VMware Carbon Black Cloud

Workload

最新のデータセンターにおける高度なワークロード保護

ユースケース

- クラウド ワークロードの保護
- 脆弱性の管理
- セキュリティ リスクの有無や運用上の健全性を確認するためのワークロードの監査
- Software-Defined Data Center（SDDC）のセキュリティの強化
- サーバ上の従来型アンチウイルス製品の置き換え
- ワークロードの挙動監視と EDR

インフラストラクチャ チームにとってのメリット

- vSphere Client からリアルタイムで脆弱性を評価可能
- クラス最高レベルの優先順位付けによるパッチ適用効率の向上
- 既存のインフラストラクチャに組み込まれたセキュリティ機能の活用
- プロアクティブな IT ハイジーンを確立してセキュリティ侵害を防止
- オーバーヘッドの削減。インフラストラクチャの追加や負荷の高いスキャンが不要
- サーバ上の従来型アンチウイルス製品を置き換えて処理能力を節約

セキュリティ チームにとってのメリット

- 既知および未知の攻撃からのワークロードの保護
- セキュリティ ツールの統合による複雑性の低減
- セキュリティ インシデントの容易な調査
- 攻撃チェーンのリアルタイムの可視化
- 平均修復時間（MTTR）の短縮
- セキュリティ分析と IT 運用との間の障壁の撤廃
- VMware のセキュリティ エキスパートや一般のユーザーが参加する活発なユーザー コミュニティとの連携

組織は、クラウドの変革とアプリケーションのモダン化の実現を進めるなかで、強力かつ運用しやすい最新のセキュリティ ソリューションを求めています。VMware Carbon Black Cloud Workload™ は、最新のワークロードの保護に特化した高度な保護機能を備え、攻撃対象領域の縮小とセキュリティの強化を実現します。この革新的なソリューションは、優先順位付けされた脆弱性レポートと基本的なワークロードの強化に、業界をリードする防御、検知、対応機能を組み合わせて、仮想環境、プライベートクラウド環境、およびハイブリッドクラウド環境で実行されているワークロードを保護します。

vSphere と緊密に統合された VMware Carbon Black Cloud Workload は、エージェントレスでセキュリティを提供し、インストールと管理のオーバーヘッドを削減します。また、テレメトリ収集を一元管理し、多様なワークロード セキュリティのユースケースに対応します。この統合ソリューションにより、セキュリティ チームとインフラストラクチャ チームは、セキュリティ ライフサイクルのあらゆる局面で新規および既存のワークロードを自動的に保護しながら、運用を簡素化し、IT スタックとセキュリティ スタックを統合できます。

リスクの特定とワークロードの保護強化

VMware Carbon Black Cloud Workload は、セキュリティ チームとインフラストラクチャ チームが、環境全体でもっともリスクの高い脆弱性や狙われやすいエクスプロイトに集中して取り組めるようにサポートします。これは、検知可能な脆弱性の数をただ増やすのではなく、環境にとって脅威となる脆弱性を検知するというアプローチです。共通脆弱性評価システム（CVSS）の情報、実環境での悪用可能性、攻撃の頻度などの指標を組み合わせて脆弱性の優先順位を決め、クラス最高レベルの優先順位付けによりパッチ適用の効率性を高めます。

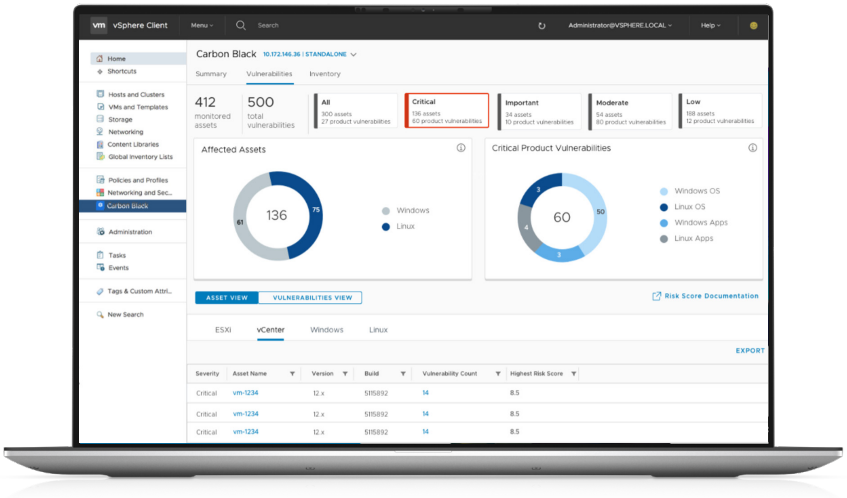

図 1：vCenter Client での優先順位付けされた脆弱性レポート

機能

- スキャン不要の、リスクに基づいて優先順位付けされた脆弱性評価
- ワークロードのインベントリとライフサイクル管理
- vCenter プラグイン
- ワークロードの挙動監視
- 何千ものワークロード アーティファクトに対するオンデマンドでのクエリ
- 次世代アンチウイルス(NGAV)
- ワークロードの EDR
- 継続的な評価の実行による IT ハイジーンの経時的管理

プラットフォーム

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Red Hat 6/7
- CentOS 6/7
- Ubuntu 16/18/19/20
- SLES 12/15

最小技術要件

- vSphere 6.5 以降
- VMware Tools 11.2 以降
- vCenter 6.7 以降
- VMware Carbon Black Cloud へのインターネット接続

詳細情報

個別のデモのご要望や、詳細情報については、contact@carbonblack.com に E メールでお問い合わせいただくか、carbonblack.com/workload をご参照ください。

リアルタイムの脆弱性評価は、セキュリティ チームとインフラストラクチャ チームが脆弱性のコンテキスト情報を把握するのに役立つ、リスク スコアと National Vulnerability Database へのリンクを提供します。この評価は追加の管理オーバーヘッドやセットアップを伴わずに実行でき、大量のリソースを消費するスキャンの必要性を排除します。VMware Carbon Black Cloud Workload では、運用環境の健全性、セキュリティ侵害インジケーター(IoC)、攻撃手口(TTP:戦術、技術、手順)、およびシステムで発生する通常のイベントを把握することもできます。

vSphere 管理者は、仮想マシン インベントリの一括有効化とライフサイクル管理を使用して、機能としてのワークロード保護を vSphere Client から簡単にアクティブ化できます。インフラストラクチャ チームは vSphere のダッシュボードからアプライアンスの健全性、インベントリの状況、インストールのワークフローを可視化し、環境全体で見つかったオペレーティング システムおよびアプリケーションの脆弱性のリストを確認できます。このリストではリスクに基づいて脆弱性が優先順位付けされています。VMware Carbon Black Cloud Workload は、これまでにないレベルで環境を詳細に可視化することでリスクの削減とワークロードの保護強化を実現し、セキュリティの効率化と運用を支援します。

高度な攻撃に対する防御、検知、対応

極めて動的な仮想データセンター環境では、セキュリティ チームに視認性と管理性が不足することが多くあります。VMware Carbon Black Cloud Workload は、基本的な脆弱性評価とワークロードの保護強化に加え、業界をリードする次世代アンチウイルス(NGAV)、ワークロードの挙動監視、およびワークロードの Endpoint Detection and Response (EDR)を活用することで、そのような環境で実行されるワークロードを保護します。

セキュリティ チームは VMware Carbon Black の高度なワークロード保護機能を活用することで、攻撃者の振る舞いパターンを経時的に分析し、既知の正常なソフトウェアを操る攻撃も含め、過去に観察されたことのない攻撃も検知して阻止することができます。境界防御を迂回する攻撃があっても、セキュリティ チームは VMware Carbon Black Cloud Workload を使って、データ侵害が発生する前に攻撃を阻止できます。インフラストラクチャにセキュリティを組み込むことで、現在のシステム状態を簡単に監査して、セキュリティ状態の追跡とワークロードの保護強化を行えるようになります。また、vSphere 管理者と容易に連携し、既知の脆弱性への対処を行うことができます。

IT およびセキュリティ チームの運用の簡素化

VMware では、本質的なセキュリティというアプローチ、すなわちワークロードが展開されるすべてのインフラストラクチャにセキュリティを組み込むというアプローチでセキュリティを提供しています。インフラストラクチャ チームとセキュリティ チームは、VMware のこの独自のアプローチにより、重大な脆弱性や攻撃に迅速に対処できるよう一元化された情報を活用することで、セキュリティの強化と運用の簡素化の両立を実現すると同時に、チーム間の摩擦の解消とコラボレーションの促進を図ることができます。VMware Carbon Black Cloud Workload に移行することで、複数の単体セキュリティ ツールによるリソースの競合を解消し、既存の IT スタックおよびセキュリティ スタックの簡素化と統合を実現できます。

ヴイエムウェア株式会社 〒105-0013 東京都港区浜松町 1-30-5 浜松町スクエア 13F www.vmware.com/jp