DELL Technologies

Dell SafeGuard and Response

VMware Carbon Black Cloud Endpoint Advanced

La piattaforma per la protezione degli endpoint con VMware Carbon Black Cloud Endpoint Standard e VMware Carbon Black Cloud Audit & Remediation™

	Antivirus di nuova generazione (NGAV)	Tecnologia EDR (Endpoint Detection and Response) comportamentale	Protezione attiva dell'IT	Query sugli endpoint in tempo reale (verifica del sistema)	Correzione degli endpoint
CB Cloud Endpoint Standard	x	x			
CB Cloud Audit and Remediation			x	x	x

CB Cloud Endpoint Standard offre un antivirus di nuova generazione (NGAV) leader del settore insieme a una soluzione EDR (Endpoint Detection and Response) comportamentale. Viene distribuito tramite VMware Carbon Black Cloud, una piattaforma di protezione degli endpoint che consolida la loro sicurezza nel cloud utilizzando un singolo agent e un'unica console. Certificato* per sostituire gli antivirus tradizionali, CB Cloud Endpoint Standard è progettato per offrire la massima sicurezza degli endpoint con una gestione minima. Offre protezione da tutti i tipi di attacchi informatici moderni poiché è in grado di rilevare, prevenire e neutralizzare sia i malware noti che gli attacchi non malware sconosciuti.

CB Cloud Audit and Remediation è una soluzione di verifica e correzione in tempo reale, che consente ai team addetti alla sicurezza di verificare e modificare in modo facile e veloce lo stato del sistema per endpoint e container. Utilizza in modo ottimale lo stesso agent e la stessa console di VMware Carbon Black Cloud per consentire all'IT, agli amministratori e ai team addetti alla sicurezza di mantenere la protezione attiva dell'IT, rispondere agli incidenti e valutare le vulnerabilità, nonché di prendere decisioni rapide e affidabili per migliorare il profilo di sicurezza. VMware Carbon Black Cloud Audit & Remediation risolve i problemi legati alla sicurezza e alle operazioni consentendo agli amministratori e ai team di sicurezza di eseguire indagini complete e intraprendere azioni per correggere gli endpoint da remoto.

Piattaforma di protezione degli endpoint

VMware Carbon Black Cloud non si limita semplicemente a bloccare i comportamenti malevoli, ma offre anche la possibilità di analizzare l'attività degli endpoint, adattare le misure preventive esistenti alle minacce emergenti e automatizzare le attività manuali per l'intero stack di sicurezza. Il tutto da un'unica console con un singolo agent leggero per proteggere gli endpoint online e offline.

Apprendimento e prevenzione

I modelli avanzati di apprendimento automatico analizzano tutti i dati degli endpoint per rilevare comportamenti malevoli e bloccare ogni tipo di attacco, online e offline.

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

Ulteriori informazioni sono disponibili sul sito DellEMC.com/endpointsecurity

© 2021 Dell Technologies o sue società controllate.

vmware Carbon Black

Acquisizione e analisi
Questa soluzione acquisisce continuamente i dati sull'attività di ogni endpoint, analizzando tutti i flussi di eventi nel contesto per scoprire eventuali attacchi emergenti non rilevati dalle altre soluzioni.

Risposta rapida
Le funzionalità di rilevamento e risposta leader del settore individuano le minacce in tempo reale, così da rispondere a qualsiasi tipo di attacco non appena viene identificato. Tutte le fasi dell'attacco vengono rappresentate in una catena dettagliata e di facile consultazione, che consente di scoprire la root cause in pochi minuti.

Query on-demand
Fornisci al team delle operazioni IT e di sicurezza la visibilità accurata dello stato del sistema attuale di tutti gli endpoint, in modo tale da prendere decisioni rapide e sicure per ridurre i rischi e ottenendo la possibilità di interrogare gli endpoint in merito ai vettori di minacce più recenti, gli indicatori di compromissione e gli indicatori di attacco.

Integrazione di Dell SafeBIOS
Combinati tra loro, VMware Carbon Black Audit and Remediation e Dell SafeBIOS offrono elevati livelli di sicurezza sia al di sopra che al di sotto del sistema operativo, consentendo anche la telemetria dello stato di verifica del BIOS off-host sui PC commerciali Dell. Con questa soluzione integrata, i team IT e di sicurezza possono automatizzare il reporting dello stato di verifica e intraprendere azioni per correggere eventuali problemi derivanti da manomissioni del BIOS. L'integrazione tra questi due prodotti consolida la posizione di Dell come fornitore dei PC commerciali più sicuri del settore.

Correzione immediata in remoto
Questa funzione colma il divario tra sicurezza e operazioni, fornendo agli amministratori una shell remota direttamente all'interno degli endpoint per eseguire indagini complete e apportare correzioni in remoto, il tutto da un'unica piattaforma basata sul cloud.

Creazione semplificata di report operativi
Con questa funzione, gli amministratori e i team addetti alla sicurezza salvano ed eseguono nuovamente le query, automatizzano il reporting operativo sui livelli delle patch, sui privilegi dell'utente, sullo stato della crittografia del disco e altro ancora, al fine di soddisfare le esigenze degli ambienti in continua evoluzione. È inoltre possibile creare con facilità query personalizzate e restituire risultati da tutti gli endpoint nell'ambiente a un'unica console basata sul cloud.

Consolidamento dello stack SecOps
Consolida lo stack di sicurezza utilizzando l'esclusivo strumento di audit e correzione in tempo reale integrato nella piattaforma di sicurezza degli endpoint basata sul cloud.

Protezione attiva dell'IT
È utile agli amministratori IT e al team SecOps per comprendere di quali strumenti dispongono, in che modo sono collegati e come sono configurati su cloud, endpoint, API, dispositivi e account utente. Questa funzione prevede inoltre la gestione delle vulnerabilità, l'applicazione di patch a livello del firmware, del sistema operativo e delle applicazioni, comprese le funzioni di verifica.

Gestione delle vulnerabilità
Utilizza in modo ottimale un approccio comprovato di Data Science relativo al punteggio di rischio delle vulnerabilità per consentire ai team addetti alla sicurezza di concentrarsi sull'applicazione di patch o sulla risoluzione delle vulnerabilità più critiche nel proprio ambiente. Consente ai team di accedere direttamente all'intelligence e al contesto delle vulnerabilità per assegnare una priorità maggiore nelle attività di correzione alle vulnerabilità con un rischio più elevato per la sicurezza rispetto ad altre meno critiche.

Casi d'uso
Antivirus di nuova generazione | Tecnologia EDR comportamentale | Mantenimento della protezione attiva dell'IT e rilevamento delle deviazioni | Valutazione delle vulnerabilità in tempo reale | Dimostrazione e mantenimento della conformità | Risposta sicura agli incidenti

Contattare gli esperti per la sicurezza degli endpoint Dell dedicati all'indirizzo endpointsecurity@dell.com per saperne di più sui prodotti Dell SafeGuard and Response che possono migliorare il profilo di sicurezza dell'azienda

Ulteriori informazioni sono disponibili sul sito DellEMC.com/endpointsecurity

© 2021 Dell Technologies o sue società controllate.

vmware Carbon Black