ネットワークセキュリティを
より強化する
VMware NSX-T Advanced Threat Prevention

ゼロトラストと相性の良い
VMware のネットワークセキュリティを、
AI を活用してより強化

志茂野 利夫

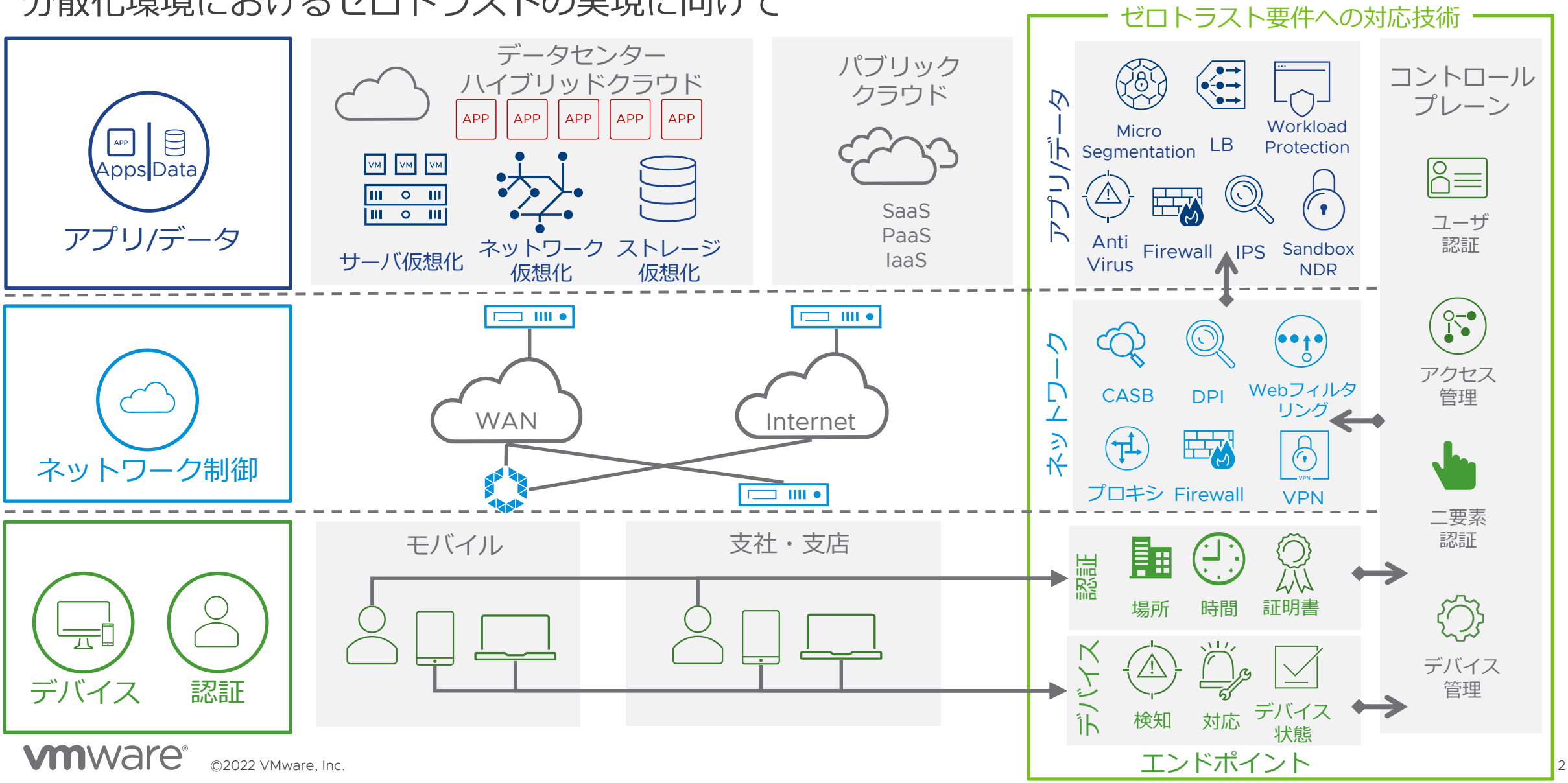
ヴイエムウェア株式会社

ネットワーク&セキュリティ技術本部
シニア スペシャリストエンジニア

vmware®

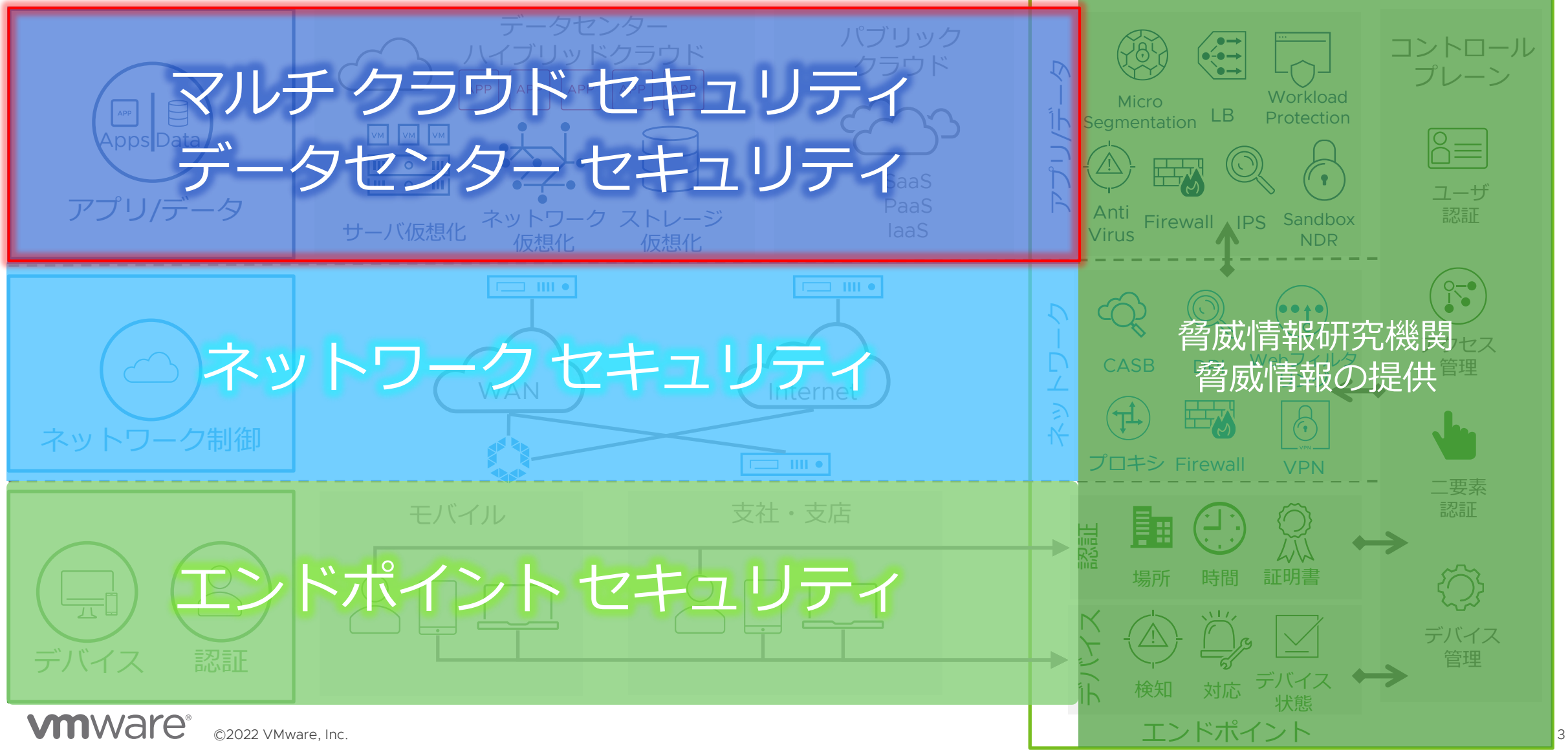
VMware Security の全体像

分散化環境におけるゼロトラストの実現に向けて



VMware Security の全体像

分散化環境におけるゼロトラストの実現に向けて



VMware のデータセンター セキュリティ

VMware のゼロトラスト

課題
- 攻撃の高度化・多様化、アタック サーフィスの増加
  - 従来の境界型防御では防御ができなくなった

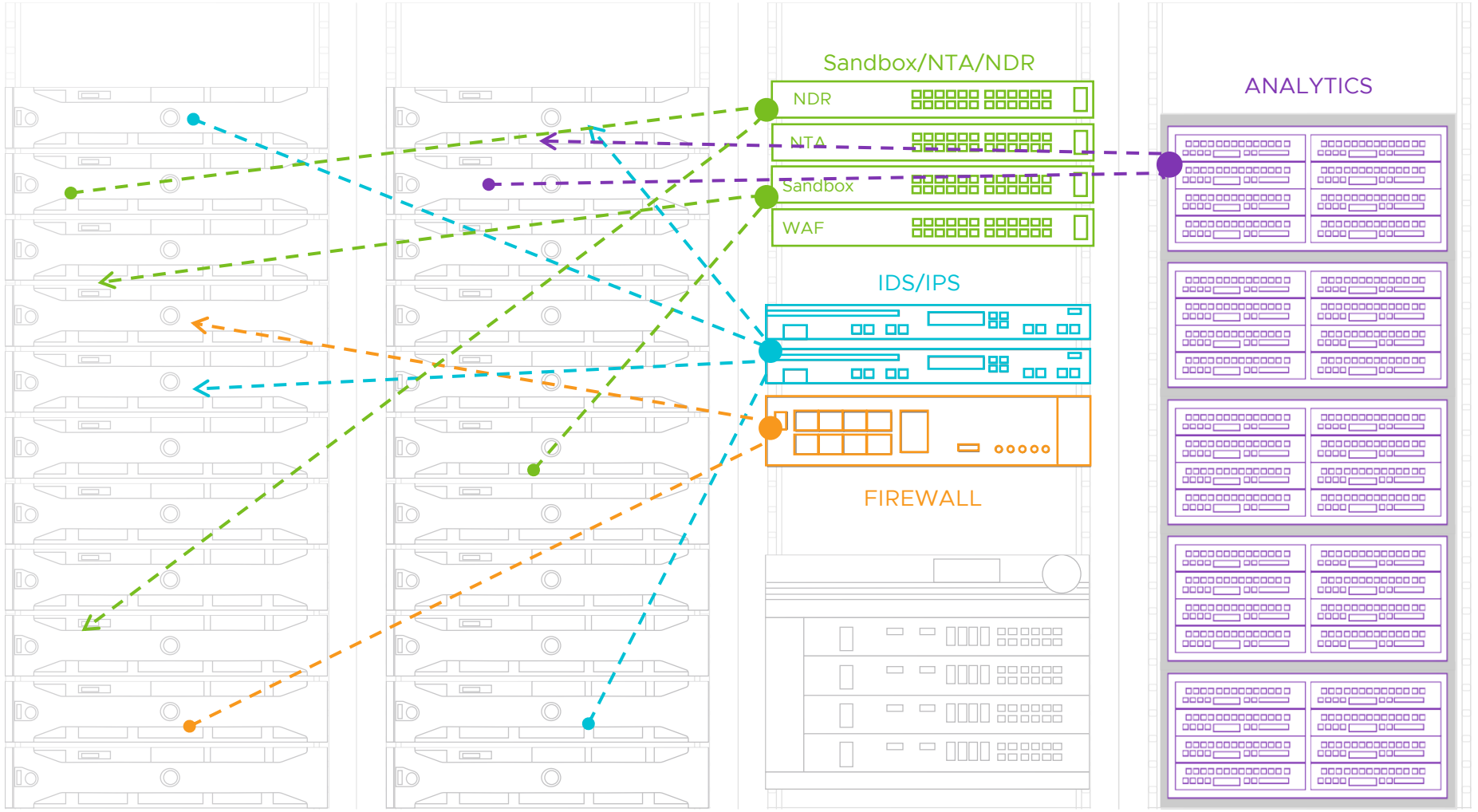
ソリューション
- 多層防御
- マイクロセグメンテーション

VMware ネットワーク セキュリティ ソリューション
- 分散型ファイアウォール
- 分散型 IDS・IPS
- サンドボックス（Full Emulation System）
- NDR (Network Detection and Response)

ビルトイン実装

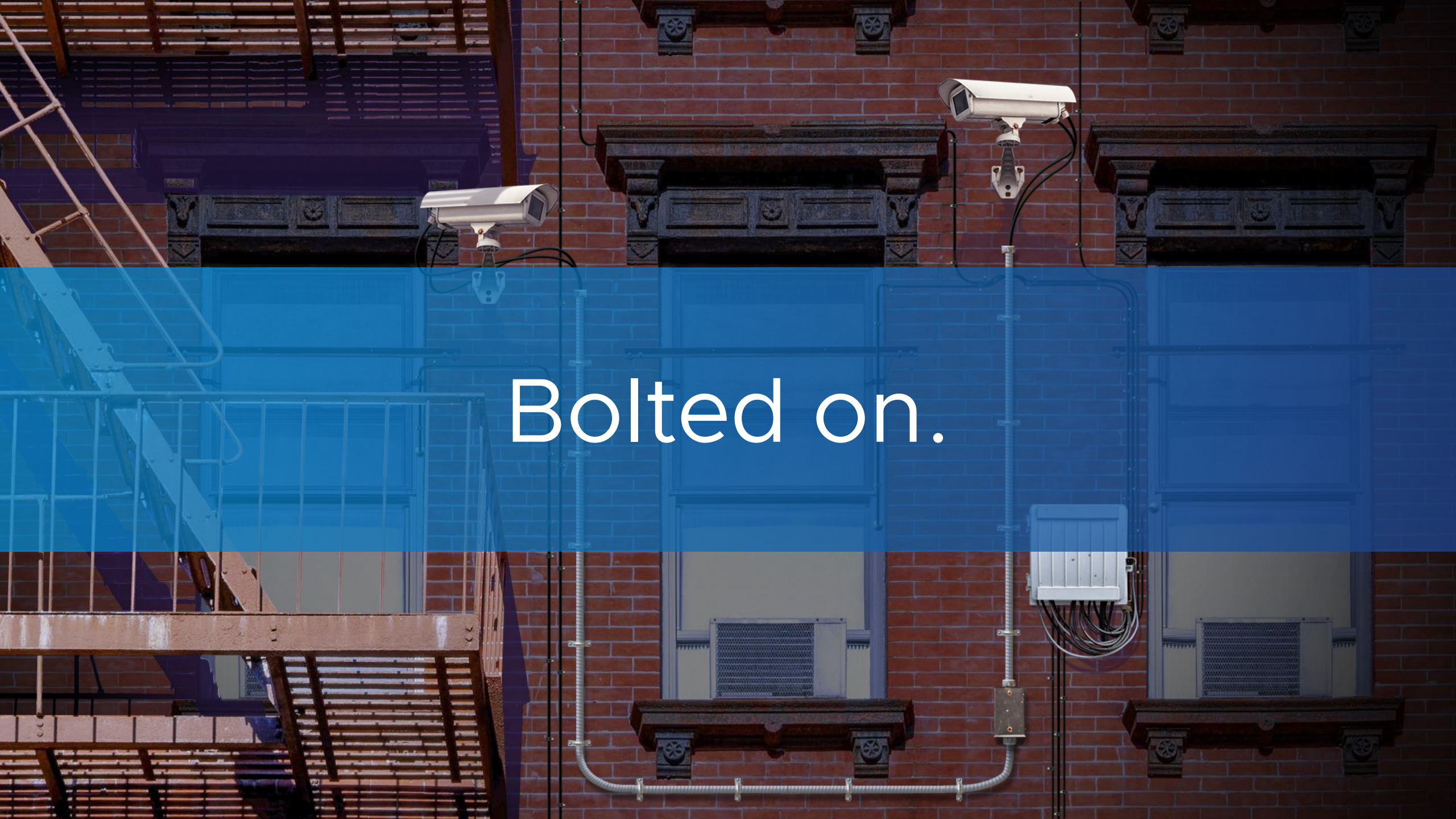
従来のゲートウェイ型

境界型の限界とハードウェア依存の課題

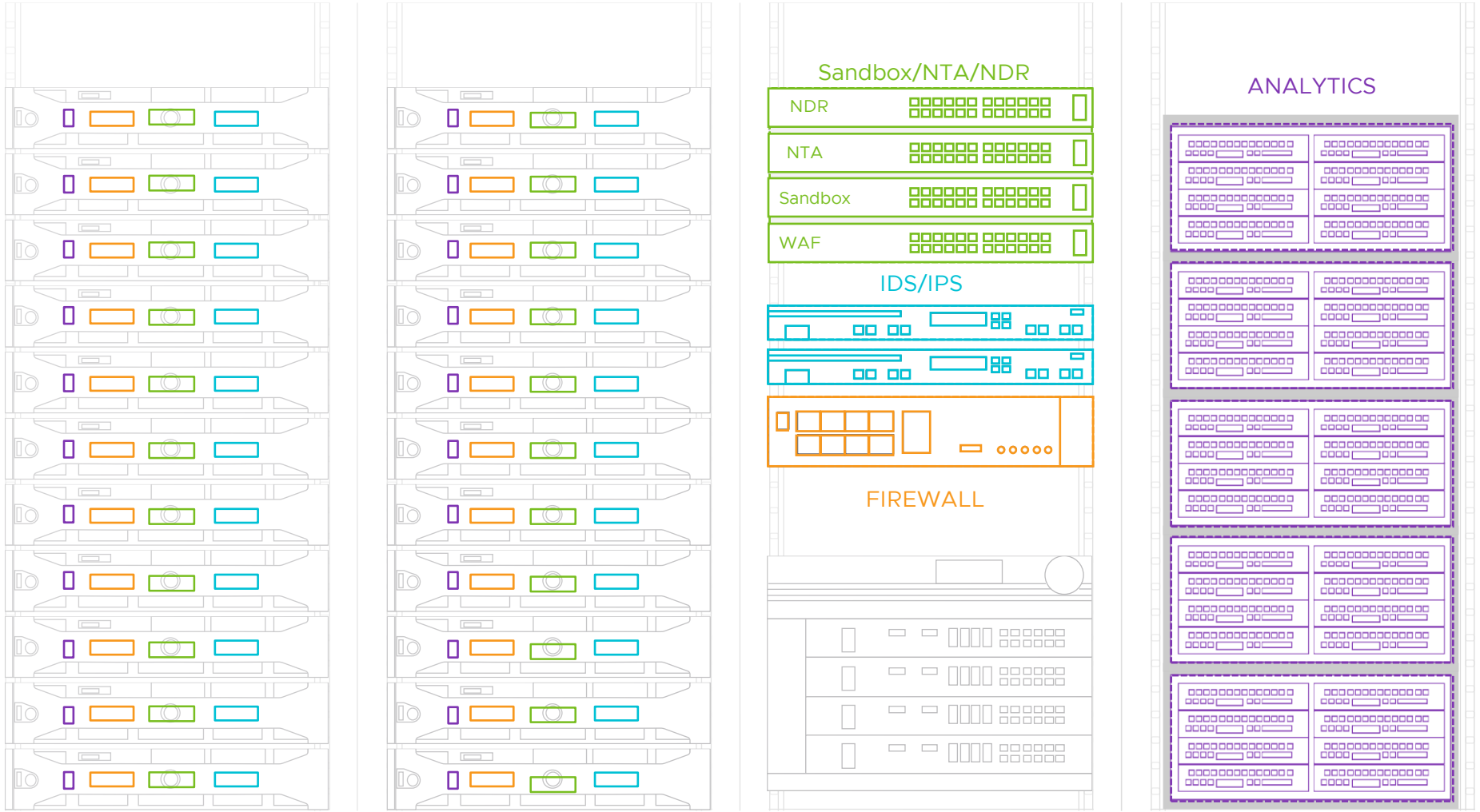


現実

- 全トラフィック検査は非現実的
- ヘアピントラフィック多発
- ブラインドスポットが発生
- 柔軟なスケールアウトが困難
- 非統一なセキュリティポリシー
- 高価なCAPEX/OPEX (ハードウェアメンテナンス、電力、ケーブリング、ラックスペース...)


Bolted on.

分散型ファイアウォール　IDS/IPS
ワークロードレベルのマイクロセグメンテーション

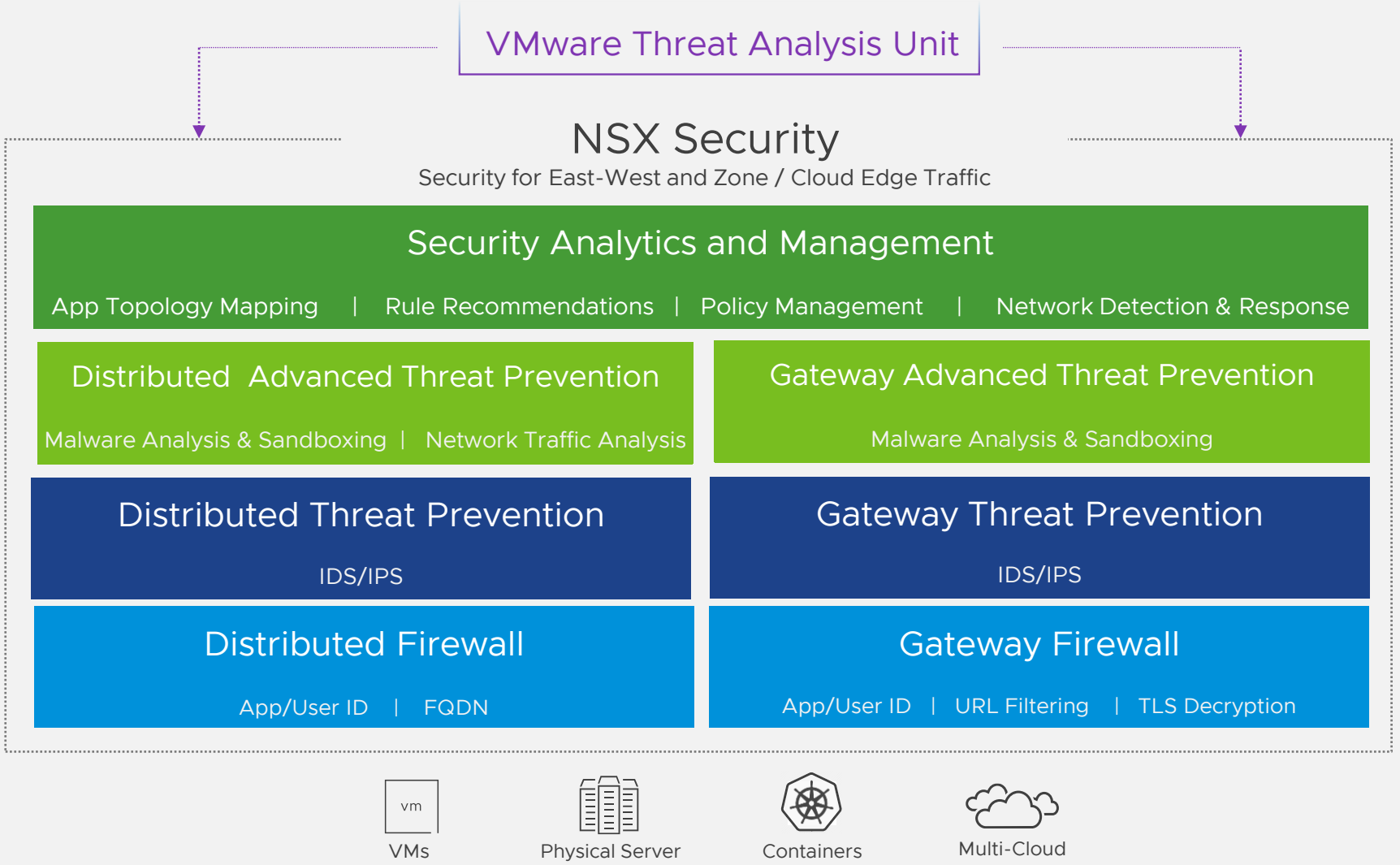


NSX による解決

- ヘアピントラフィック消滅
- TAP不要
- 統合された管理プレーン
- ソフトウェアベースの柔軟な実装
- 統一的オペレーションによるマルチクラウド対応
- 高いコスト削減効果 (70%+ 削減実績)


Built-in Surveillance
Built-in... Differently.
Built-in Fire Egress
Built-in Security

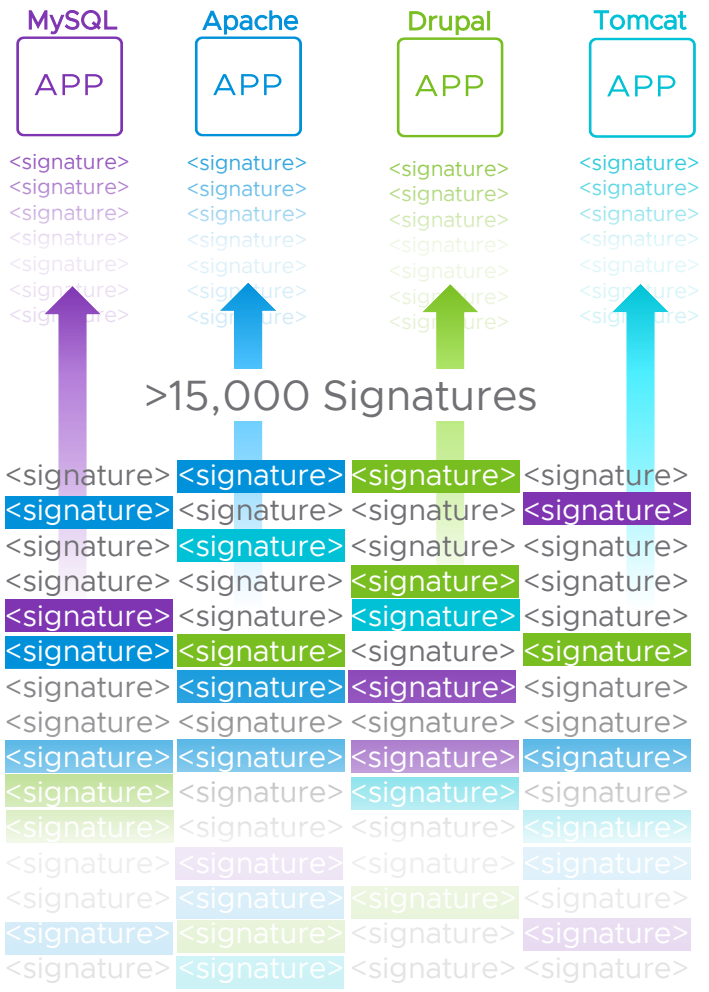
NSX Security: Modern Network Defense



ELASTIC SCALE | APPLICATION AWARE | NO NETWORK CHANGES | POLICY AUTOMATION

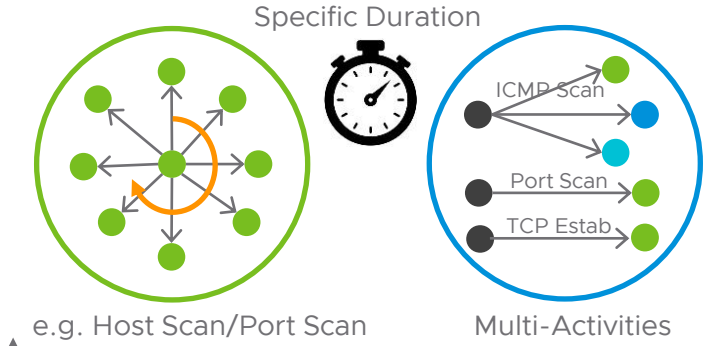
既知の脅威ーIDS/IPS（シグネチャ検知と振る舞い検知）

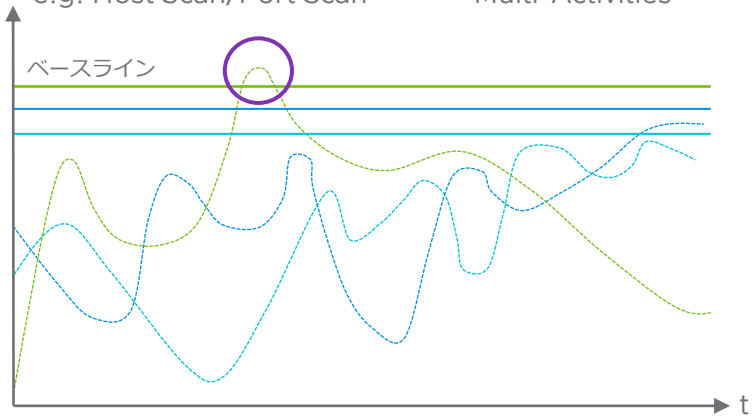
分散IDS/IPSによるシグネチャマッチング



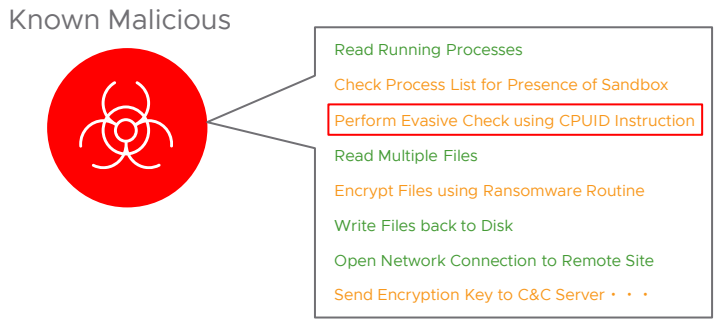
Behavioral IDSによる行動分析

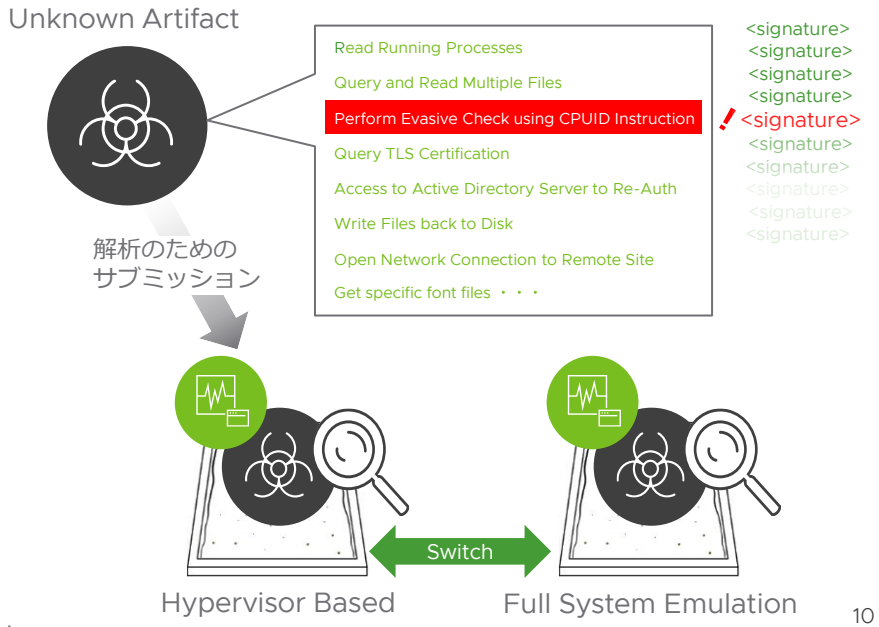
“ssh”トラフィックを検出したら、その後のトラフィック量を計測し異常を検出





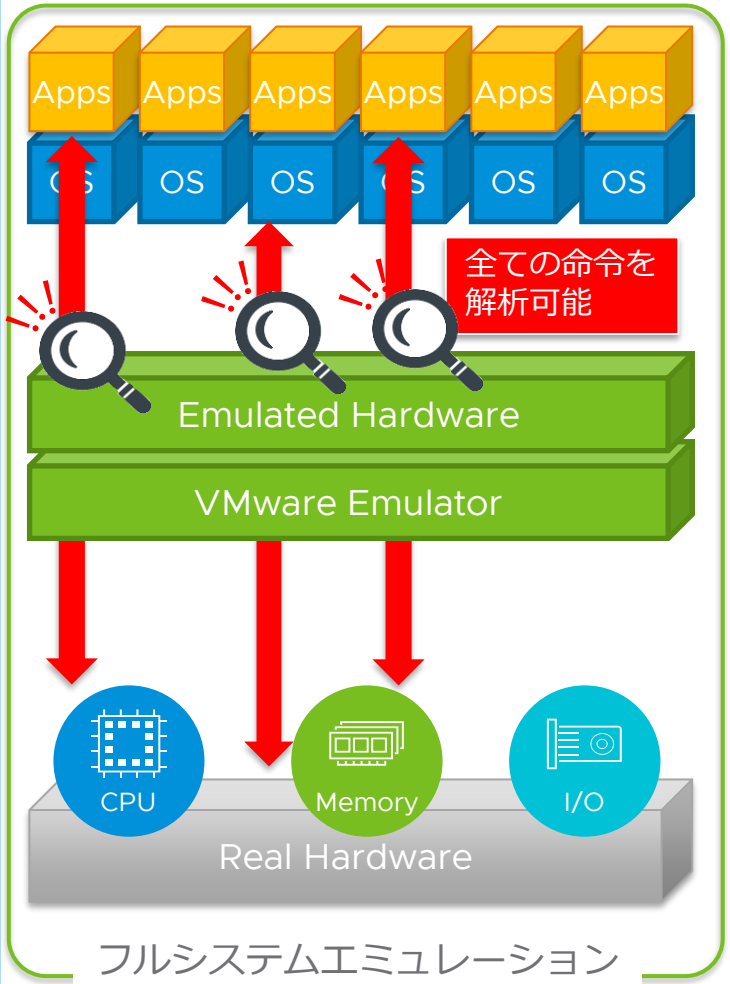
次の解析プロセスを決定づけるIDS



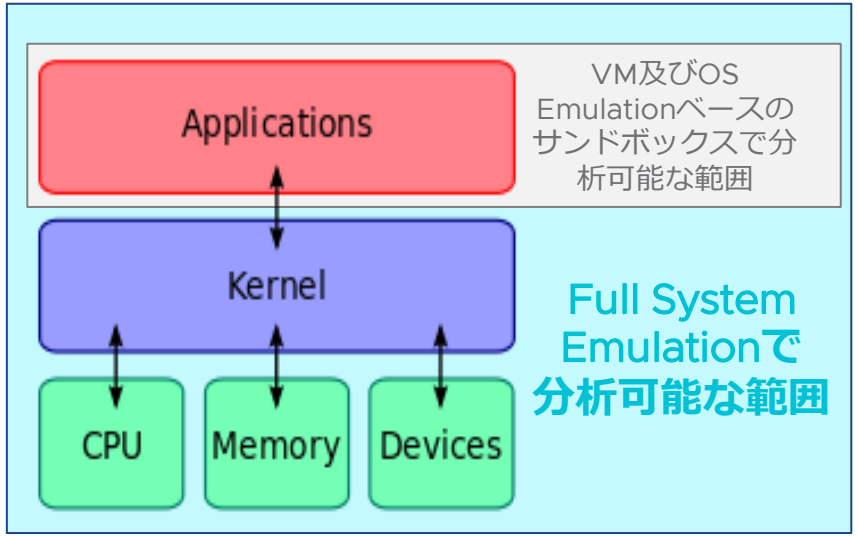


未知の脅威ーサンドボックスによるマルウェア検知

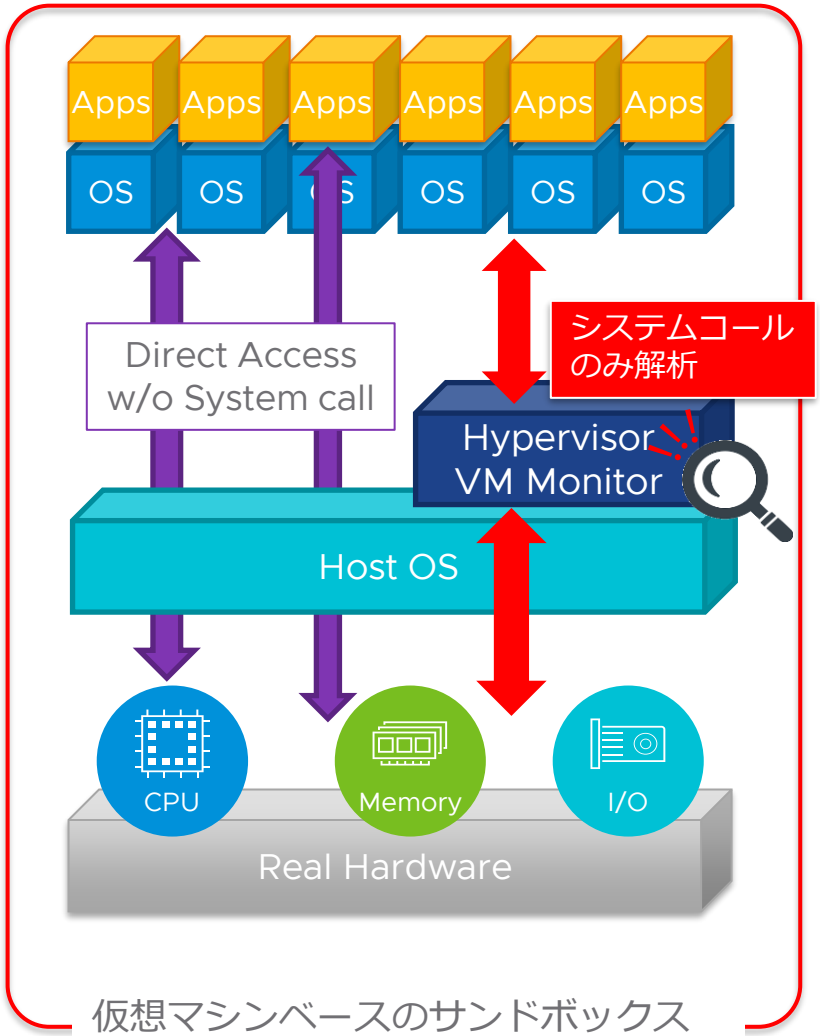
Full System Emulation と Hypervisor Based



フルシステムエミュレーション
サンドボックス



- ✓ OSやAppsからCPU, Memory、I/Oへの命令は、仮想マシンベースでは解析不可
- ✓ 回避テクニックの検知のため、両サンドボックスースを同時に実施（ハイブリッド構造）
- ✓ 「高い検出能力」と「低い誤検知率」の実現



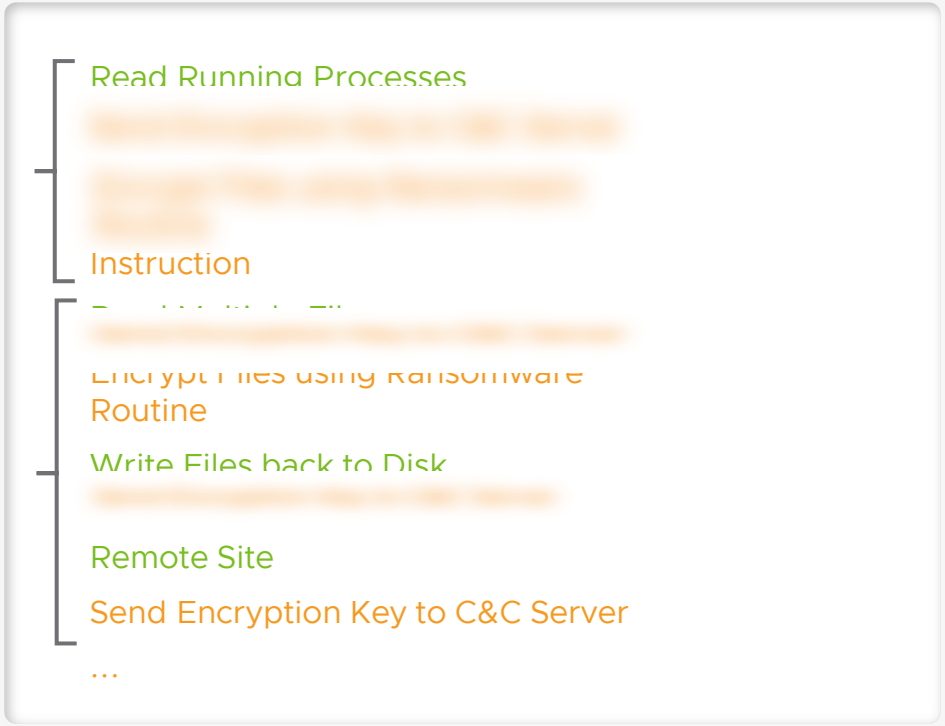
仮想マシンベースのサンドボックス

マルウェア検出技術 – フルシステムエミュレーション
全ての命令を解析

サンドボックス回避

一見普通に見える

ランサムウェアのアクティビティ



- OS が把握する命令のみならず、全命令を把握
- 解析回避行動も検出
- マルウェア振る舞い解析の精度が高い
- C2シグネチャのリアルタイム生成

トラディショナルなサンドボックスでは、マルウェアが実行する命令の一部しか見えない

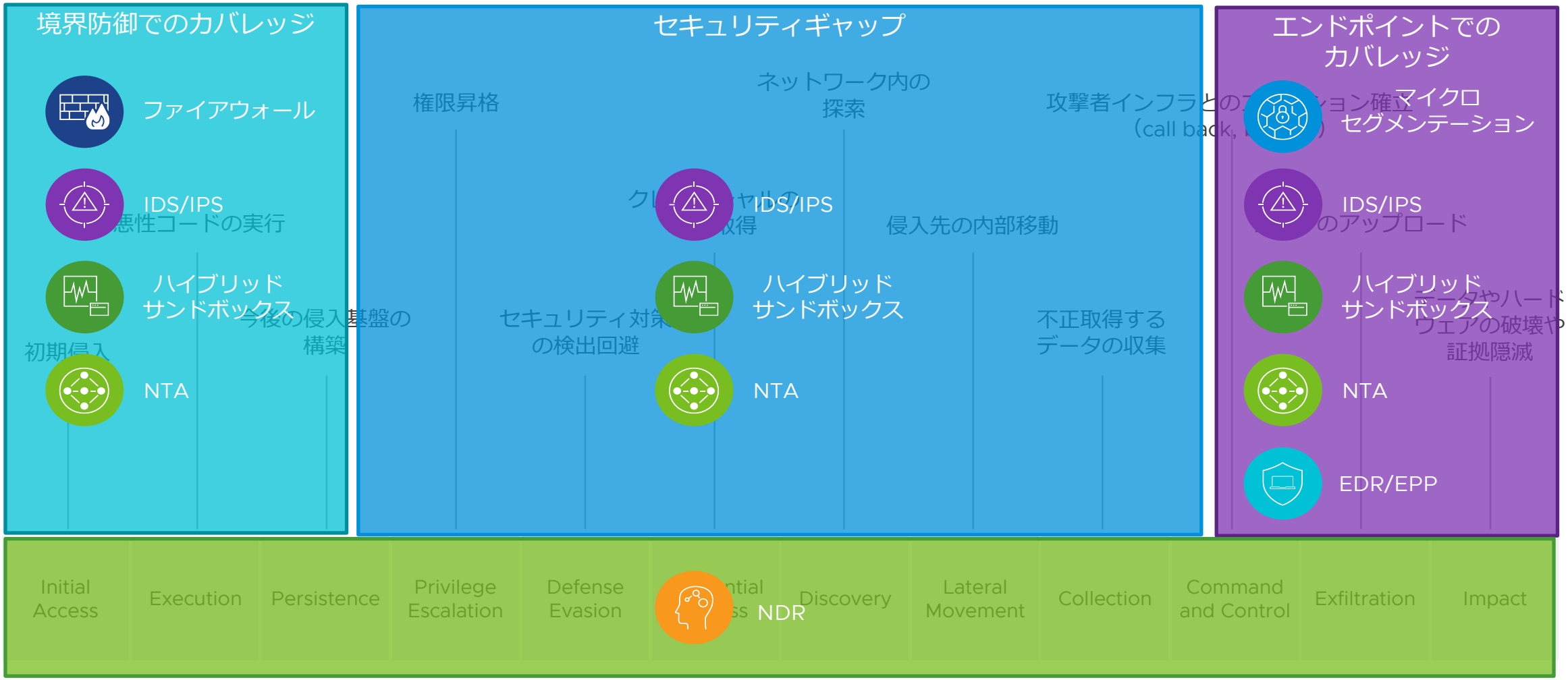
MITRE ATT&CK フレームワークにおけるカバレッジ

敵対者の戦術とテクニックのナレッジベース

Tactics (戦術)	FW	IDPS	NTA	Sandbox
Initial Access（初期アクセス）	● ●	● ●		●
Execution（不正コード実行）				●
Persistence（永続性）		● ●	●	●
Privilege Escalation（特権昇格）	●	●	●	●
Defense Evasion（防御回避）	●	●		●
Credential Access（認証情報アクセス）		●	●	●
Discovery（検索）	●	●	●	●
Lateral Movement（水平展開）	●	●	●	●
Collection（情報収集）		●	●	●
Command and Control（C&C）		● ●	●	●
Exfiltration（情報送信）		●	●	
Impact（影響）		●	●	●

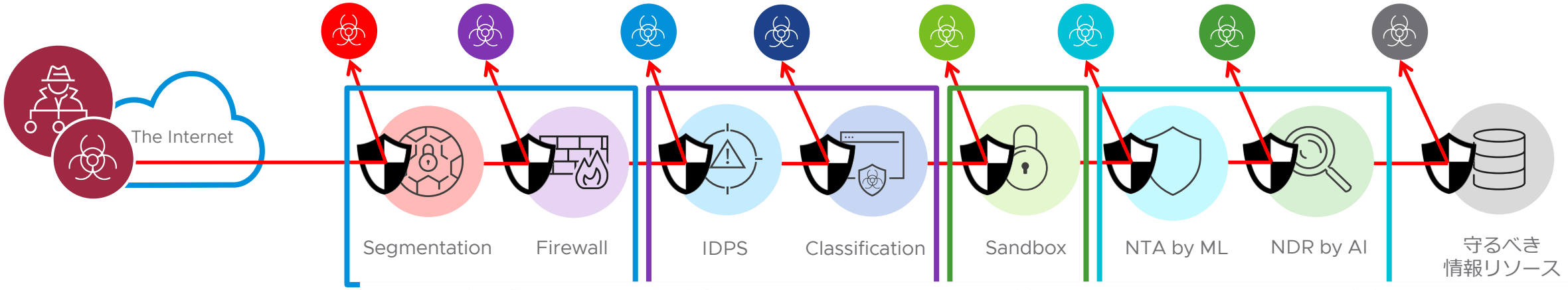
- ● 境界型によるカバレッジ
- ● NSX によるカバレッジ

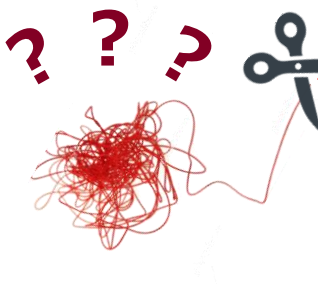
MITRE ATT&CK フレームワーク 時系列におけるカバレッジ



「多層防御」の副作用

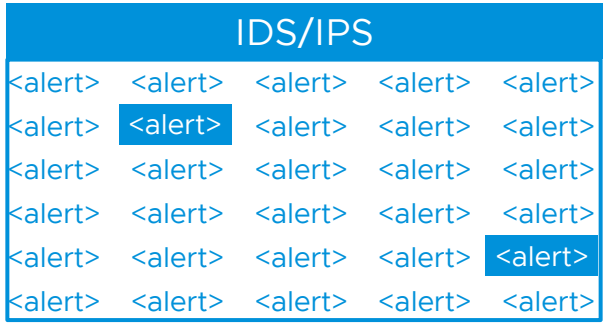
サイロ化問題





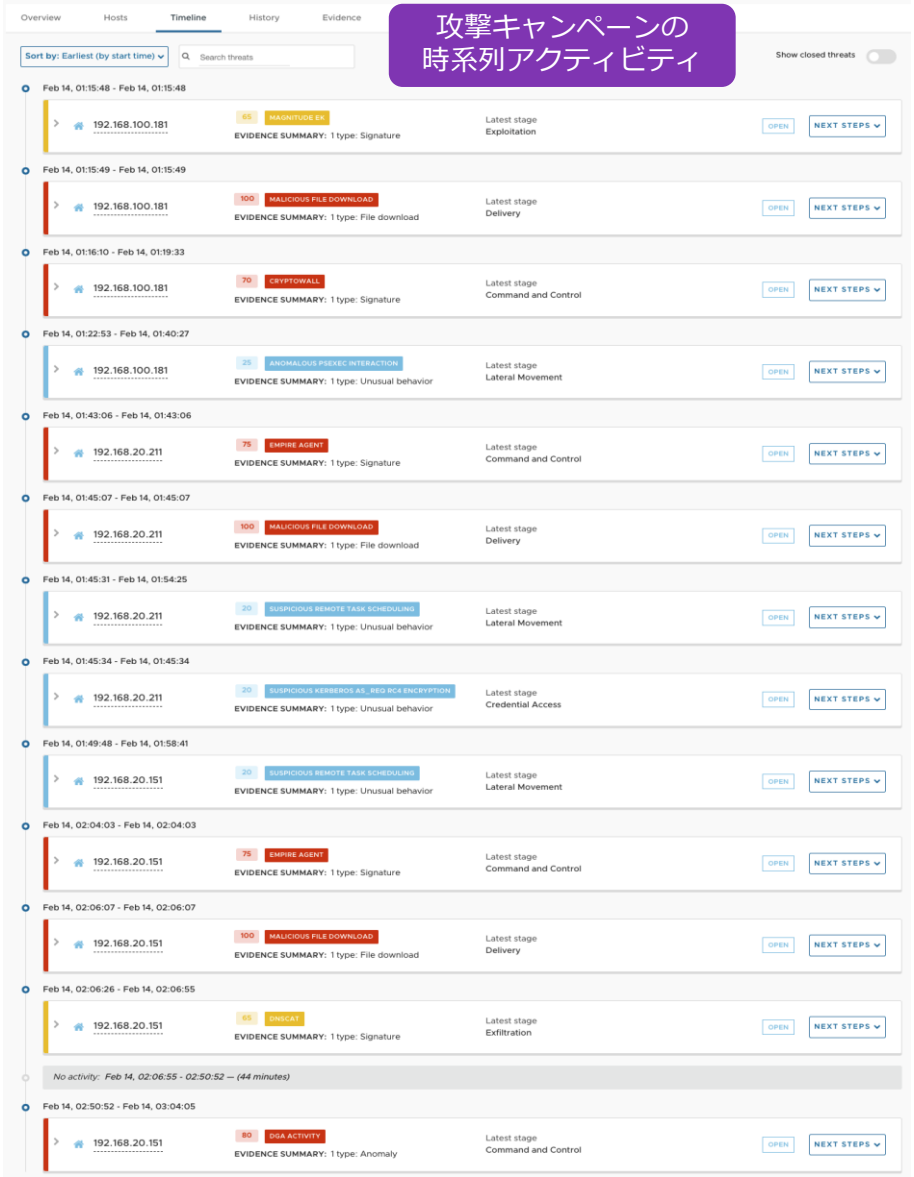
全イベントの相関関係と一連攻撃のMITRE ATT&CKマッピング

意味のある「コンテキスト」で攻撃全体を把握



攻撃キャンペーン全体を可視化ーNDR

全体を網羅した可視化と統一した操作性



NDRの定義

- Gartner社の定義

✓ 非シグネチャベース（機械学習など）の解析技術を主に用いて不審トラフィックを検出

✓ 生のトラフィックやフローレコードを継続解析し、通常の振る舞いをモデル構築

✓ 不審なトラフィックパターンを検出したらアラート通知

✓ 南北トラフィックのみならず、東西トラフィックも監視

✓ 自動・手動のレスポンスは共通した必須要素

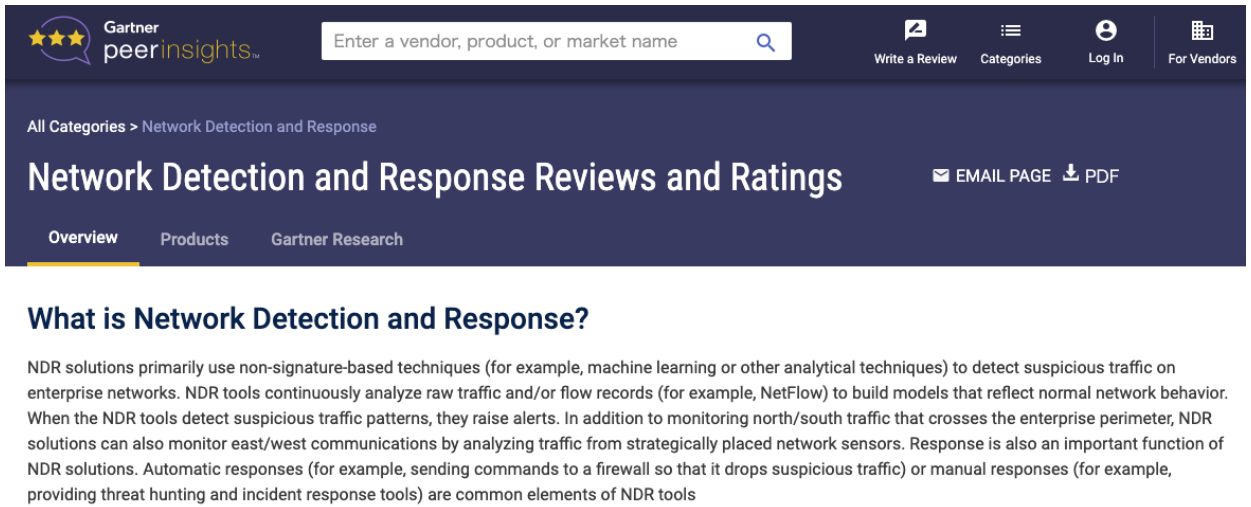
NTA

＋

レスポンスのための証拠と詳細情報

＝

NDR

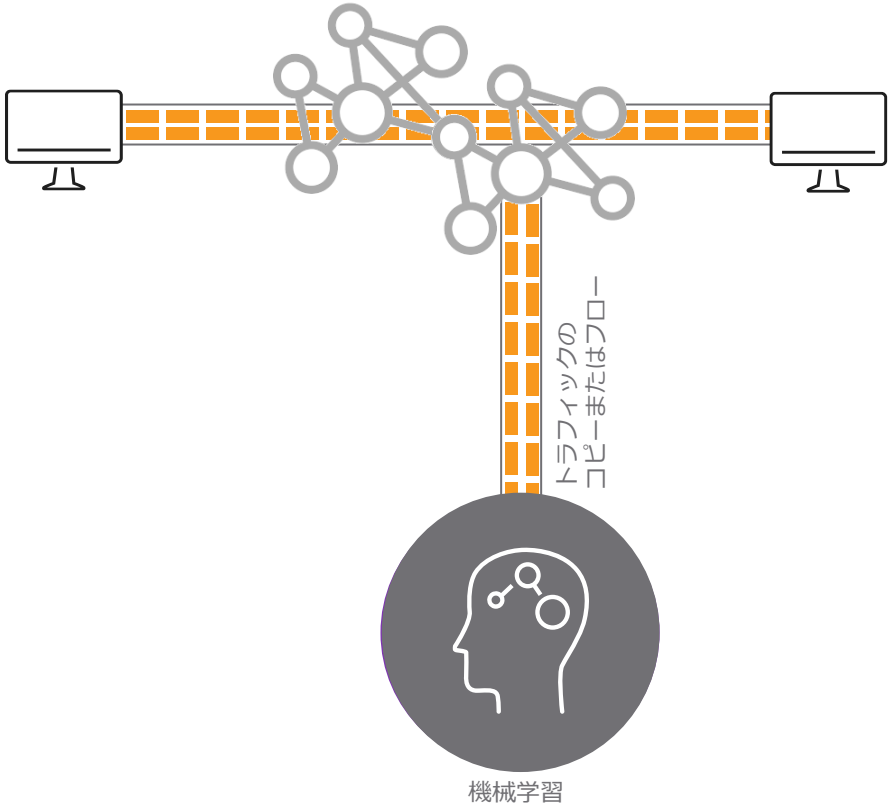


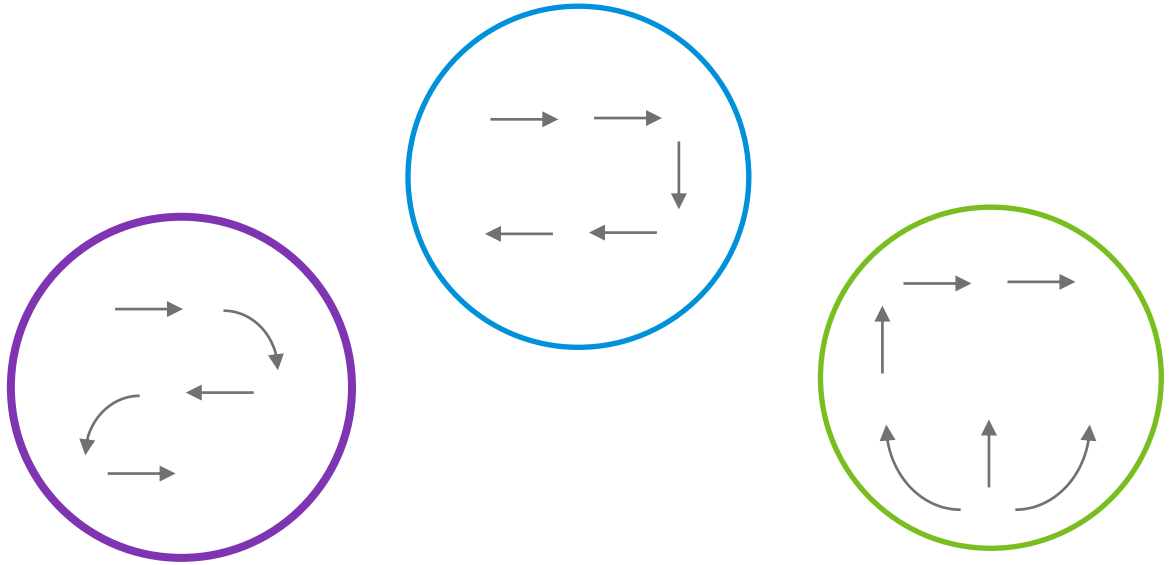
NTA: Network Traffic Analysis
NDR: Network Detection & Response

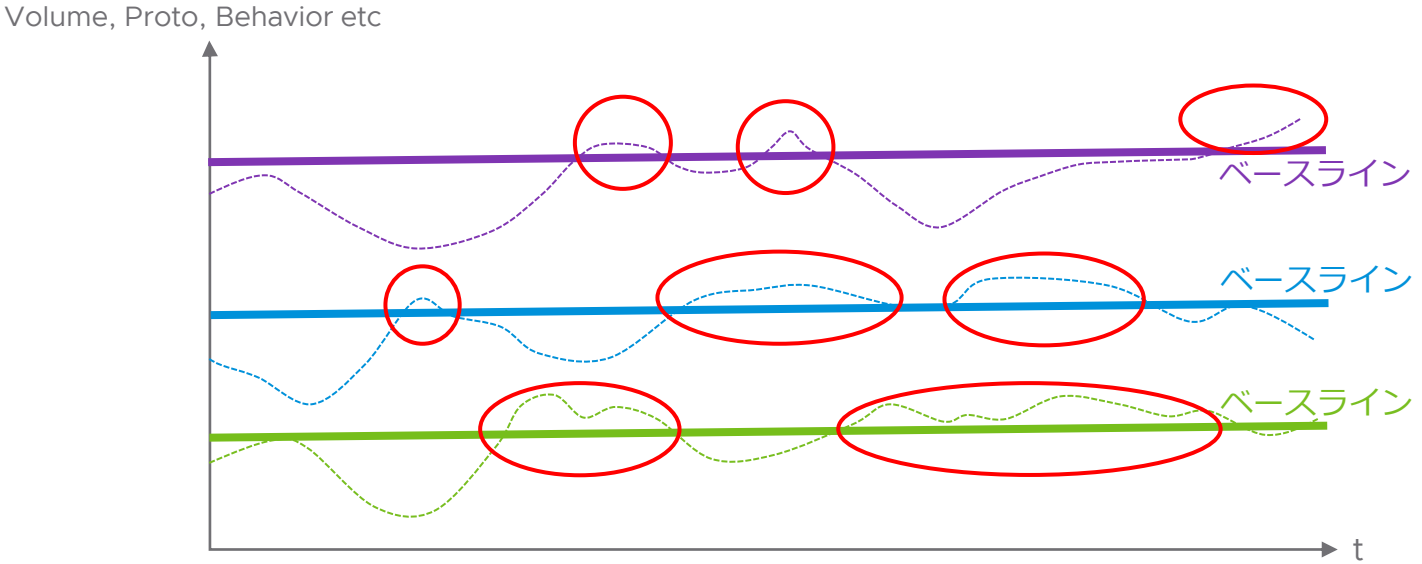
Source: https://www.gartner.com/reviews/market/network-detection-and-response

NTA

Network Traffic Analysisとは

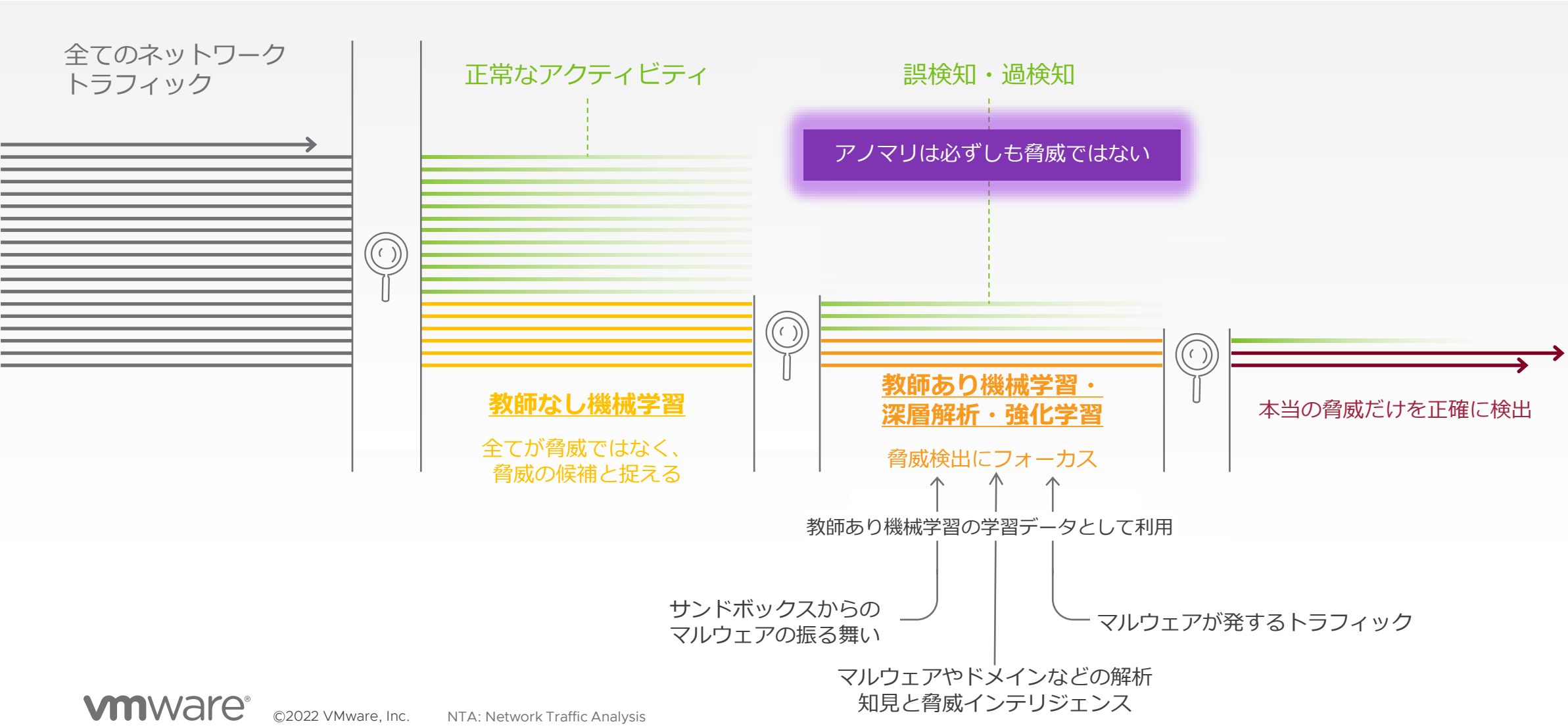






NTA: Network Traffic Analysis
NDR: Network Detection & Response

AI による NDR
フォルスポジティブの排除



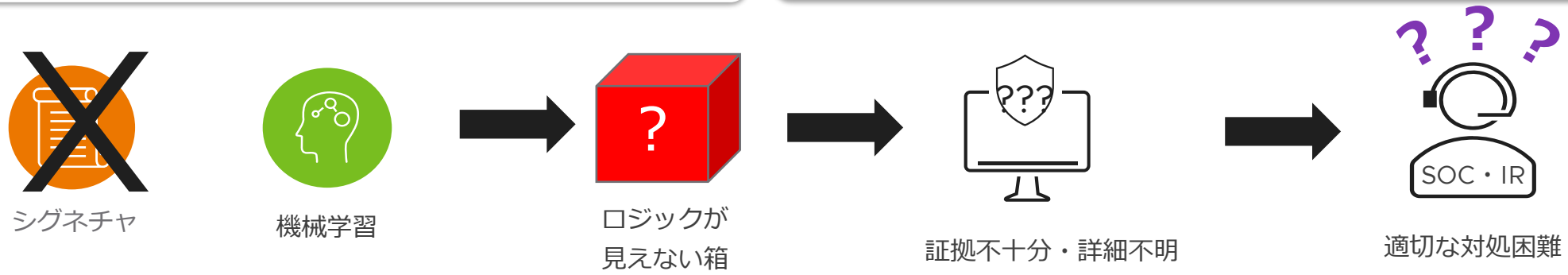
NTA: Network Traffic Analysis

「適切なレスポンス」に必要なもの

NTA / 一般的 NDR

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

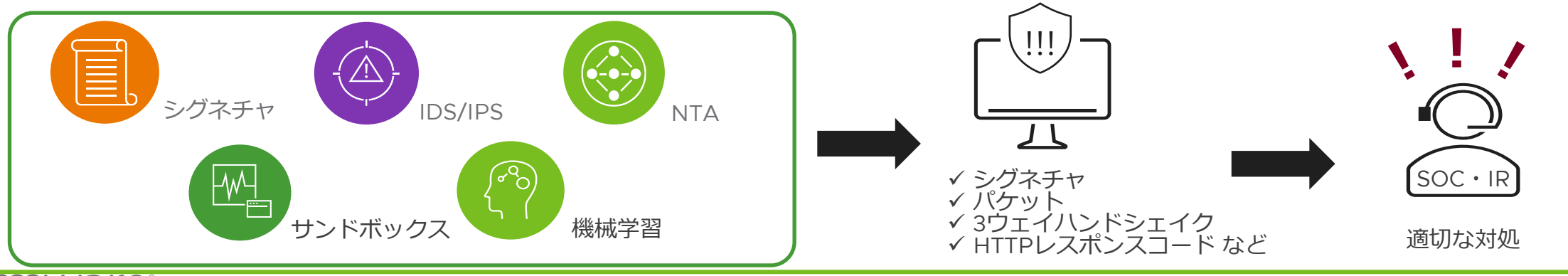
普通ではないようだ....が根拠不明...



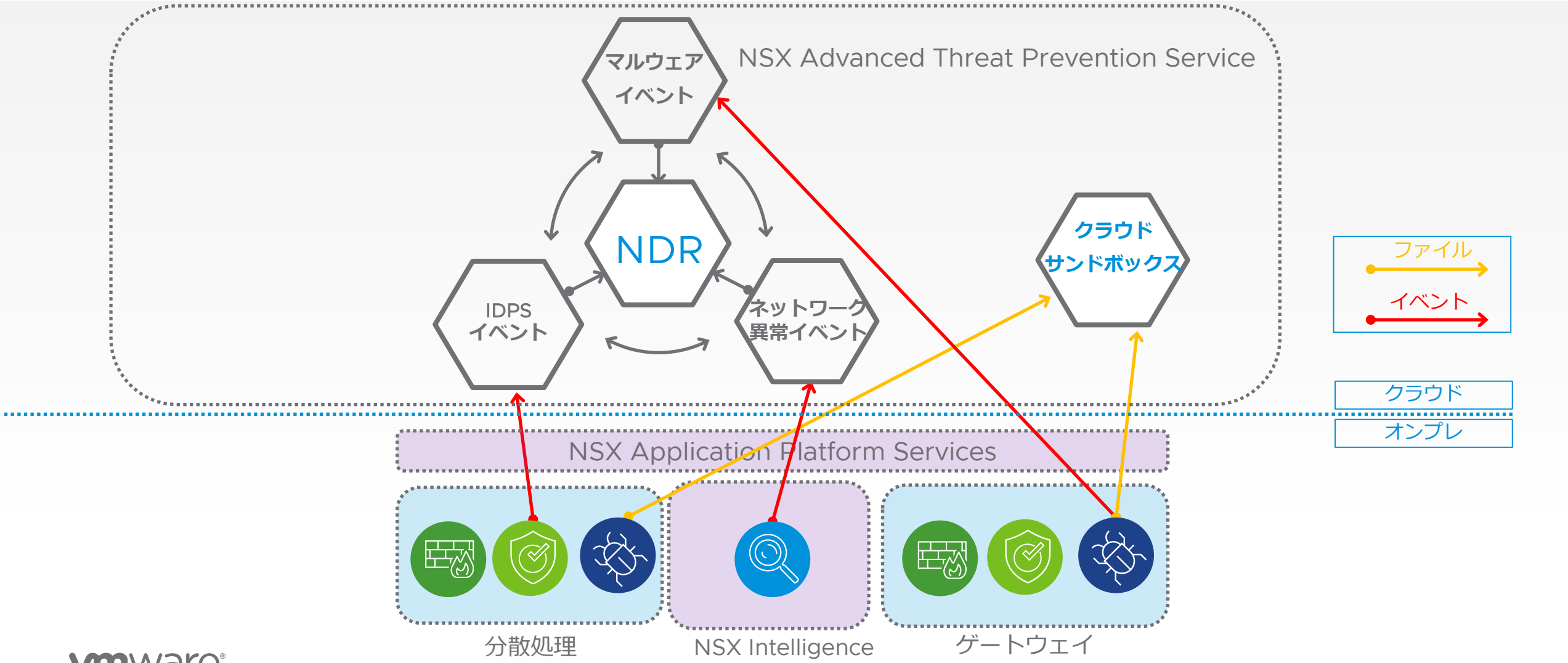
VMware NDR

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**

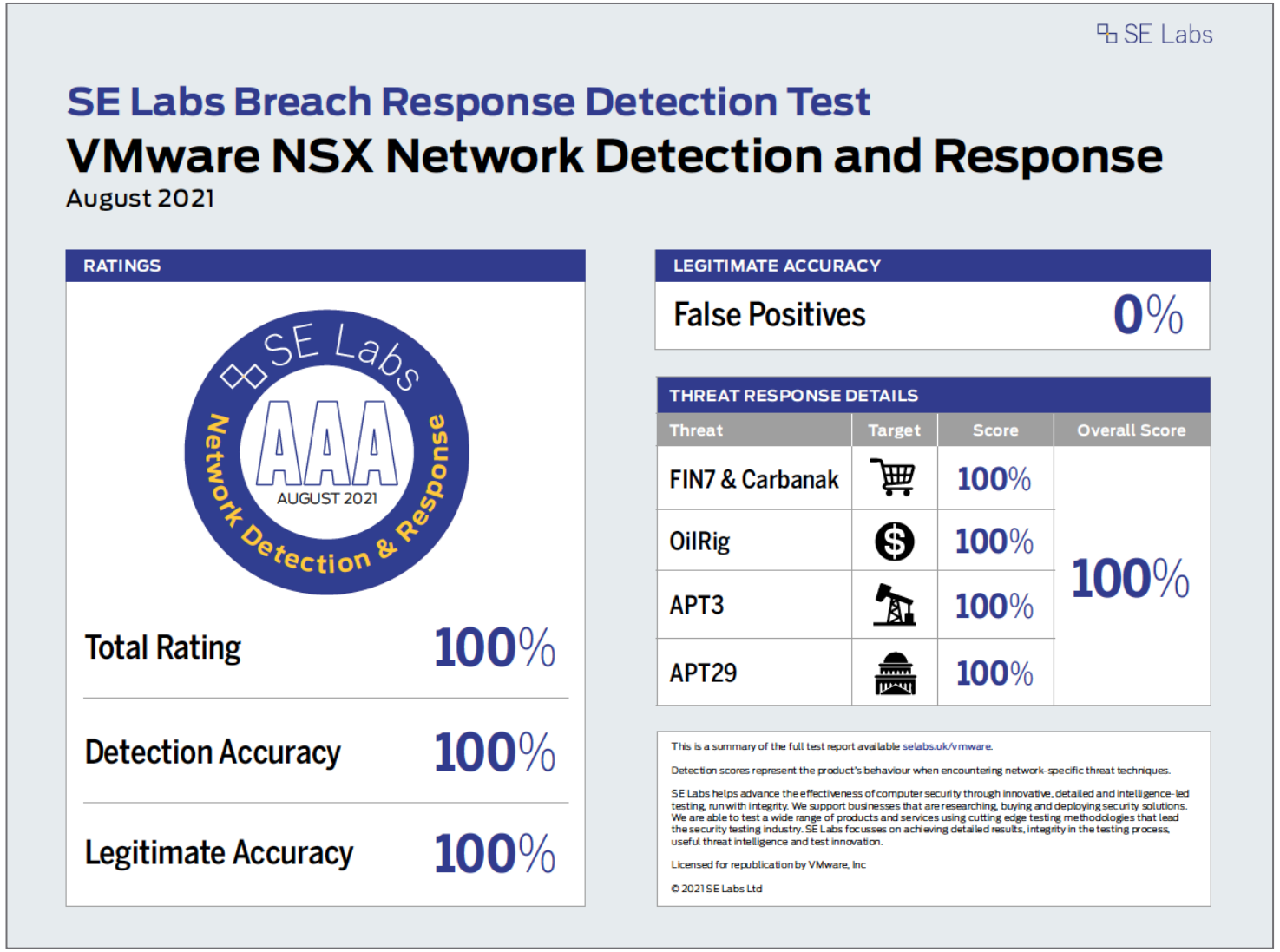
対処のための証拠・詳細情報そして「コンテキスト」



NDR
イベントの関連付け ー クラウド連携実装



第三者機関による NSX NDR の評価



SE Labs

SE Labs Breach Response Detection Test

VMware NSX Network Detection and Response

August 2021

RATINGS

SE Labs AAA Network Detection & Response AUGUST 2021

Total Rating	100%
Detection Accuracy	100%
Legitimate Accuracy	100%

LEGITIMATE ACCURACY

False Positives	0%

THREAT RESPONSE DETAILS

Threat	Target	Score	Overall Score
FIN7 & Carbanak		100%	100%
OilRig		100%	
APT3		100%	
APT29		100%	

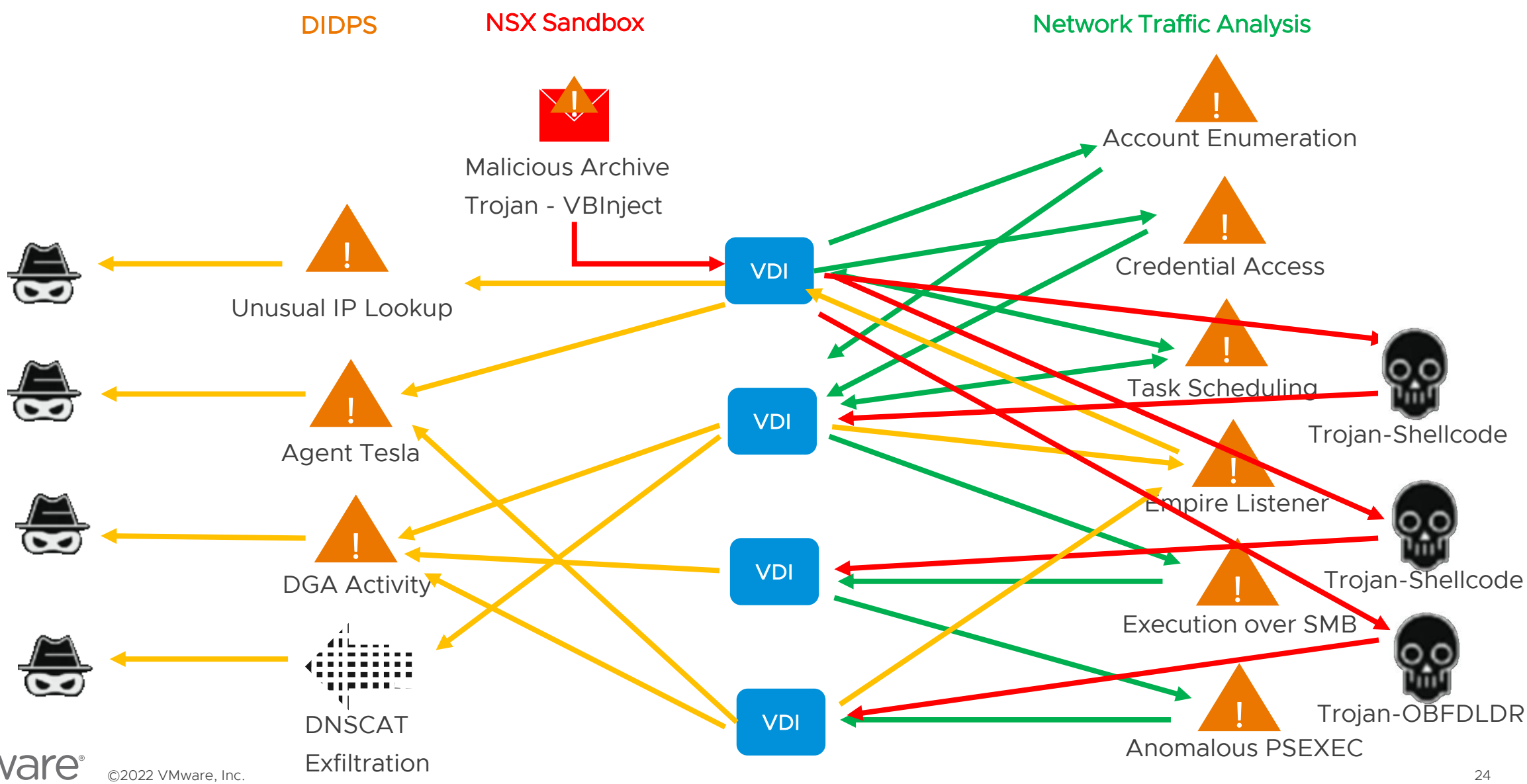
This is a summary of the full test report available selabs.uk/vmware.

Detection scores represent the product's behaviour when encountering network-specific threat techniques.

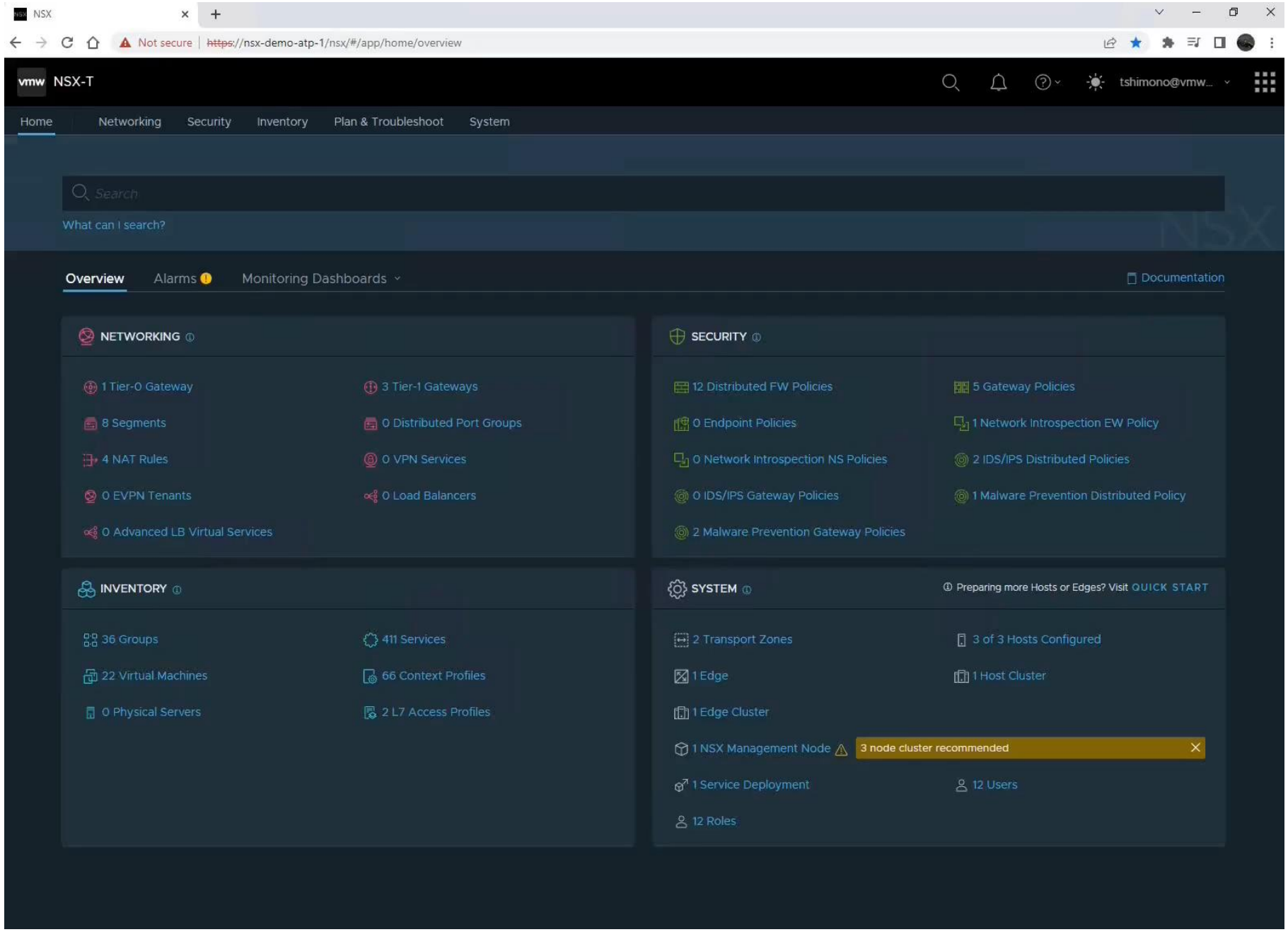
SE Labs helps advance the effectiveness of computer security through innovative, detailed and intelligence-led testing, run with integrity. We support businesses that are researching, buying and deploying security solutions. We are able to test a wide range of products and services using cutting edge testing methodologies that lead the security testing industry. SE Labs focusses on achieving detailed results, integrity in the testing process, useful threat intelligence and test innovation.

Licensed for republication by VMware, Inc

Oilrig APT (APT34) のアクティビティ



デモ



Thank You