# Dell SafeGuard and Response

## VMware Carbon Black Cloud Endpoint Advanced

## VMware Carbon Black Cloud Endpoint StandardとVMware Carbon Black Cloud Audit and Remediation™を組み合わせたエンドポイント保護プラットフォーム

| | 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ハイジーン（衛生管理） | エンドポイントのリアルタイムクエリ（システム監査） | エンドポイントの修復 |
|---|---|---|---|---|---|
| CB Cloud Endpoint Standard | x | x | | | |
| CB Cloud Audit and Remediation | | | x | 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。このソリューションは、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。

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トップクラスのエンドポイント セキュリティを実現する設計になっています。また、既知のマルウェア攻撃や未知の非マルウェア攻撃の検出と防止機能、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 and Remediation**は、リアルタイムの監査および修復ソリューションです。このソリューションにより、セキュリティ チームはエンドポイントとコンテナのシステム状態をすばやく簡単に監査、変更することができます。同じVMware Carbon Black Cloudを活用するクラウド エージェントとコンソールを活用することで、IT管理者とセキュリティ チームが、ITハイジーン（衛生管理）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判断を、迅速かつ自信を持って下せるようになります。VMware Carbon Black Cloud Audit and Remediationは、セキュリティと運用のギャップを解消します。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取れるようにすることで実現されます。

### エンドポイント保護プラットフォーム

VMware Carbon Black Cloudによって、単に攻撃者の行動を阻止するだけでなく、IT部門がエンドポイント アクティビティの分析、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を行えるようになります。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とオフラインで保護します。

### 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とオフラインの両方で阻止します。

*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

**継続的な収集と分析**すべてのエンドポイントからアクティビティを収集、各イベント ストリームをコンテキスト内で分析し、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にも特定次第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。

### オンデマンド クエリ

セキュリティ チームとIT運用チームに対して、全エンドポイントの現在のシステム状態を極めて正確に可視化するため、お客様はリスクを低減するための判断を、迅速かつ自信を持って下せます。また、エンドポイントに対してクエリを実行し、最新の脅威ベクトル、侵害の兆候、攻撃の兆候がないか調べることができます。

### Dell SafeBIOSとの統合

VMware Carbon Black Cloud Audit and RemediationとDell SafeBIOSのパワーを組み合わせることにより、OS内外で最新のセキュリティを提供し、Dellのビジネス向けPC製品においてオフホストのBIOS検証ステータスからのテレメトリーを実現します。この統合ソリューションにより、セキュリティ チームとITチームは検証ステータスのレポート機能を自動化して、BIOSの改ざんに起因する侵害の修復措置を取ることができます。このパートナーシップは、Dellが業界屈指の安全なビジネス向けPCプロバイダーであるという認識を強めています。

### 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、クエリを保存、再実行し、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関する運用レポート作成を自動化することで、変化し続ける環境の最新情報を常に把握できます。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すことができます。

### 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ハイジーン（衛生管理）

IT管理者とSecOpsチームが、自分の所有物とその接続および構成状況について、クラウド、エンドポイント、API、デバイス、ユーザー アカウント全体にわたって把握するために役立ちます。この機能は、監査機能を含め、脆弱性管理や、ファームウェア、OS、アプリケーション レベルでのパッチ適用も提供します。

### USBデバイス制御

VMware Carbon Black Cloud Endpoint Standardとv3.6.0.1897以降のセンサーの組み合わせにより、あらゆるWindowsエンドポイントに接続されている外部USBストレージ デバイスを検出およびモニタリングして、可視化することができます。読み取り、書き込み、実行の各操作をブロックすることで、USBストレージ デバイスに関連する一般的な脅威を低減します。ブロックが発生するたびに、自動アラートによって社内のユーザーと管理者に通知し、情報を伝えることができます。承認されたUSBデバイスを、製造元番号またはシリアル番号によって識別することができます。

### 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 | ITハイジーン（衛生管理）の維持とドリフトの追跡 | 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 | 確信を持ってインシデントに対処 リアルタイム | コンプライアンスの実証と維持 | 確信を持ってインシデントに対処

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、
Dell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