Dell SafeGuard and Response

VMware Carbon Black Cloud Endpoint Enterprise エンドポイント保護プラットフォームの主な機能

VMware Carbon Black Cloud Endpoint Standard、Audit & Remediation、およびEnterprise EDR

	次世代ウイルス対策（NGAV）	行動ベースのエンドポイント検出および対応（EDR）	ITのセキュリティ	エンドポイントのリアルタイム検索（システム監査）	Endpoint Remediation	エンタープライズのためのエンドポイントでの検出および対応（EDR）	高度なイベント分析（脅威のハンティング）
CB Cloud Endpoint Standard	x	x					
CB Cloud Audit & Remediation			x	x	x		
CB Cloud Enterprise EDR						x	x

CB Cloud Endpoint Standardは、業界をリードする次世代ウイルス対策（NGAV）ソリューションであり、行動ベースのエンドポイント検出および対応（EDR）ソリューションです。単一のエージェントとコンソールを使用してクラウドにエンドポイント セキュリティを統合するエンドポイント保護プラットフォームである、VMware Carbon Black Cloudを通じて提供されます。

これは標準のウイルス対策に代わるものとして認定されており*、管理の負担を最小限に抑えながら業界をリードするエンドポイント セキュリティを実現する設計になっています。既知のマルウェア攻撃および未知の非マルウェア攻撃の検出と防止機能、また攻撃への対応機能などにより、最新のあらゆるサイバー攻撃から保護します。

CB Cloud Audit & Remediationは、セキュリティ チームがエンドポイントとコンテナーのシステム状態をすばやく簡単に監査および変更するのを可能にした、リアルタイムの監査および修復ソリューションです。同じVMware Carbon Black Cloudエージェントとコンソールを活用することで、IT管理者およびセキュリティ チームは、ITのセキュリティの維持、インシデントへの対応、脆弱性の評価を行い、セキュリティ態勢を強化するための決定を迅速に自信を持って下すことができます。VMware Carbon Black Audit & Remediationによって、セキュリティと運用のギャップが解消されます。これは、管理者とセキュリティ チームが徹底した調査を行い、エンドポイントをリモートで修復するための措置がとれるようにすることで実現されます。

CB Cloud Enterprise EDRのエンドポイント検出と応答ソリューションは、優れたセキュリティ運用センター（SOC）およびインシデント対応（IR）チームに継続的な可視性を提供します。Enterprise EDRによって、長くかかっていた調査時間は数日から数分に短縮され、チームはプロアクティブに脅威のハンティングを行うことができ、リアルタイムで脅威に対応して修復することができます。

エンドポイント保護プラットフォーム

VMware Carbon Black Cloudでは、単に攻撃者の行動を阻止するだけでなく、エンドポイント アクティビティの分析や、新たな脅威に対する防御策の実装、セキュリティ スタックでの手作業の自動化が可能です。すべての操作を1つのコンソールと単一の軽量エージェントから実行でき、エンドポイントをオンラインおよびオフラインで保護します。

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

詳細については、DellEMC.com/endpointsecurityをご覧ください。

vmware Carbon Black

学習と防止
高度な機械学習モデルによってエンドポイント データ全体を分析し、悪意のある動作を検知して、あらゆる種類の攻撃をオンラインおよびオフラインで阻止します。

収集と分析
すべてのエンドポイントからアクティビティを継続的に収集して、コンテキスト内の各イベント ストリームを分析し、他のソリューションでは検出されない新たな攻撃を検知します。

迅速な対応
業界をリードする検出および対応機能によって、脅威となるアクティビティをリアルタイムで把握できるため、どのような種類の攻撃が特定されてもすぐに対応できます。攻撃のあらゆる段階を可視化することで、攻撃チェーンの詳細情報を容易にたどることができるため、根本原因を数分で突き止めることができます。

On-Demandクエリ
セキュリティ & IT運用チームに、すべてのエンドポイントについて最も正確な現在のシステム状態の可視性を提供することで、自信を持ってすばやく決定を下して、リスクを低減できます。最新の脅威ベクトル、侵害インジケータ、および攻撃インジケータのエンドポイントをクエリします。

即時のリモート修復
セキュリティと運用の間のギャップを解消し、管理者にエンドポイントへのリモート シェルを直接提供して、徹底した調査とリモート修復を1つのクラウドベースのプラットフォームから実行できるようにします。

シンプル化された運用レポート
管理者とセキュリティ チームは、変化し続ける環境について最新情報を把握できるよう、パッチ レベル、ユーザー権限、ディスク暗号化ステータスなどについての運用レポートを自動化するクエリを保存して再実行できます。カスタム クエリを簡単に作成し、環境内のすべてのエンドポイントからの結果を単一のクラウドベースのコンソールに返します。

SecOpsスタックの統合
クラウドベースのエンドポイント セキュリティ プラットフォーム上に構築された、業界唯一のリアルタイム監査および修復ツールを活用して、セキュリティ スタックを統合します。

ITのセキュリティ
クラウド、エンドポイント、API、デバイス、およびユーザー アカウント全体にわたって、ユーザーが所有するもの、接続状況、および構成状況を把握します。脆弱性の管理とパッチ適用：上記の監査を含む、ファームウェア、OS、およびアプリケーション レベル。

継続的なイベント キャプチャ
通常は数日または数週間かかる調査を、わずか数分で完了することができます。CB Cloud Enterprise EDRは、エンドポイント イベントに関する包括的な情報を相互に関連付けて可視化し、大幅に向上した環境の可視性をセキュリティ専門家に提供します。

ユース ケース
次世代ウイルス対策 | 行動ベースのエンドポイント検出および対応 | インシデントへの対応 | ITのセキュリティの追跡ドリフトを維持 | 脆弱性をリアルタイムで評価 | コンプライアンスの実証と維持

セキュリティ態勢の強化に役立つSafeGuard and Response製品については、担当のデル エンドポイント セキュリティ スペシャリスト（endpointsecurity@dell.com）までお問い合わせください。

詳細については、DellEMC.com/endpointsecurityをご覧ください。

vmware Carbon Black