Dell SafeGuard and Response

VMware Carbon Black Cloud Endpoint Enterprise
Une plate-forme de protection des points de terminaison avec

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

	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	Enterprise Endpoint Detection and Response (EDR)	Analyse des événements avancée (détection des menaces)
CB Cloud Endpoint Standard	x	x					
CB Cloud Audit & Remediation			x	x	x		
CB Cloud Enterprise EDR						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 répondre aux attaques de logiciels malveillants connus et aux attaques de logiciels non malveillants inconnus.

L'outil **CB Cloud Audit & Remediation** est une solution de détection et de résolution des problèmes en temps réel qui permet aux équipes de sécurité d'accéder plus facilement et plus rapidement aux données d'audit et de modifier l'état du système des points de terminaison et des conteneurs. Il s'appuie sur un seul agent et une seule console VMware Carbon Black Cloud pour faciliter le travail des équipes chargées des opérations IT, de l'administration et de la sécurité, pour maintenir l'hygiène IT, pour répondre aux incidents et pour évaluer les failles de sécurité, afin de prendre des décisions rapides et sûres et d'améliorer la sécurité. VMware Carbon Black Audit & Remediation comble les failles entre sécurité et 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.

La solution de détection et de réponse au niveau des points de terminaison **CB Cloud Enterprise EDR** offre une visibilité continue pour les centres d'opérations de sécurité (SOC) et les équipes de réponse aux incidents (IR). Avec la solution Enterprise EDR, les longues enquêtes de plusieurs jours peuvent être effectuées en quelques minutes, ce qui permet aux équipes de détecter les menaces de manière proactive, d'y réagir et de les corriger en temps réel.

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.

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

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

vmware Carbon Black

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.

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 qui identifient l'activité des menaces en temps réel, afin que vous puissiez répondre à tout type d'attaque dès leur identification. Visualise chaque étape de l'attaque avec des informations sur la chaîne d'attaque faciles à suivre afin de découvrir la cause première en quelques minutes.

Requêtes à la demande

Offre à vos équipes chargées des opérations IT et de la sécurité une visibilité extrêmement détaillée de l'état actuel du système de tous les points de terminaison, ce qui permet de prendre des décisions rapides et informées et de réduire les risques. Interrogez les points de terminaison pour connaître les derniers vecteurs de menace, les indicateurs de compromission et les indicateurs d'attaque.

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 pour 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 votre 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 votre pile SecOps

Consolidez votre pile de sécurité en tirant profit du seul outil de détection 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

Connaissez les ressources dont vous disposez, leurs connexions et leurs configurations dans l'ensemble de votre Cloud, des points de terminaison, des API, des appareils et des comptes d'utilisateur. Gestion des failles de sécurité et correctifs : Au niveau du firmware, du système d'exploitation et des applications, y compris l'audit de ces éléments.

Capture d'événements en continu

Les enquêtes qui prennent généralement des jours ou des semaines peuvent être effectuées en quelques minutes seulement. La solution CB Cloud Enterprise EDR permet d'associer et de visualiser des informations complètes sur les événements des points de terminaison. Les professionnels disposent ainsi d'une meilleure visibilité sur leurs environnements.

Cas d'utilisation

Antivirus de nouvelle génération | Behavior Endpoint Detection and Response | Réponse aux incidents | Maintien de l'hygiène IT et suivi des dérives | Évaluer les failles de sécurité en temps réel | Assurer le respect des normes de conformité et en apporter la preuve

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

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

vmware® Carbon Black