

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？

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



自己紹介

名前

大久保 智（おおくぼ とも）, CISSP

所属：

vmware® ← Carbon Black.

ネットワーク&アドバンスドセキュリティビジネスグループ
リードセキュリティソリューションエンジニア

経歴

約10年に渡り、セキュリティ製品のプリセールスエンジニアを担当
直近4年間はEDR に注力

2018 年に Carbon Black 入社

2019 年にVMware によるCarbon Black 買収に伴い、VMware 入社



自己紹介

橋本 賢一郎（はしもと けんいちろう）

所属 : **vmware**® ← **lastline**
VMware株式会社
セキュリティエバンジェリスト

経歴 : ✓ ネットワーク業界で20年間、プリセールスエンジニアや営業を担当し、その後セキュリティ業界に転身
✓ セキュリティ業界では、サンドボックスやプロキシ、IPSなどを担当し、前職はラストラインで北アジア全般を担当

社外活動① : **IPA**
情報処理安全確保支援士 試験委員

執筆 : ✓ 電子情報通信学会 インターネットアーキテクチャ研究会
✓ ソフトウェア デザイン ネットワークセキュリティ関連



社外活動② : **Interop Tokyo** #show.net ← **SHOWNET**
ShowNet NOCチームメンバー



社外活動③ : **SDN Japan ONIC Japan**
Open Networking Conference Japan 実行委員



最近の脅威動向と対策上の課題

日系企業の 昨今のセキュリティインシデント

大手企業で十分な対策をしても被害に遭っています

	業種	公表時期	概 要
1	アニメ制作会社	2022 年 3 月	2022年3月に改ざんされたダウンロードサイトから、悪意あるソフトウェアが同時にダウンロードされ、サーバやPCがランサムウェアに感染し暗号化された。アニメ制作が継続できず、 新作の放送遅延や関連グッズの販売時期に影響 。
2	自動車部品製造	2022 年 3 月	2021年12月のメキシコ工場で受けたランサムウェア「Rook」の攻撃に続き、ドイツの子会社でランサムウェア「Pandra」の攻撃を受け被害に。157,000件/1.4TBの データがDarkWeb上でリーク された。
3	タイヤメーカー	2022 年 2 月	2月27日にアメリカ子会社にランサムウェア「LockBit 2.0」の攻撃を受け被害に。身代金要求に応じずに リークサイトでファイルが公開 された
4	自動車製造業	2022 年 2 月	樹脂部品の仕入れ先企業のシステム障害によって、週末を含む二日間でも復旧せず、国内14工場、28ラインの 生産を一日間停止し、13,000台の生産に影響 。 子会社のVPN脆弱性を悪用 され侵入し、ランサムウェア攻撃と公表。
5	IT・電気工事	2022年 1 月	2021年大晦日の未明に、 log4jの脆弱性を悪用 した攻撃を受け、お客様取引情報等の データの漏洩 と「Night Sky」による 暗号化の被害
6	病院	2021年 10 月	パッチ未適用のVPNの 脆弱性を悪用 、リークアカウントを利用して侵入 LockBit2.0によって電子カルテデータなどランサムウェアの二重脅迫され、 二ヶ月間手作業で病院業務を強行 。約 二億円 をかけて再インストールして復旧

インシデントから見えてくるキーワード

脆弱性の悪用

ラテラル
ムーブメント
サプライチェーン

事業継続の阻害

早期発見
早期（暫定）対策

移動するインフラの
常時監視

早期発見・対策
実行阻止
バックアップ

対策するための考え方と適用箇所と技術と

FORRESTER®
Zero Trust



MITRE
ATT&CK™

MITRE
DEFEND™

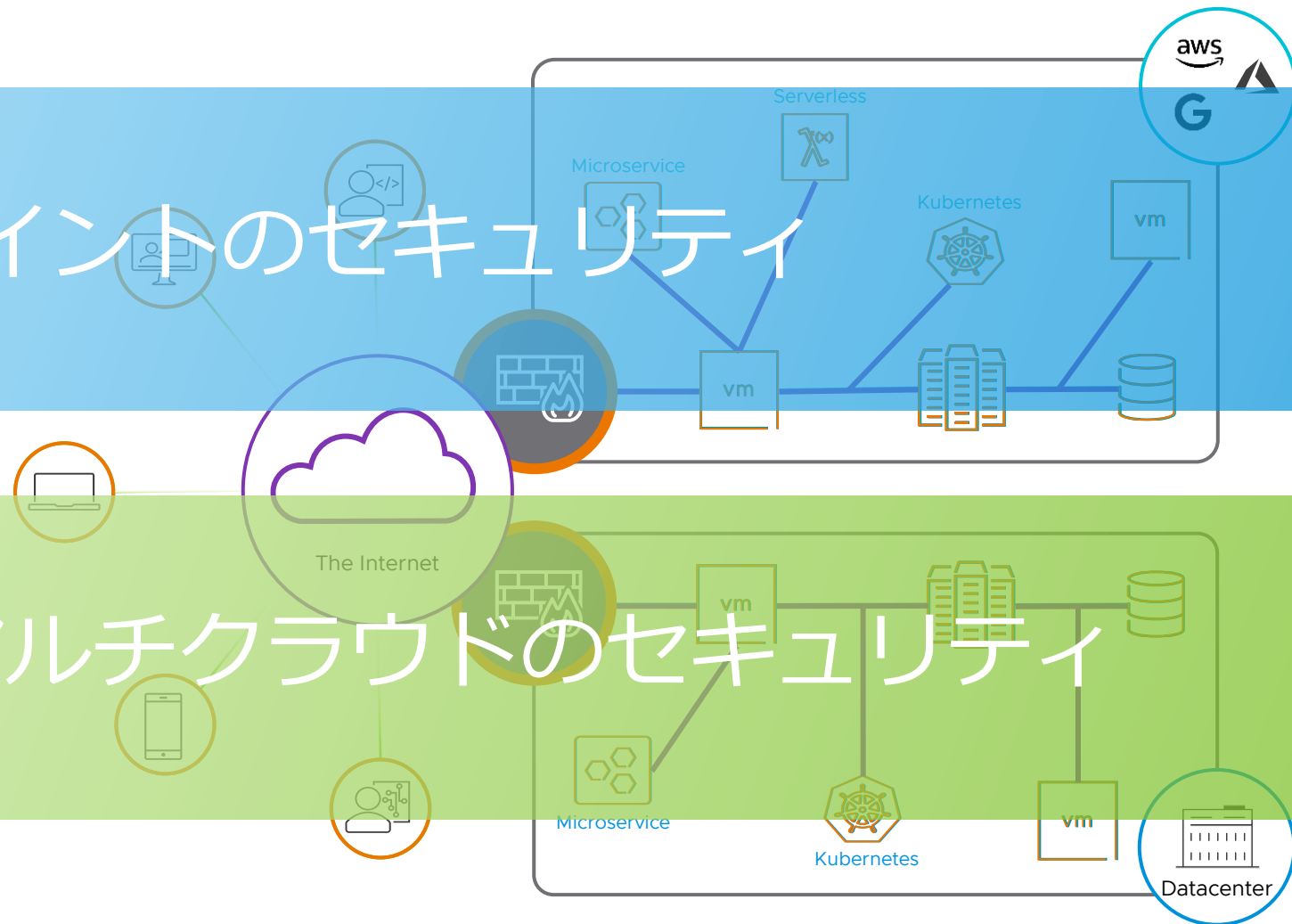
MITRE | Shield


エンドポイントのセキュリティ

ハイブリッド・マルチクラウドのセキュリティ


vmware®

©2022 VMware, Inc.





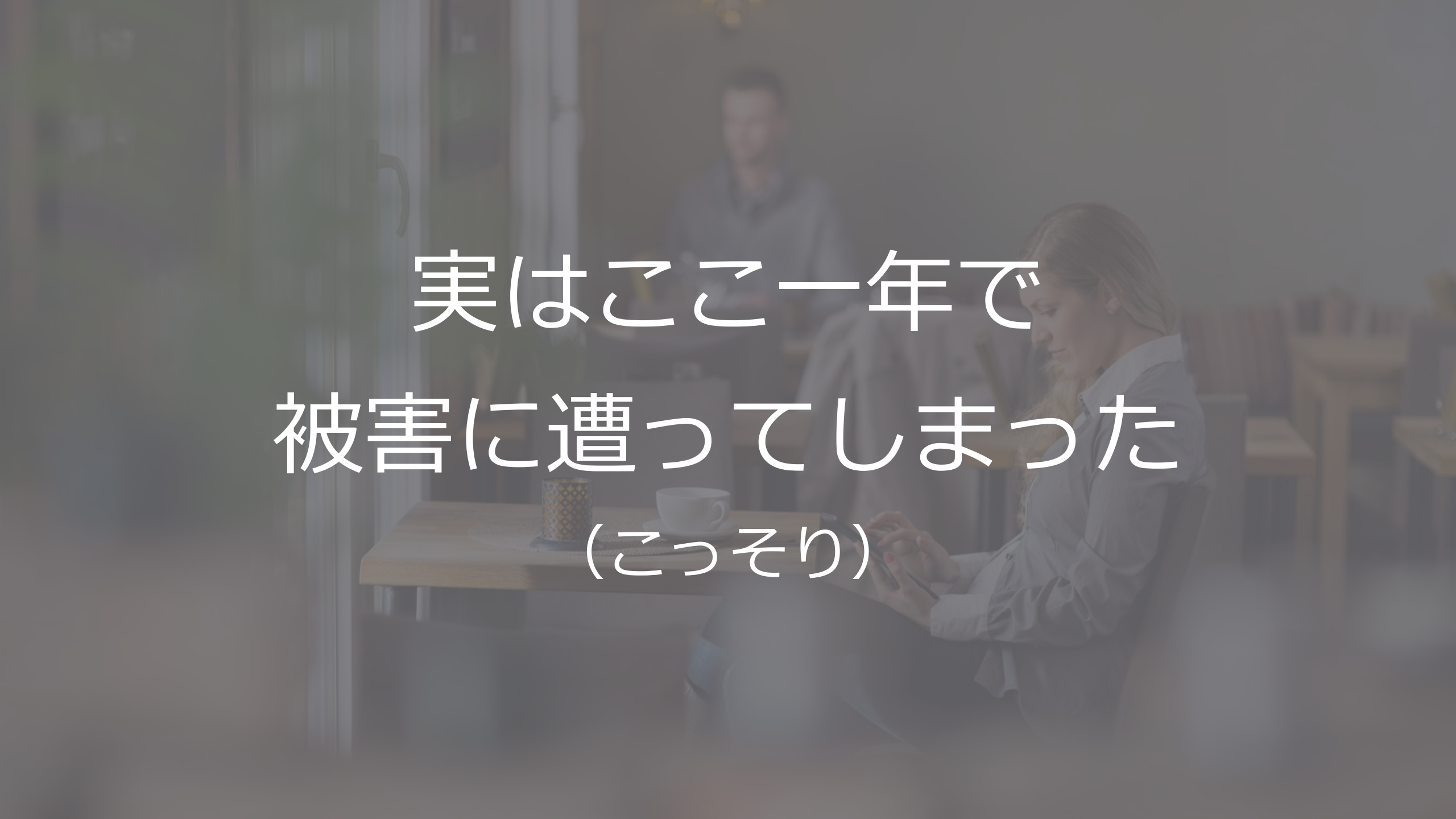
皆さんにご質問



EDR or NDR 導入してありますか？



導入してから何年経ちますか？

A woman with long blonde hair, wearing a light blue button-down shirt and dark pants, is sitting at a wooden table in a cafe. She is looking down at a smartphone in her hands. On the table, there is a white coffee cup on a saucer and a small patterned container. In the background, a man is sitting at another table, looking towards the camera. The scene is dimly lit, with a soft glow from the windows.

実はここ一年で
被害に遭ってしまった
(こっそり)

よくある質問と誤解

よくある質問・誤解

EDR編

誤解

01

EDR = EPP ?

No

EDR ≠ EPP

EPP = Endpoint Protection Platform
防御機能を有するツール

EDR = Endpoint Detection & Response
インシデント対応支援ツール

よくある質問・誤解

EDR編

誤解

02

EDRを導入すれば 万事解決？

No

EDR ≠ 魔法のツール

調査内容の向上やインシデント対応の
迅速が望めるのは確か

現場にとっても上層部にとっても
導入効果が見込めるツール

よくある質問・誤解

NDR編

誤解

01

EDRがあれば

No

目的とする保護対象と役割が違う

NDRはいらないよね

02 EDRを...

Yes & No

ベストは両方, ただし環境や利用者依存

先に導入すべきだよね

EDRとNDR, 得意・不得意

EDR編

得意：エンドポイント上の監視

テレメトリとしての役割

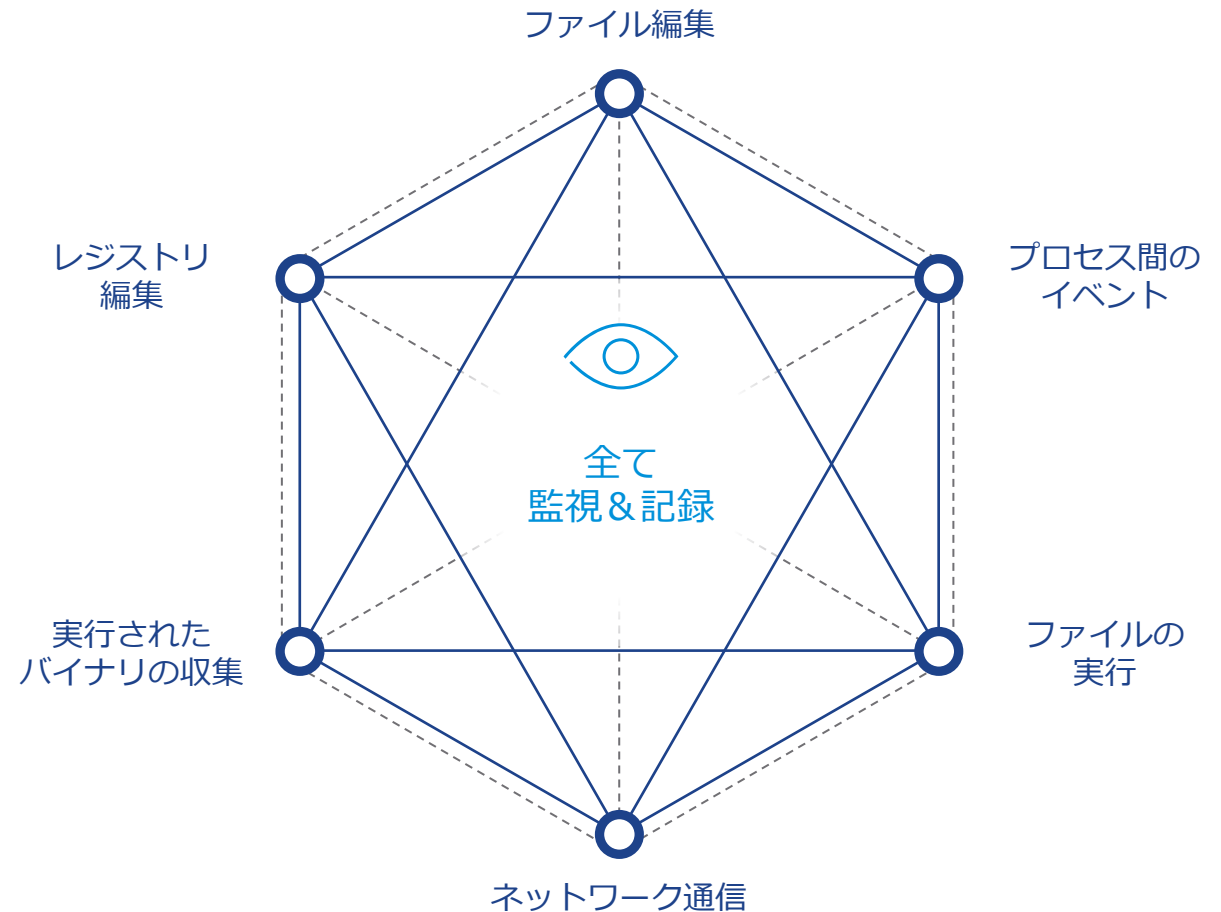
常時記録 & 集中管理

根本原因の特定

影響範囲の絞り込み

攻撃パターンの可視化

時間を遡った調査



EDRとNDRの得意・不得意

NDR編

「Response」するための証拠と詳細情報とは

NTA: Network Traffic Analysis
NDR: Network Detection & Response

シグネチャを利用せずに、不審なトラフィックを検出する

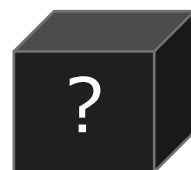
NTAや一般的なNDRの実装



シグネチャ



機械学習



ブラックボックス



証拠不十分・詳細不明



判断できない

VMware NDRの実装

シグネチャも利用して、不審なトラフィックを検出し組み立てる



シグネチャ



IDS/IPS



NTA



サンドボックス



機械学習



✓ シグネチャ
✓ パケット
✓ 3ウェイハンドシェイク
✓ HTTPレスポンスコード など



判断して的確な
対処が可能

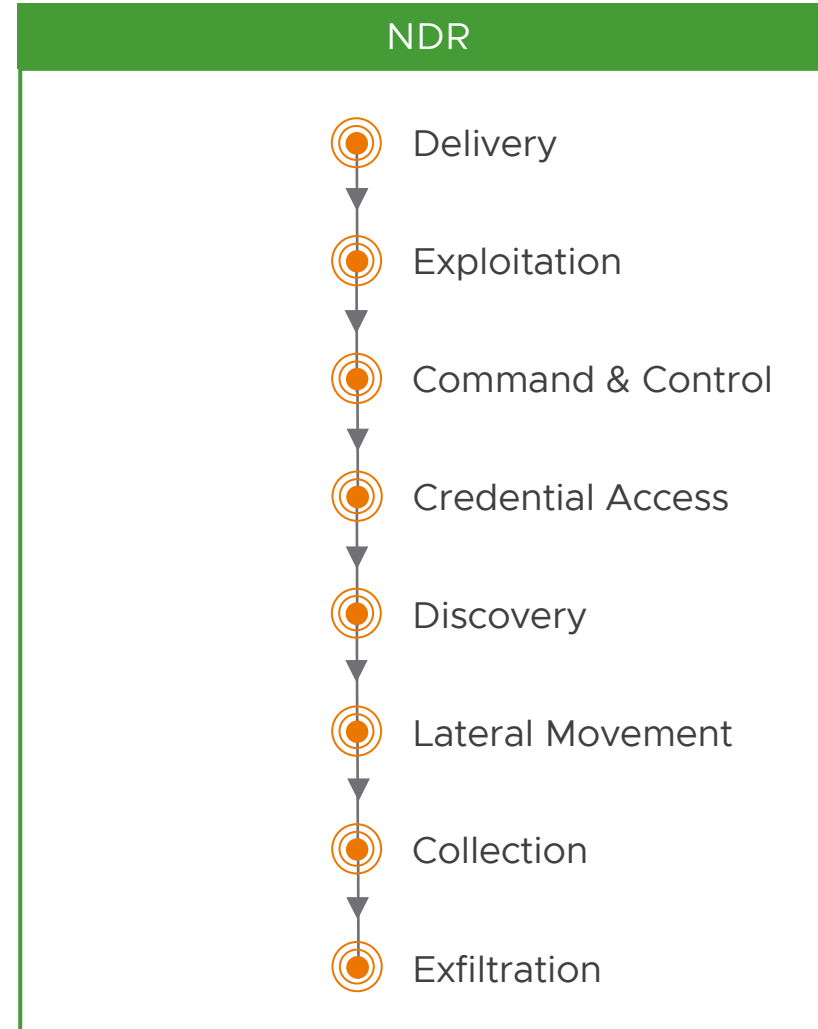
得意：ネットワーク上での振る舞いとエンドポイントの特定

AI解析によるNDR（Network Detection & Response） - NOT NTA

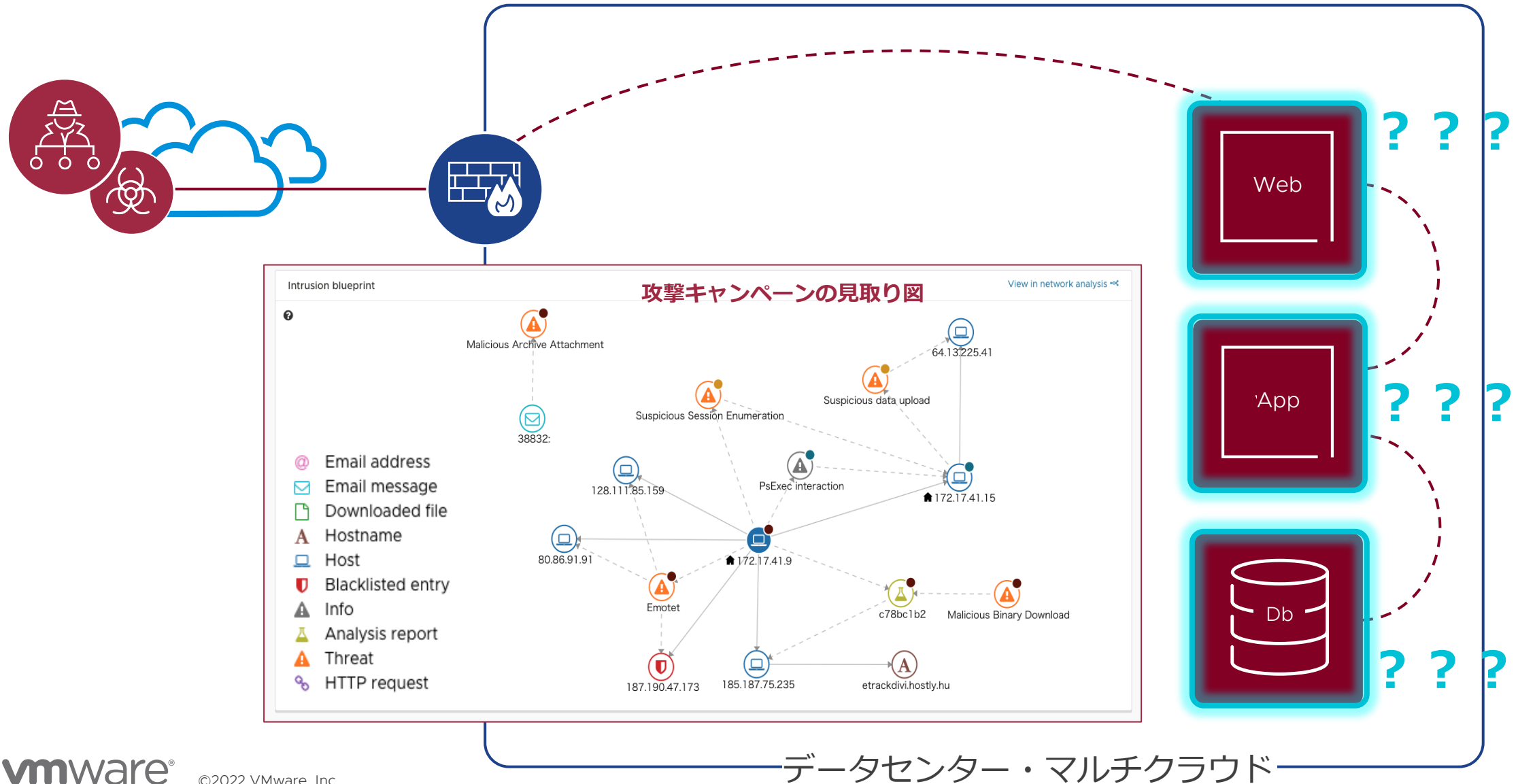
IDS/IPS				
<alert>	<alert>	<alert>	<alert>	<alert>
<alert>	<alert>	<alert>	<alert>	<alert>
<alert>	<alert>	<alert>	<alert>	<alert>
<alert>	<alert>	<alert>	<alert>	<alert>
<alert>	<alert>	<alert>	<alert>	<alert>

サンドボックス				
<alert>	<alert>	<alert>	<alert>	<alert>
<alert>	<alert>	<alert>	<alert>	<alert>
<alert>	<alert>	<alert>	<alert>	<alert>
<alert>	<alert>	<alert>	<alert>	<alert>
<alert>	<alert>	<alert>	<alert>	<alert>

NTA				
<alert>	<alert>	<alert>	<alert>	<alert>
<alert>	<alert>	<alert>	<alert>	<alert>
<alert>	<alert>	<alert>	<alert>	<alert>
<alert>	<alert>	<alert>	<alert>	<alert>
<alert>	<alert>	<alert>	<alert>	<alert>



不得意：エンドポイントの中まではわからない



EDRとNDR, どう使い分ける？

SOC Visibility Triad - Gartner

三種の神器：EDRとNDRの定義

Gartner社が提唱する、SOC運用で重要な3つの要素

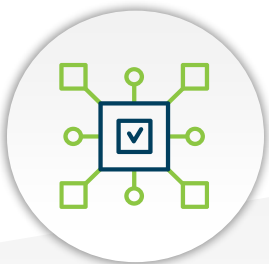
Use Cases



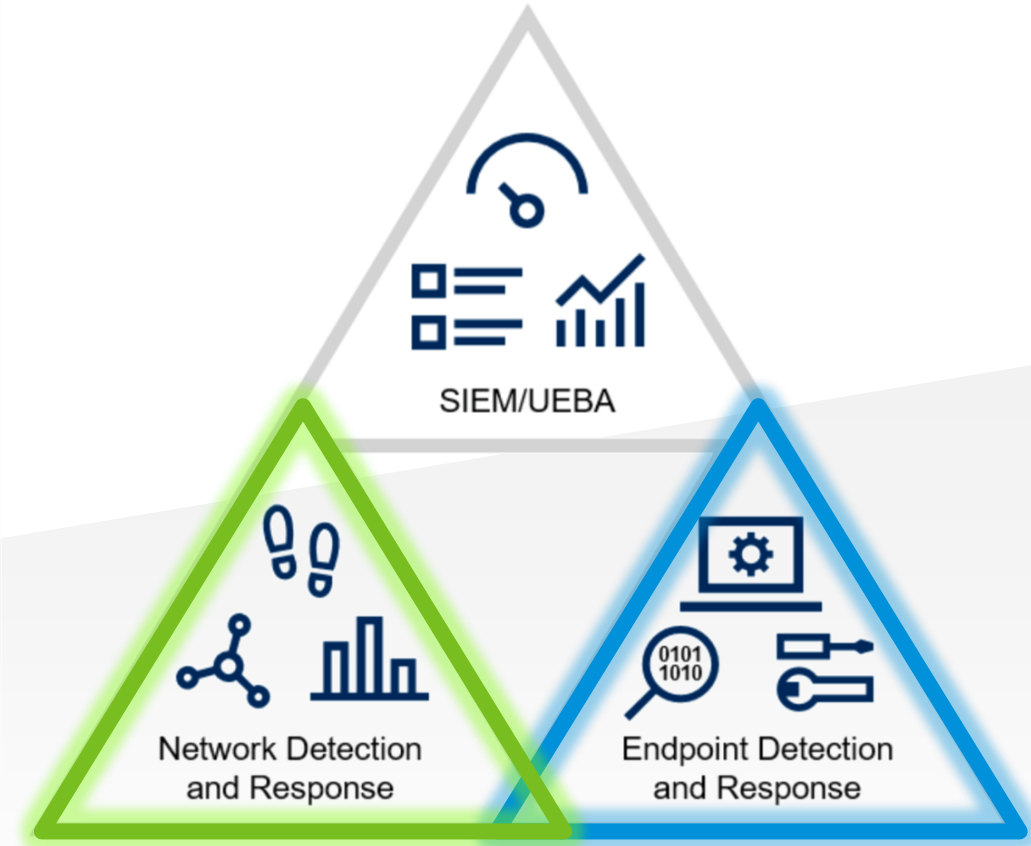
脅威検出の向上



脅威追跡と捕獲
への対応



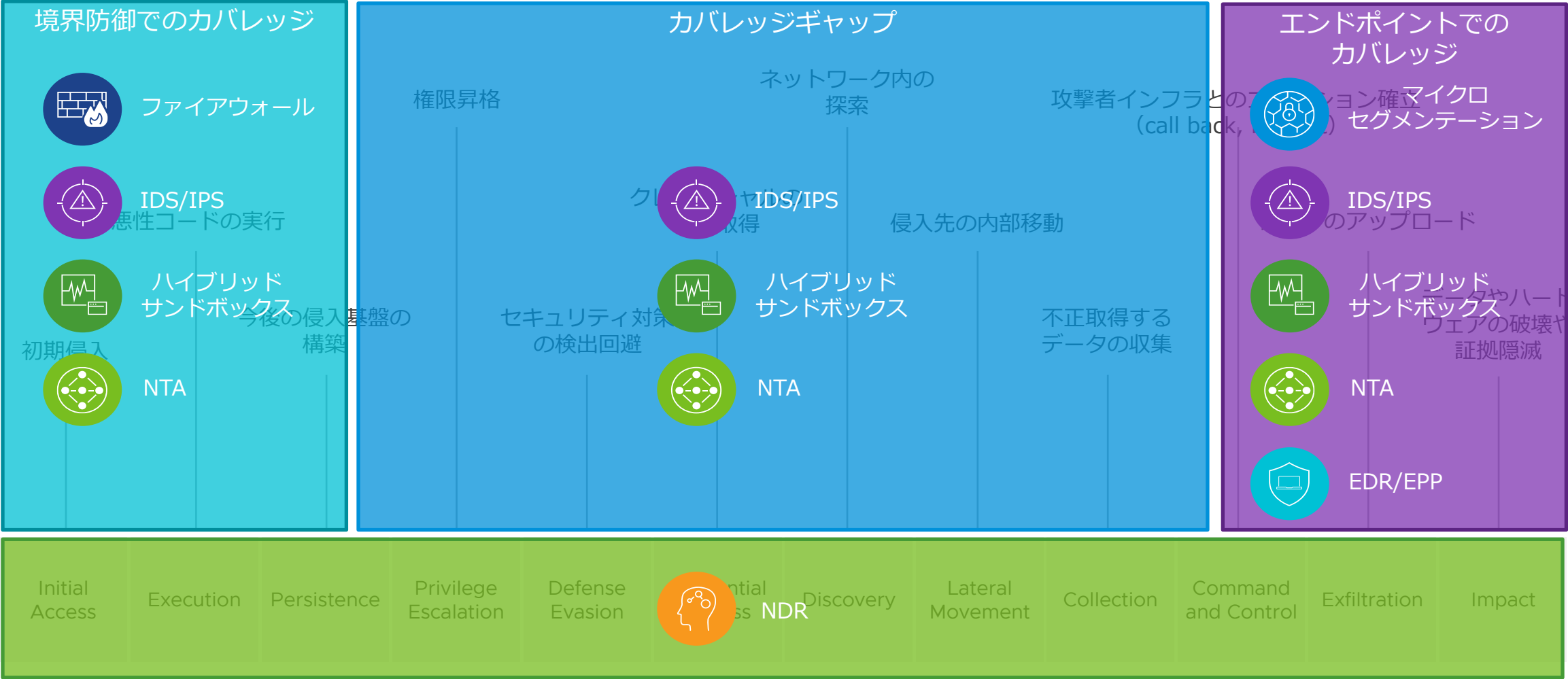
インシデント
レスポンスの向上



Functions	EDR	NDR
Detection	不審なシステムの振る舞いを、エンドポイントレベルで検出	不審なネットワークの振る舞いをネットワークレベルで検出
Response	危険な行動を阻止し、過去に何が実行されたのか、その証拠から侵害を受けたシステムを復旧するための対処方法を提供	過去に何が実行されたのか、その証拠から防御設定の自動化や、脅威ハンティングやIRなどのマニュアル対応など、対処に必要な情報を提供

二つの〇DRによってカバレッジギャップを排除

NDRでデータ侵害のライフサイクル全体をカバー



二つの○DRとそれぞれに最適な利用方法について

EDR (Endpoint) とNDR (Network)

→ EDRによる調査

エンドポイント内で、

どのプロセスが、いつから存在し、いつ何を行ったのか、
を調査するためのツール

NDRによる常時監視

ネットワーク上で、

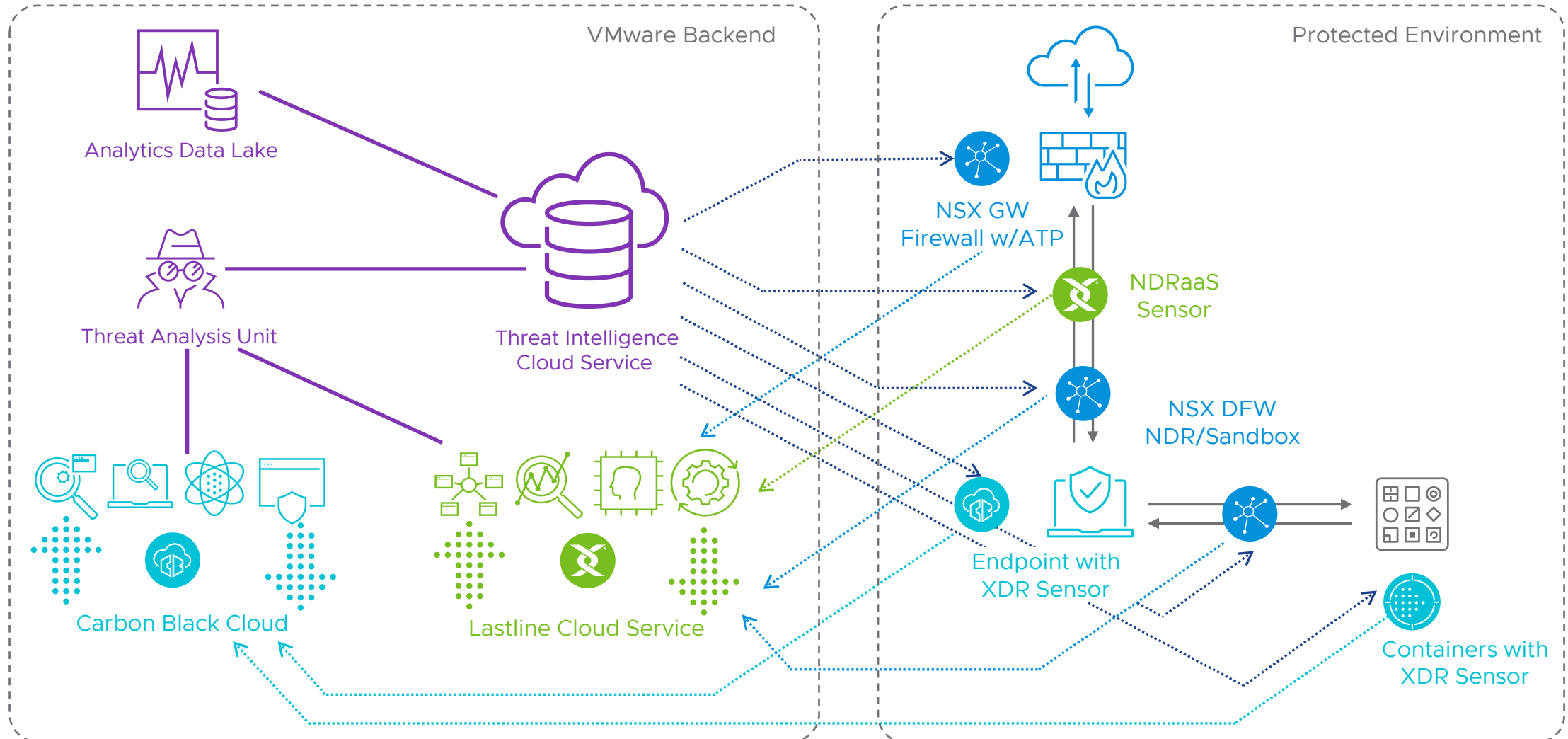
どのエンドポイントが、いつ誰から何をされて、他のどのエンドポイントへ拡散したのか、
を調査するためのツール

→ NDRによる調査

今後...のE/NDR (XDR) ?

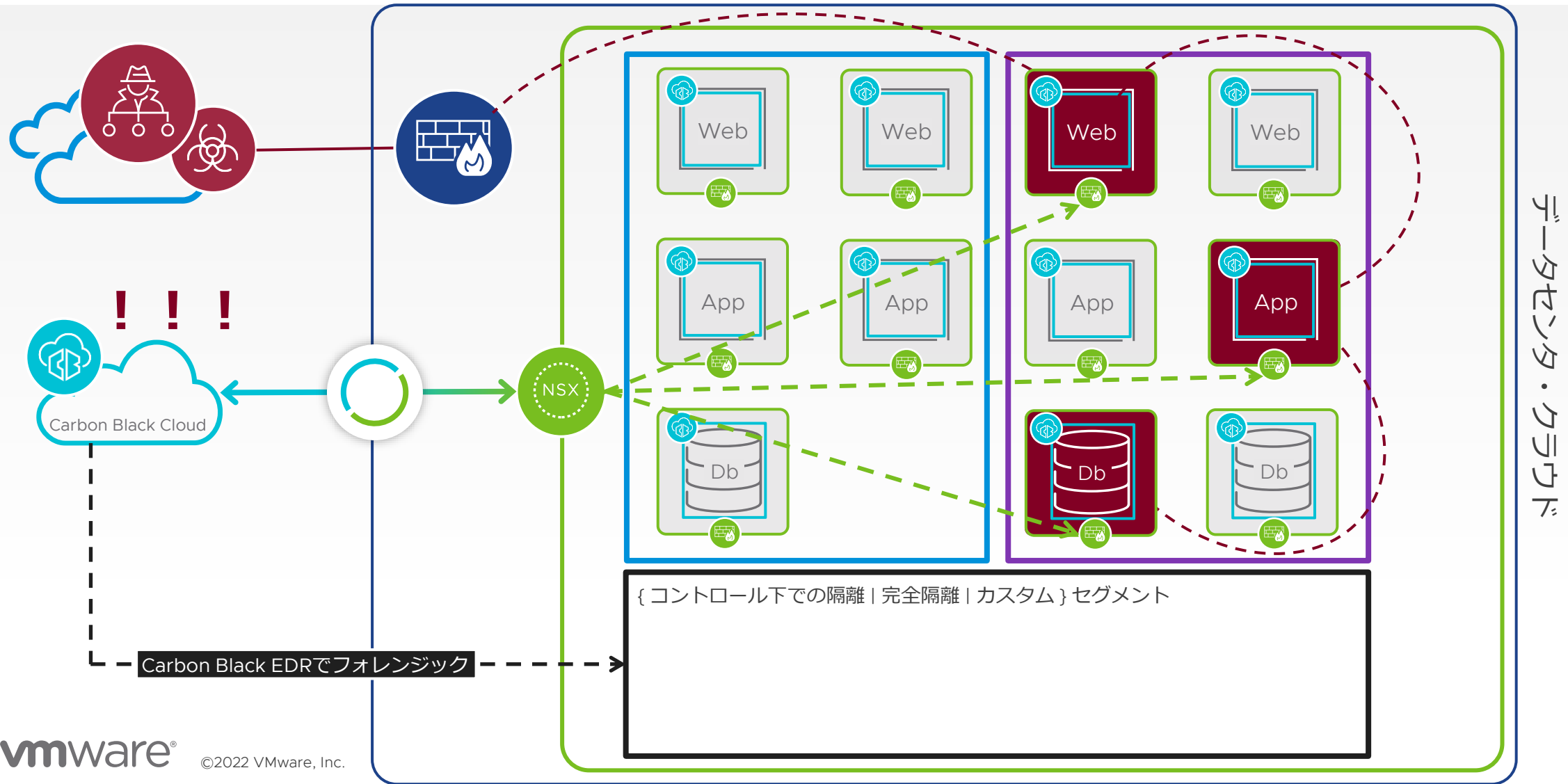
VMware XDR Architecture

エンドポイントとネットワークの脅威情報や詳細プロセスを共有して対処



EDRでの脅威検出をトリガーにネットワークで制御して対処

Integrated with Carbon Black Cloud Workload



Carbon Blackと連携した仮想パッチの適用

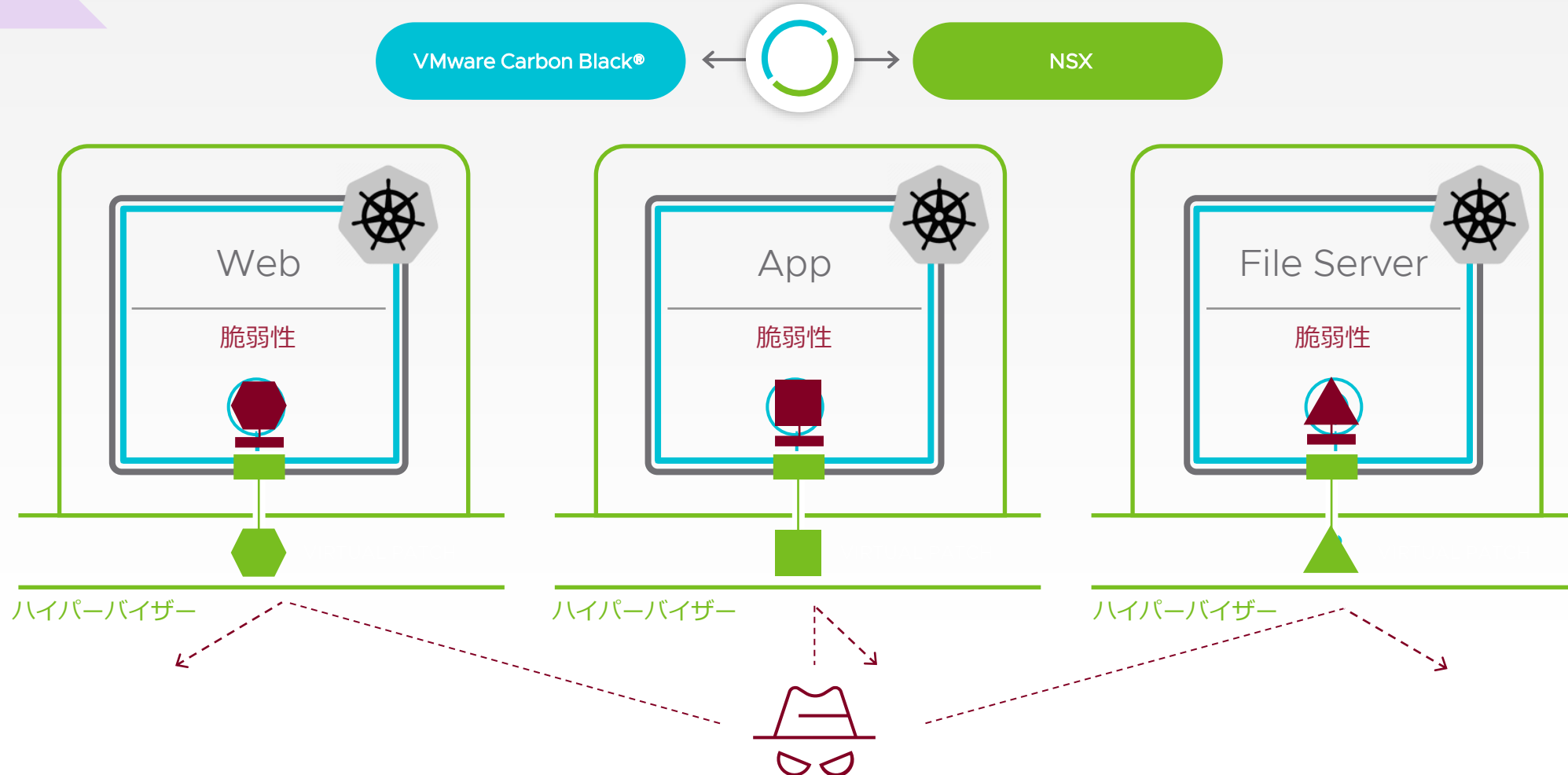
データセンタ内の至るところで求められるソリューション

注意：

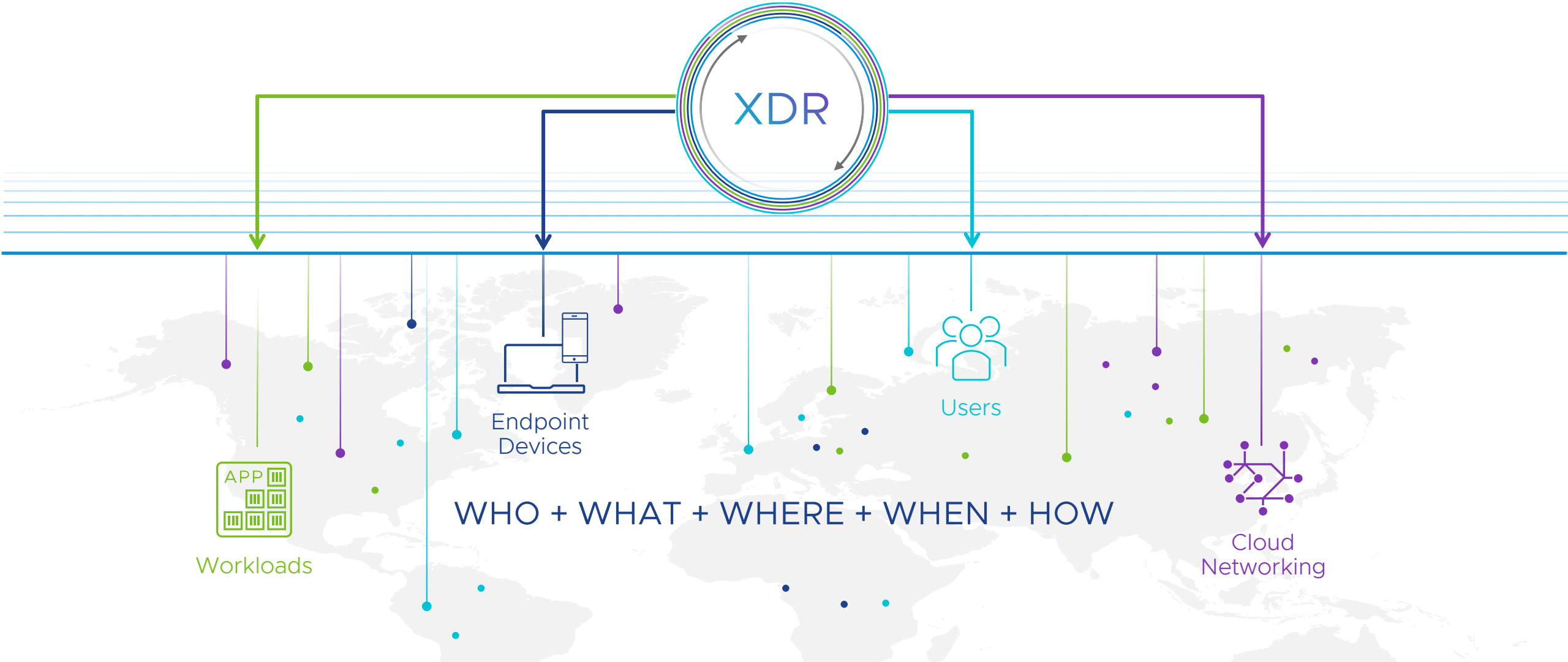
本ソリューションはあくまで一時的な暫定対策としてのご利用をお願いします。

ベンダーからパッチが提供された場合には、速やかに正規のパッチ適用をお願いします。

Future Release



信頼性の高いセキュリティコンテキストをあらゆる実行ポイントに



IDS/IPS, Network Sandbox,
Network Traffic Analysis

NDR



EDR

Behavioral Detection, Threat Intel,
Endpoint Collection



Thank You