進化するVMware Carbon Black
VMware Carbon Black Cloud™

VMware Carbon Black Cloud

膨大なデータを収集・蓄積し、独自のビックデータ分析で、未来のセキュリティ攻撃を予測・分析し、迅速に製品に反映します。
また、単一エージェント、単一コンソールで提供し高い管理性を実現します。

“Unfiltered”なデータ活用
フィルタリングせず“Unfiltered”データで収集して、分析に活用

ストリーミングアナリティクス
ストリーミングアナリティクスによる独自のビックデータ解析

統合されたコンソール
NGAVやEDR、スレットハンティングなどの様々な機能を単一エージェント、コンソールでの提供が可能です。

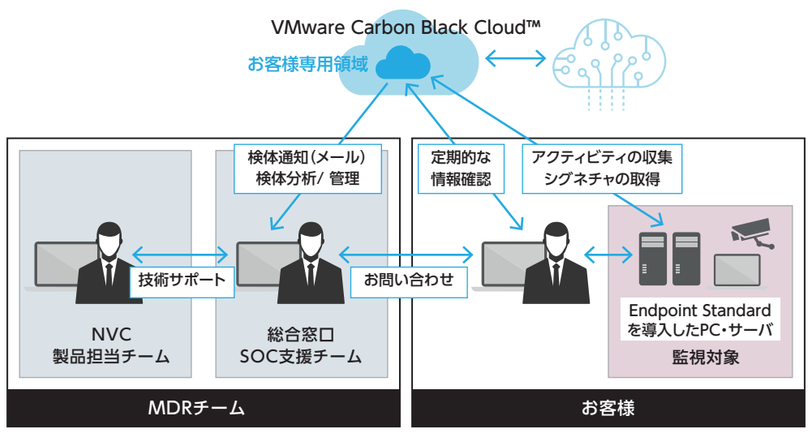
- Endpoint Standard — 次世代アンチウイルス+EDR
- Audit and Remediation — リアルタイムクエリ調査
- Enterprise EDR — 脅威ハンティング

運用もお任せ NVC セキュリティ運用サービス（MDR）

EDR機能を運用するには　SOC（Security Operation Center）やMDR(Managed Detection & Response)などのセキュリティ運用体制を整備する必要があります。
NVCでは、お客様さまの代わりに24時間/365日の体制でMDRサービスを提供。設計・構築から運用も含めたトータル提案を実現します。

サービス内容

- 脅威検知
- 脅威分析
- 脅威封じ込め
- 脅威除去支援
- 回復支援
- 月次レポート
- 脅威ハンティング：月に1回、ハッカーの攻撃手口や、各情報機関の注意喚起を基にした未検知の脅威の手動検索を実施

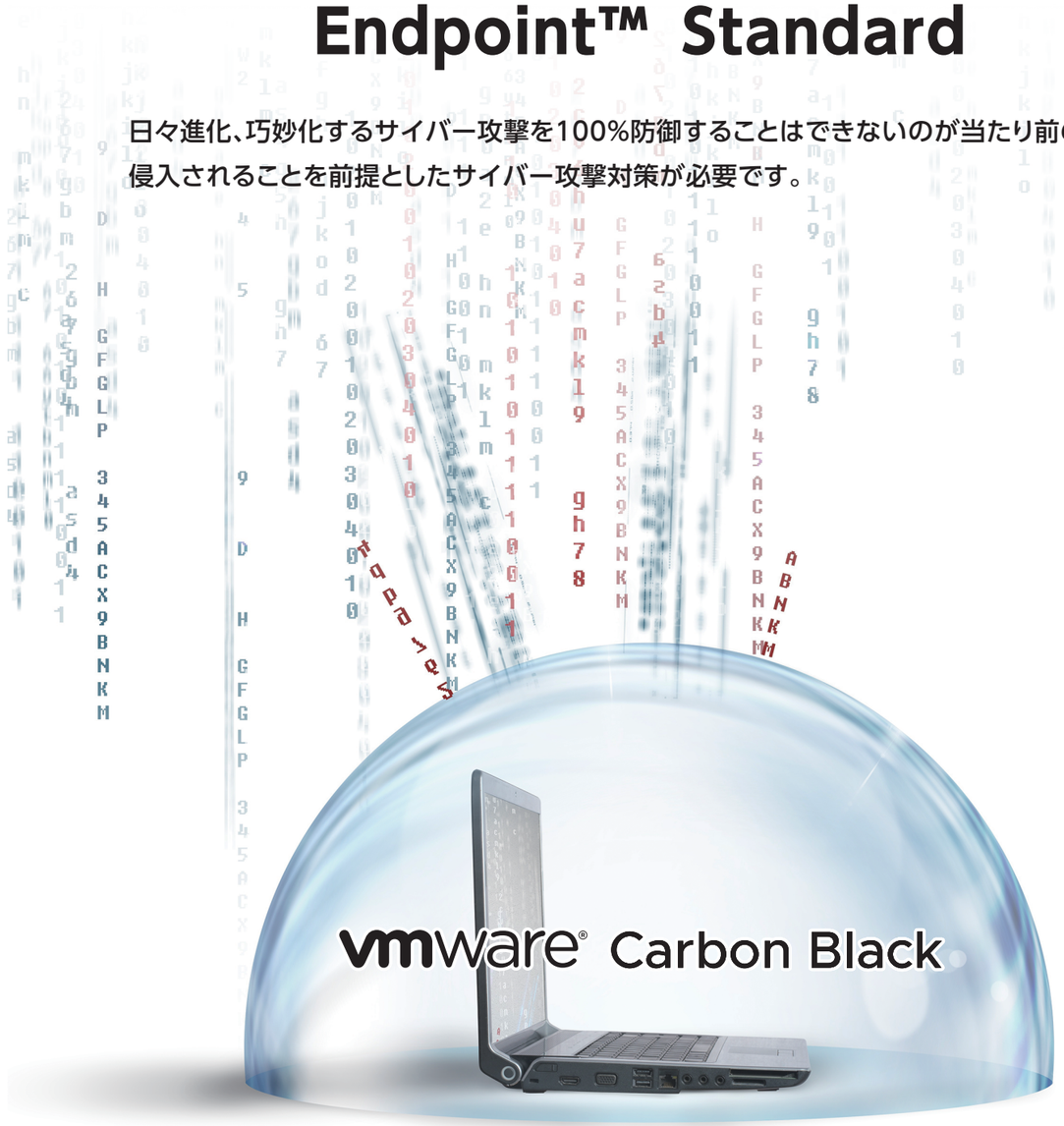


株式会社ネットワークバリューコンポネンツ
〒144-0035
東京都大田区南蒲田2-16-2　テクノポート大樹生命ビル
TEL:03-5714-2050　FAX:03-5714-2051
E-mail:sales@nvc.co.jp
https://www.nvc.co.jp/

NVC

VMware Carbon Black Cloud Endpoint™ Standard

日々進化、巧妙化するサイバー攻撃を100%防御することはできないのが当たり前の時代。
侵入されることを前提としたサイバー攻撃対策が必要です。

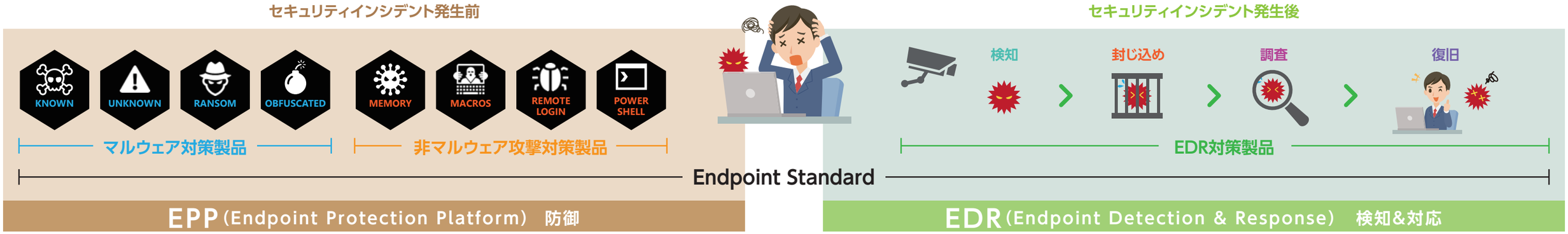


VMware Carbon Black Cloud Endpoint Standardは侵入前(EPP※1)と侵入後(EDR※2)の両方に対応する次世代エンドポイントセキュリティ製品です。

※1 Endpoint Protection Platform　※2 Endpoint Detection & Response

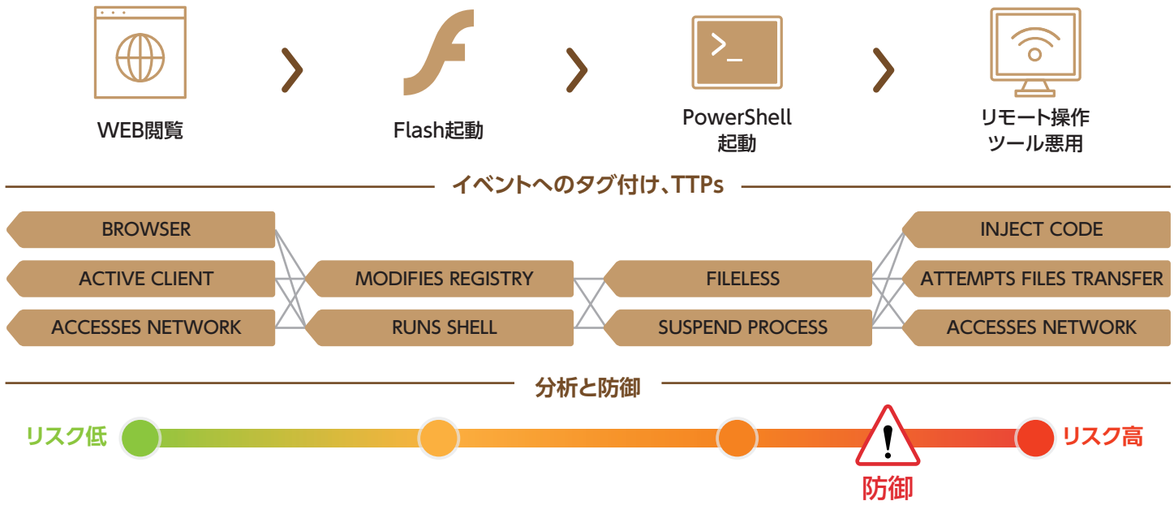
次世代エンドポイントセキュリティ
VMware Carbon Black Cloud Endpoint Standard

日々進化・巧妙化するサイバー攻撃を100%防御することは不可能であり、企業は侵入されることを前提とした対策が求められています。
そのため、昨今では侵入後のセキュリティインシデントの検知や調査・復旧にフォーカスしたEDR製品の導入が進んでいます。
VMware Carbon Black Cloud Endpoint Standardは、従来のEPP製品では防御できなかった未知のマルウェアや非マルウェア攻撃までを含めた防御（EPP）機能と、侵入後の検知・調査・復旧のEDR機能を併せ持ちます。Endpoint Standardだけで、侵入前と侵入後に対応することが可能です



特許技術の防御「ストリーミングプリベンション」

ファイルベースでの防御ではなく、端末の実際の挙動からマルウェアや非マルウェアの活動や非マルウェア攻撃を検出し、防御します。



セキュリティインシデント発生後の調査・復旧を支援する「EDR機能」

EDR機能は、防ぎきれなかった脅威を検出し、発生しているセキュリティインシデントの調査・復旧を支援します。

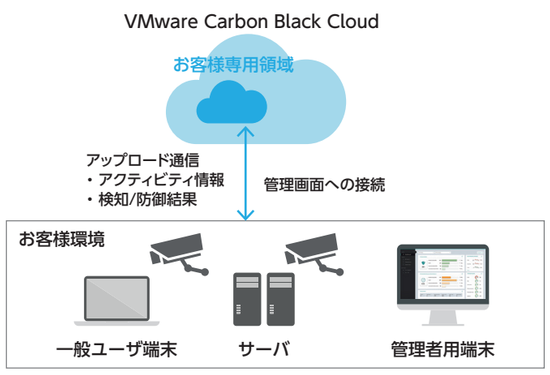
	検知	封じ込め	調査	復旧
EPPをすり抜けた時の対応方法の違い				
EDRなし	・検知不可	・人海戦術による対応	・人海戦術による対応	・人海戦術による対応
EDRあり	・収集したログから検出可能	・リモートによる隔離で即時分離	・収集されたログから調査・分析・特定	・原因ファイルの駆除
Endpoint Standardの主なEDR機能	・収集したアクティビティから脅威を検出 - クラウド上での解析(IoC/IoA含む) - ストリーミングアナリシス機能	・端末のリモート隔離 ・任意ファイルの起動禁止	・全EPのアクティビティに対する全文検索と可視化 ・拡大範囲と端末影響の特定	・マルウェアの削除 ・リモート操作機能によるリモートからの復旧支援
オプション機能	・Enterprise EDR	–	・Audit and Remediation ・Enterprise EDR	–

vmware® Carbon Black

「EDR」という言葉を作った旧Carbon Black社

旧Carbon Black社は、EDRのコンセプトを提唱した最初の企業です。Bit9社との合併や次世代アンチウイルスのConfer社の買収などでポートフォリオを増やし、各産業の企業での導入の他、75社以上のIR/MSSの事業者がMDRサービスのツールとしてCarbonBlackを採用しているEDRのパイオニアです。2019年にVMwareと統合し、現在に至ります。

Endpoint Standardのクラウド型のシステム構成



強化された機能(オプション)

①Audit and Remediation

EDRで収集したログに対する調査に加え、クエリを用いた端末内のリアルタイム情報に対する調査が可能になります。

②Enterprise EDR

カスタム検知ルールの提供や全ての挙動の可視化などEDR機能を強化し、スレットハンティング機能を提供します。

他次世代エンドポイントセキュリティとの違い

	Endpoint Standard	AI・機械学習型 アンチウイルス製品	従来型 アンチウイルス製品	EDR製品
既知のマルウェア	●	●	●	▲
未知のマルウェア	●	●	×	▲
未知のランサムウェア	●	●	×	▲
非マルウェア攻撃	●	×	×	▲
検知・調査（EDR機能）	●	×	×	●

▲ 検知のみ