

改めて見直す！ EDR が果たすべき役割と 求められる機能

Carbon Black Cloud の EDR 機能で実現する
エンドポイント強化策

藤田 平

VMware株式会社

セキュリティ事業部

シニアソリューションエンジニア



免責事項

- このセッションには、現在開発中の製品/サービスの機能が含まれている場合があります。
- 新しいテクノロジーに関するこのセッションおよび概要は、VMware が市販の製品/サービスにこれらの機能を搭載することを約束するものではありません。
- 機能は変更される場合があるため、いかなる種類の契約書、受注書、または販売契約書に記述してはなりません。
- 技術的な問題および市場の需要により、最終的に出荷される製品/サービスでは機能が変わる場合があります。
- ここで検討されているまたは提示されている新しいテクノロジーまたは機能の価格およびパッケージは、決定されたものではありません。

Agenda

Endpoint Detection and Response (EDR) について

EDR に求められる 3 つの要素

NDR ・ XDR について

Endpoint Detection and Response (EDR) について

EDR が果たすべき役割と必要性を再確認



EDR とは？

Endpoint Detection and Response の略称

- ネットワークに接続されている端末（Endpoint）を常時監視することで、
- サイバー攻撃による不審な痕跡を検知（Detection）し、
- 原因の調査および問題のある端末の隔離や修復などの対応（Response）を支援するもの



EDR が求められた背景

ゲートウェイやエンドポイントでは検知し防止できない攻撃が増えている

- 標的型攻撃、ファイルレス攻撃、LOL、ランサムウェア...etc

万が一防止できない攻撃が行われても、その攻撃の兆候から検知し対処を支援するためのツールが必要



EDR (Endpoint Detection and Response) をとりまく環境

EDR の導入状況

- 大規模の企業や組織での導入は進んでいる
- ただし全体で見るとウイルス対策製品のようにほぼすべての企業に導入されているとは言えない状況



EDR を導入しない理由

1. 検知してからの対応では遅い
2. 誤検知が多い
3. 検知だけで隔離や駆除は自動でやってくれない

「EDRは意味がない・・・？」
「EDRは役に立たない・・・？」
「EDRだけでは不十分・・・？」



EDR に対する評価

1. 検知してからの対応では遅い

- 「検知」と「防止」を混同していませんか？
- 「エンドポイント(Endpoint)」で「検知(Detection)」し「対応(Response)」するためのツール



EDR に対する評価

2. 誤検知が多い

- 不正行為は気づかれないよう通常動作に紛れて行われている
- 未知の攻撃を見つけるためには、起動するすべてのプロセスにおけるあらゆるイベントを収集する必要がある



EDR に対する評価

3. 検知だけで隔離や駆除は自動でやってくれない
 - EDR が検知するアラートには疑わしい行為と判断された正常な活動も含まれる
 - もし誤検知（過検知）で自動隔離してしまったら業務に多大な影響を与える場合がある

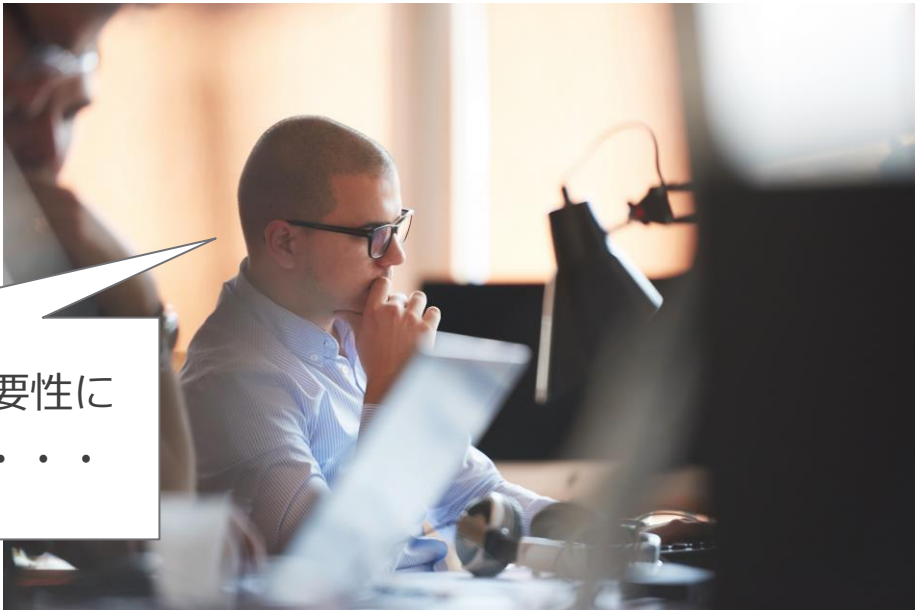


ということで、EDR を再認識

「EDR」という言葉だけで従来のアンチウイルス製品に置き換わる、何か新しいエンドポイントセキュリティ製品と捉えられがち

EDR はエンドポイントセキュリティ対策というという意味で間違っていないが、
「検知・対応」と「防止・自動対応」は別

- EDR そのもので防止したり自動的に対応したりするものではない
- あくまでもインシデント対応のプロセスの一部で証拠として利用されるもの



EDR は再認識したが、必要性についてはよくわからない・・・

乗り物のお話

最近の車には当たり前のように装備されているもの

= ドライブレコーダー

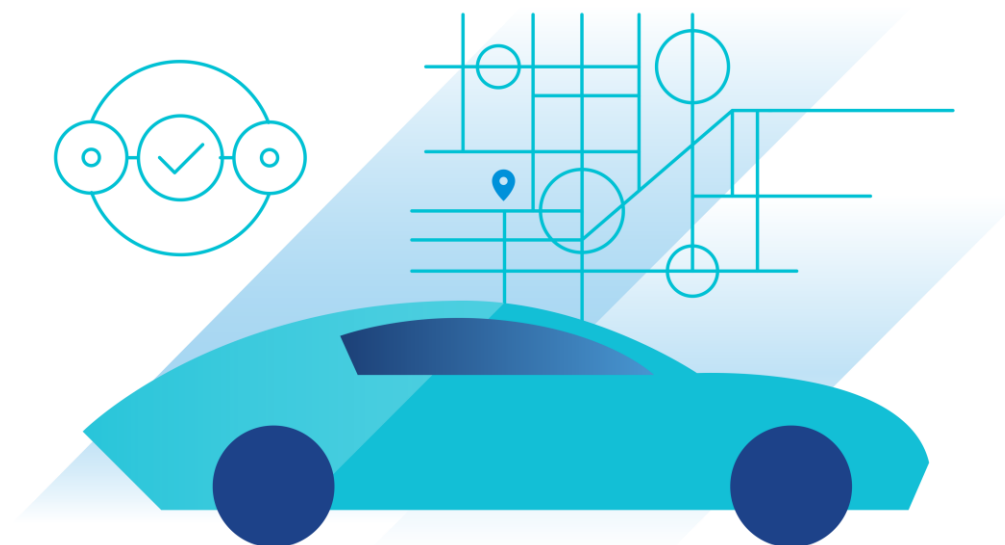
ドライブレコーダーの役割

= 事故やトラブルがあった際の証拠を「記録」する

ドライブレコーダーの役割

≠ 事故を「防止」する

- ドライブレコーダーそのもので事故を防止するものではない
- あくまでも事故対応のプロセスの一部において証拠として利用されるもの



“一般的”なドライブレコーダーについて再確認

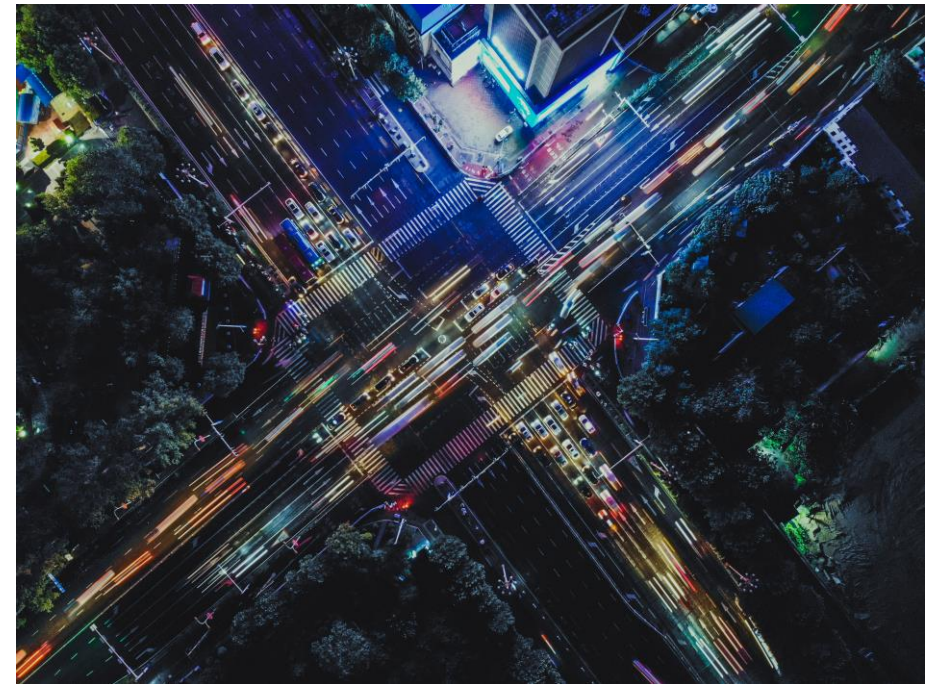
“一般的”なドライブレコーダー

= 車の外でどのような事が起こったのか？を記録する

- 信号を守っているのに車が突っ込んできた
- 突然人が飛び出してきた
- あおり運転

...etc

ここで、なぜわざわざ
「“一般的”なドライブレコーダー」
という表現をしたかと言いますと・・・



一般的なドライブレコーダーの役割を PC 端末に置き換えると・・・

一般的なドライブレコーダーは車外を記録しているが車内は記録していない

= PC 端末に置き換えると「外部との疑わしい行為」を「記録」すること

- PC 端末に対して外部のどこからどのような攻撃があったのか？
- 不正なWebサイトからマルウェアがダウンロード
- 不正なサーバに対して定期的に通信を行っている

では、一般的なドライブレコーダーは EDR と言えるでしょうか？

- PC 端末において、外部との疑わしい行為は記録するが、内部の疑わしい行為は記録していないということになる
- しかし疑わしい行為はPC 端末の“内部”でも行われている・・・



乗り物に搭載するカメラにはもう一つ種類があります

タクシーやバス、電車など公共交通機関に搭載している車内向けカメラ

- ドライバーや乗務員、乗客に対する暴力行為の抑止・記録
- ドライバーや乗務員による犯罪行為の抑止・記録

...etc



EDR はドライブレコーダー + 車内向けのカメラ

	個人	企業
乗り物	<ul style="list-style-type: none">● ドライブレコーダー<ul style="list-style-type: none">・ 乗るのは親族や知人ぐらい（他人は乗らない）・ 車内は基本安全・ 車内向けカメラは必要ない	<ul style="list-style-type: none">● ドライブレコーダー + 車内向けカメラ<ul style="list-style-type: none">・ 善人・悪人関わらずどんな人でも乗せる・ 車内で何が起ころのかわからない・ 車内での記録するカメラが必要
エンドポイント 端末	<ul style="list-style-type: none">● 従来型のアンチウイルス製品の付加機能<ul style="list-style-type: none">・ 個人のデータの取り扱いがメイン・ そもそも重要なデータは取り扱わない・ 外からの攻撃を防止することで十分・ 従来型のアンチウイルス製品を強化する保護機能<ul style="list-style-type: none">✓ クライアントファイアウォール✓ ホストベースの不正侵入防止・検知（HIDS/HIPS）✓ Web フィルタリング	<ul style="list-style-type: none">● EDR<ul style="list-style-type: none">・ 企業では重要なデータを含め業務上必要と思われるあらゆるファイルを取り扱う必要がある・ 中には見かけ上安全でも実際は不正なスクリプトが含まれているファイルも存在する・ 外からの攻撃を防止する従来型のセキュリティ対策では検知できない攻撃が増えている

考察：EDR の普及が進まない理由

「EDR は意味がない」 「EDR は役に立たない」 「EDR だけでは不十分」

→ 自家用車のイメージの延長線上で考えていることも必要性を感じていない一つの要因

- 車には事故防止の自動ブレーキシステムやトラブル対応のためのドライブレコーダーを装備
- 自家用車にはそれで充分かもしれません。
- しかし、タクシーやバス、電車などの公共交通機関では今や当たり前のように車内カメラが設置
- 車内カメラにて常に監視することによって、交通機関および乗客の安全・安心が保たれる



結論：改めて EDR の必要性を確認

公共交通機関では車内カメラが当たり前の時代のように

→ 企業や組織のエンドポイントにおいても EDR 導入が当たり前の時代となるべき

- エンドポイント内でのあらゆる不正行為をすべて記録し、重大インシデントが発生する前にその兆候を検知することで、被害を最小限に食い止めることが可能
- また万が一インシデントが発生した場合でも、エンドポイント上でなぜそのようなことが起きたのか調査し、適切な対処や各方面への説明責任を果たすことが可能
- 取り扱うエンドポイント、およびそこで取り扱うデータやそのデータの提供元に対する安全・安心が保たれる

今の時代、エンドポイントへの EDR 導入は必須！

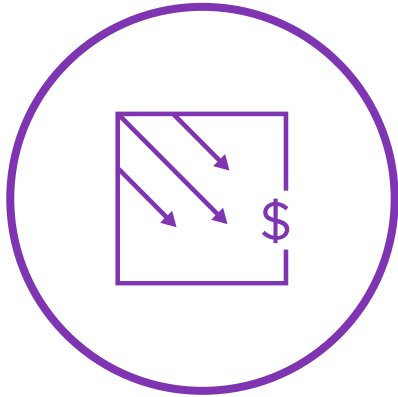


EDR に求められる 3 つの要素

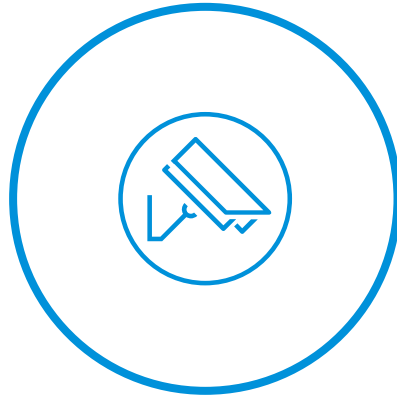
Carbon Black Cloud での EDR 機能のご紹介



EDR に求められる大切な 3 つの要素



導入・運用に
工数がかからない

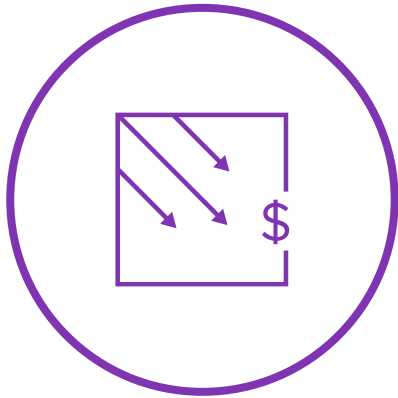


エンドポイントの
あらゆる行為を
把握



長く安全に
記録データを保持

管理工数の軽減を実現するために必要なこと



導入・運用に
工数がかからない

- 日本語による1つのコンソールで EDR 以外のセキュリティ機能もまとめて管理
- EDR 以外のセキュリティ機能もすべて1つのエージェントで簡単・迅速に展開
- 仮想環境に最適化されたソリューションで導入後すぐに検知能力を発揮

エンドポイント上の行為を把握するために必要なこと



エンドポイントの
あらゆる行為を
把握

- エンドポイント上で動作するすべてのプロセスの行為や不明なバイナリファイルをクラウドに自動保存
- IT ハイジーンや脅威ハンティングの実施
- リモートでのインシデント対応

長く安全に記録データを保持するために必要なこと

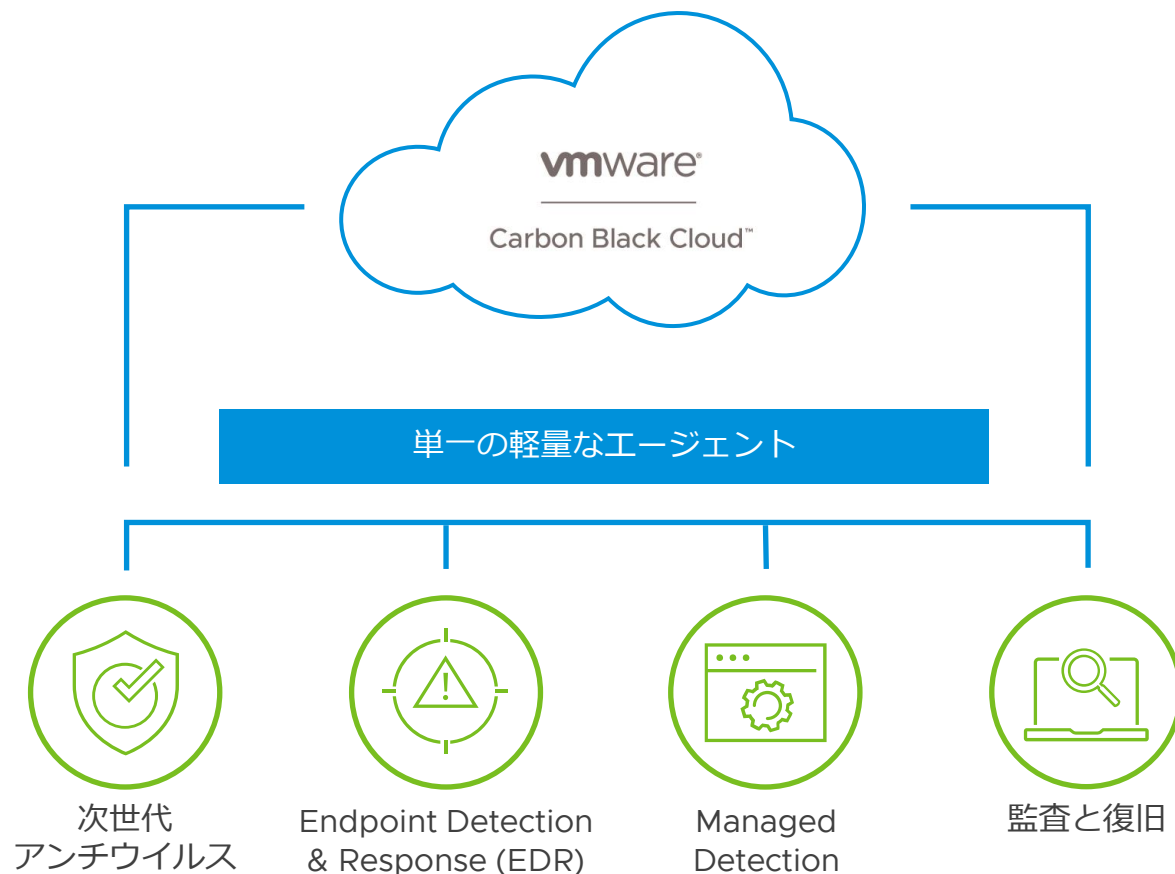


長く安全に
記録データを保持

- 日本のデータセンターに保存
- インシデント発生時より 1 か月遡っての調査が可能
- 外部のクラウドストレージへのデータ転送によりさらに長期間のデータ保存が可能

VMware Carbon Black Cloud ならすべて実現できます！

エンドポイントセキュリティに求められる機能を単一エージェント・単一コンソールで提供



- 軽量なシングルエージェントで EDR/NGAV を提供
- 日本語シングルコンソール（管理画面）にて管理可能
- クラウド上のデータベースに端末上のプロセスのすべての動作を保存
- クラウドデータセンターを日本にも設置
- 端末から収集したログは標準で30日間保存
- サーバ／クラウド／コンテナなどへの幅広い拡張性

VMware Carbon Black Cloud の構成

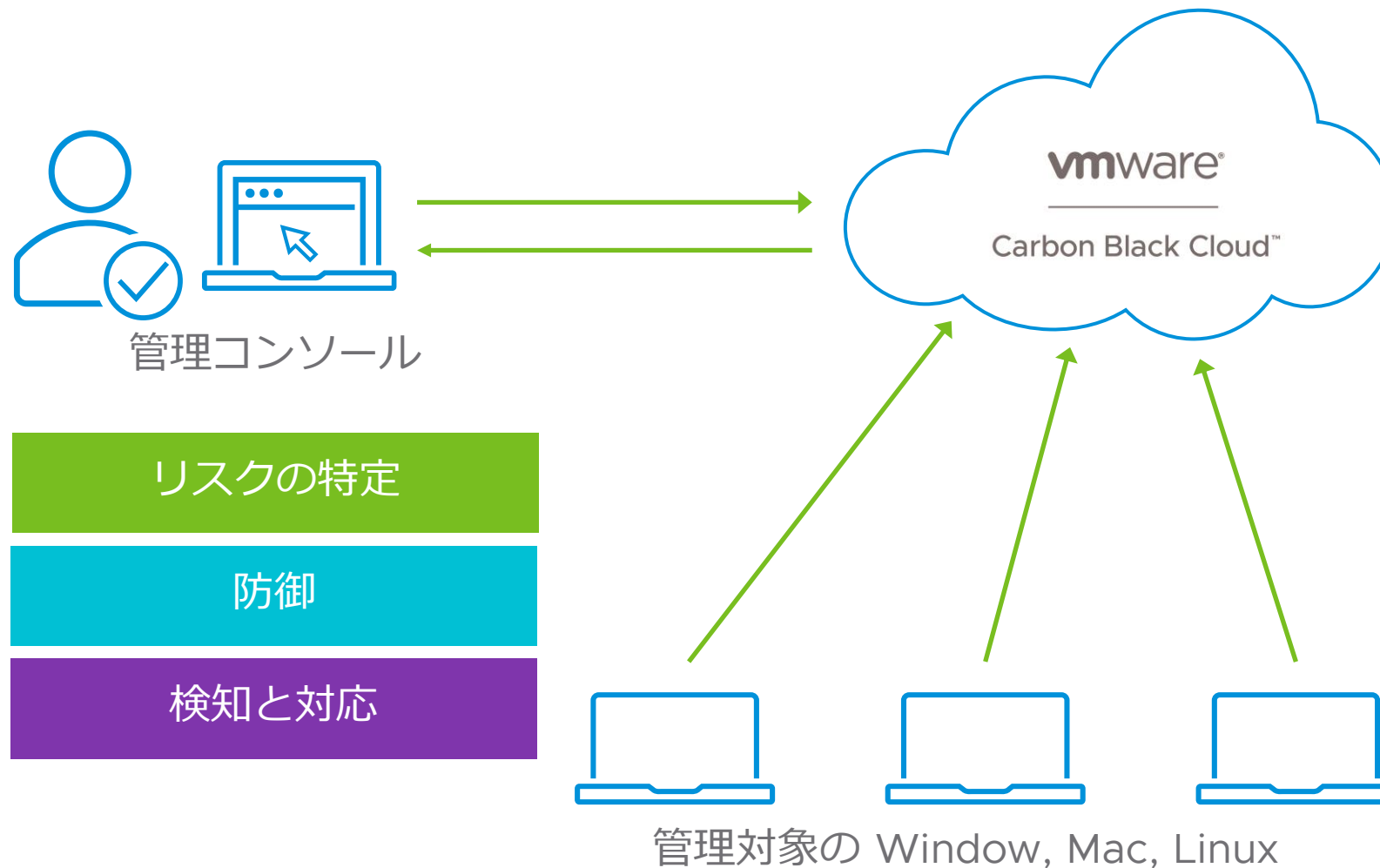
端末にセンサーをインストールし、クラウドで管理

Window, Mac,
Linux に対応

端末とクラウド上の
管理サーバとの
通信間隔は1分

Web ブラウザの
管理コンソール
から全端末の状況
を把握

管理、調査、隔離
事後対応



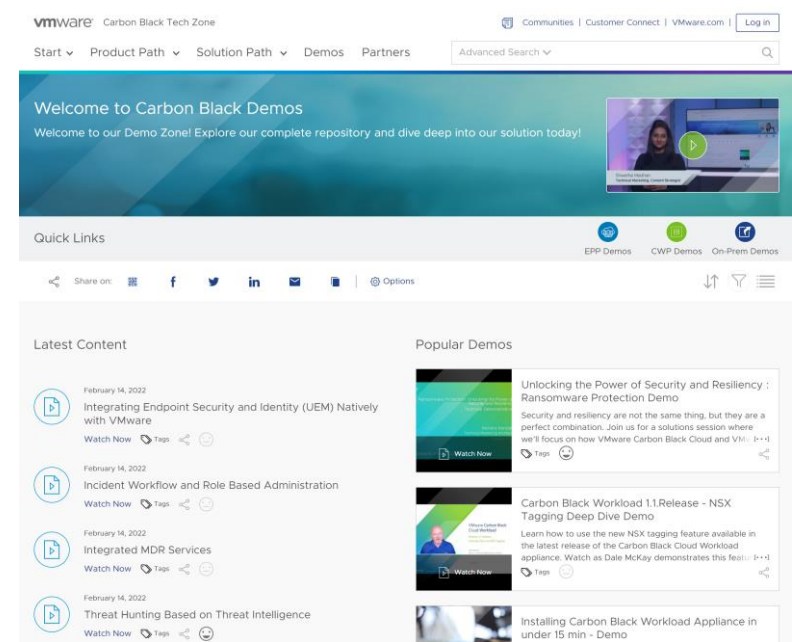
ハンズオンラボ・デモ動画のご紹介

VMware ホームページからの ハンズオンラボ（日本語）



<https://www.vmware.com/jp/products/carbon-black-cloud.html>

Carbon Black Tech Zone からの デモ動画（英語）



<https://carbonblack.vmware.com/carbon-black-demonstrations>

NDR・XDR について

VMware セキュリティの中での Carbon Black
の位置づけ

XDR のお話

最近耳にするキーワード

→ EDR よりも XDR

そもそも XDR とは？

- XDR = EDR と NDR の組み合わせを指すことが一般的
- EDR は NDR とともに XDR の実現に不可欠

EDR に加えて NDR、XDR が必要とされるシーン

- 脆弱性を悪用した攻撃やラテラルムーブメント（端末間での横展開）、外部への情報漏えいなど、組織全体で一連の攻撃をエンドポイントからネットワークまで俯瞰的に調査・分析する必要がある場合



電車で例えると・・・

事故や事件があった場合、電車内での犯罪と犯人の行動の関係性を把握することが可能

- 例えば電車内で事件があった場合
 - 犯人がいつ、どの駅から乗車したのか、電車に乗るまでの間、犯人はどのような行動をしていたのか、疑わしい行為はなかったか（＝ 駅構内の防犯カメラ）
 - 電車内でどのような犯罪行為が行われたのか、犯罪行為の経緯、および電車内の被害状況はどうか（＝ 車内カメラ）
- 駅に入ってから電車内の犯罪行為までを俯瞰的に把握するためには、駅の構内から電車内まで網羅したカメラからの情報が必要



NDR と EDR はお互いに補完しあうもの

駅構内の監視カメラ、電車内の監視カメラそれぞれの記録情報から犯罪行為を俯瞰して把握

→ ネットワークとエンドポイントの両方の状況から不正行為を俯瞰して把握

- ネットワークの状況を記録 = NDR
- エンドポイントの状況を記録 = EDR
- 両方を俯瞰して分析 = NDR + EDR = XDR

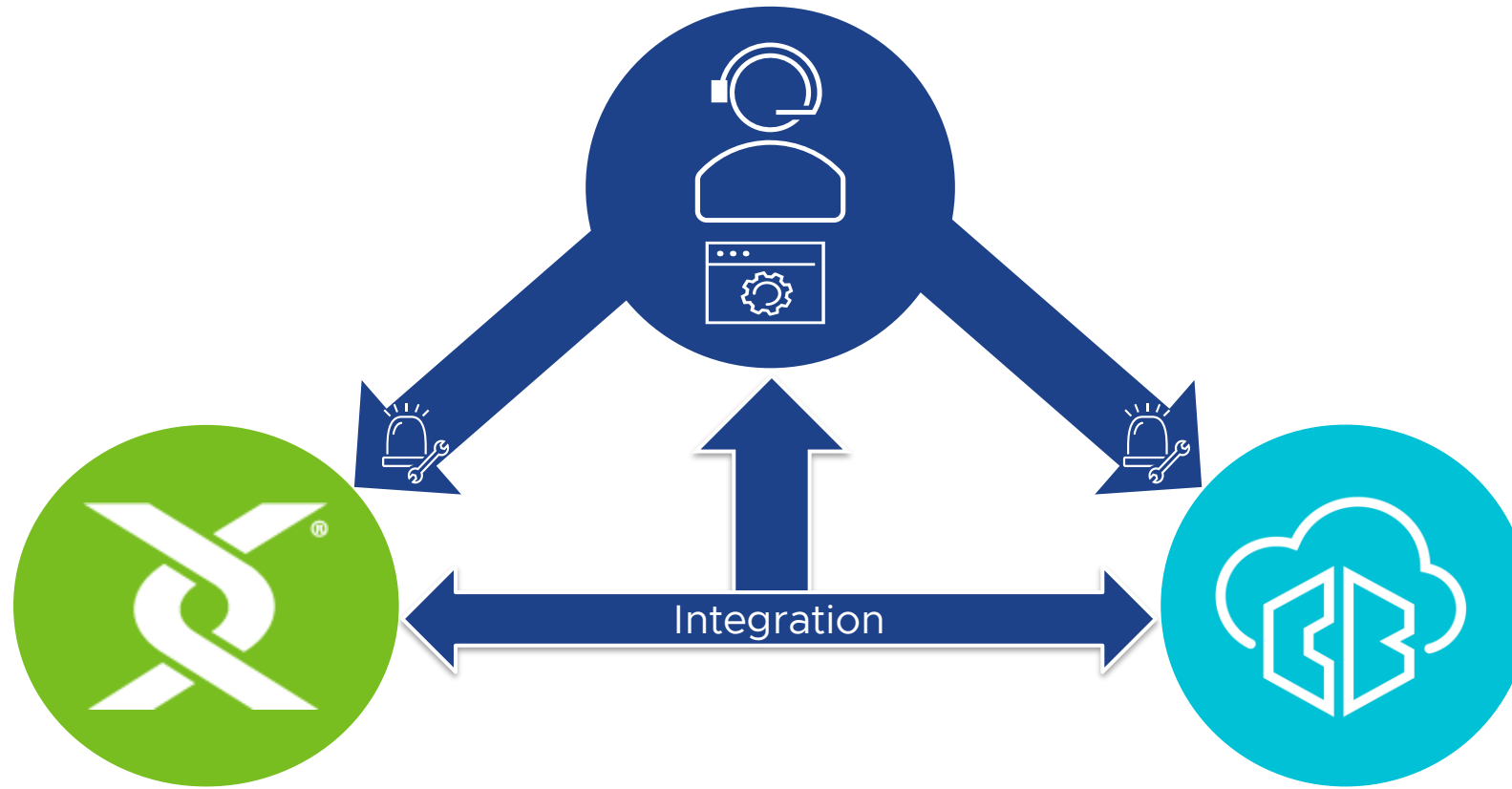
つまり、XDR を実現するためには NDR、EDRは必要な要素

- NDR は ×、EDR は ×、ではない
- NDR と EDR がお互いに補完し合い XDR を実現する



VMware は EDR、NDR 両方提供できるベンダー

Security Operation / Incident Response



Network Detection & Response

Endpoint Detection & Response

この後開催する関連セッションのご紹介

EDR と NDR のエキスパートが徹底討論！

「〇〇 DR 不要論」それ本当ですか？

15:00 - 15:40

日々の商談で多くのお客様からいただくご質問の一つが「EDRがあればNDRは不要ですか？（またはその逆）」というものです。双方の技術ともまだまだ普及段階ということもあり、利用目的やその用途、導入効果等の理解が浸透していないのが実態です。本セッションでは、EDR と NDR のエキスパートが、それぞれの技術そのものの特徴に加え、それらの役割分担やインテグレーションによる相乗効果、および EDR と NDR の双方を提供している稀有な存在である VMware が描く未来像などについて、対談形式で語り尽くします。

大久保 智
VMware株式会社
セキュリティ事業部
シニアソリューションエンジニア

橋本 賢一郎
VMware株式会社
セキュリティエバンジェリスト

こちらをあわせてご参加ください！！



Thank You