. Fournit aux équipes un accès direct à l'intelligence sur les failles de sécurité et au contexte. Elles peuvent appliquer les mesures correctives en priorité à celles qui présentent le risque de sécurité le plus élevé.

Cas d'utilisation
Antivirus de nouvelle génération | Détection et réponse comportementales au niveau des points de terminaison | Maintien de l'hygiène IT et suivi des dérives | Évaluation des failles de sécurité en temps réel | Preuve et respect de la conformité | Réponse aux incidents et aux failles de sécurité en toute confiance et en temps réel | Preuve et respect de la conformité | Réponse aux incidents en toute confiance

Contactez votre spécialiste Dell Endpoint Security dédié dès aujourd'hui à l'adresse endpointsecurity@dell.com pour en savoir plus sur les produits Dell SafeGuard and Response qui peuvent vous aider à améliorer votre posture de sécurité.

Pour en savoir plus, consultez le site DellEMC.com/endpointsecurity

vmware Carbon Black