

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

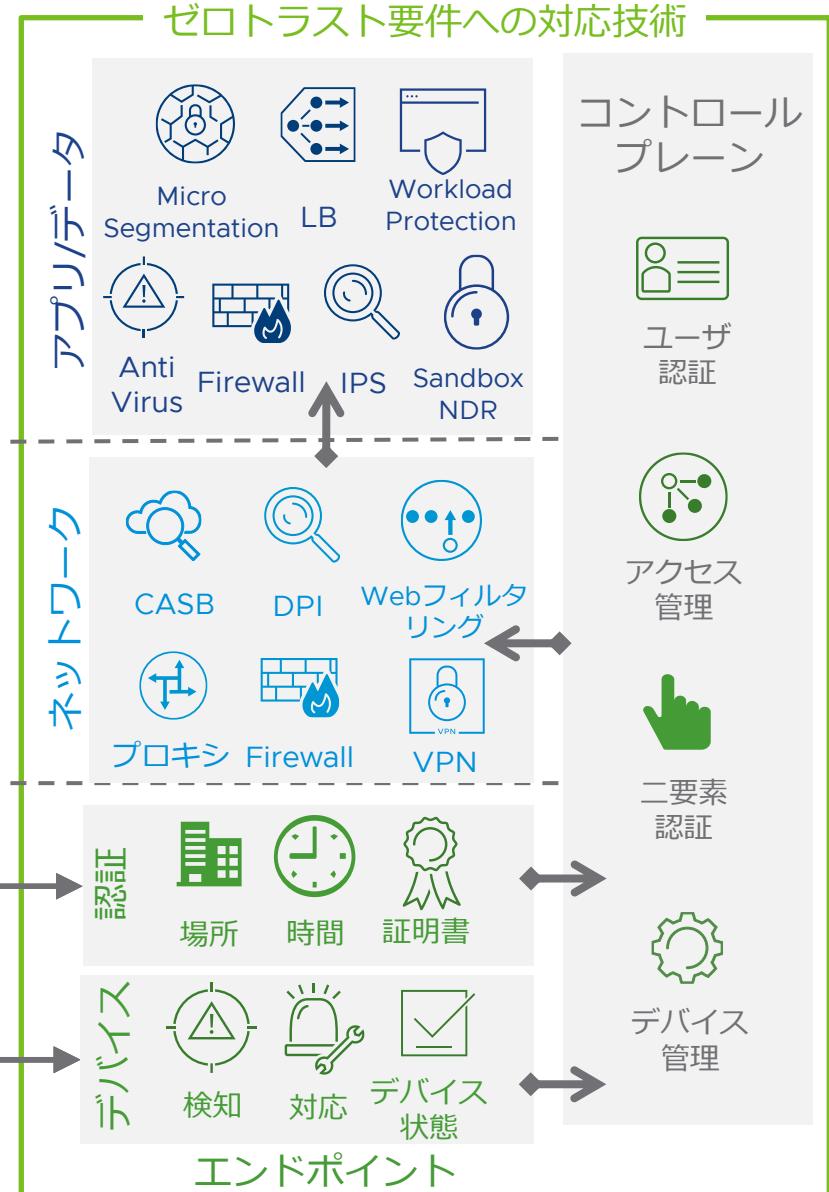
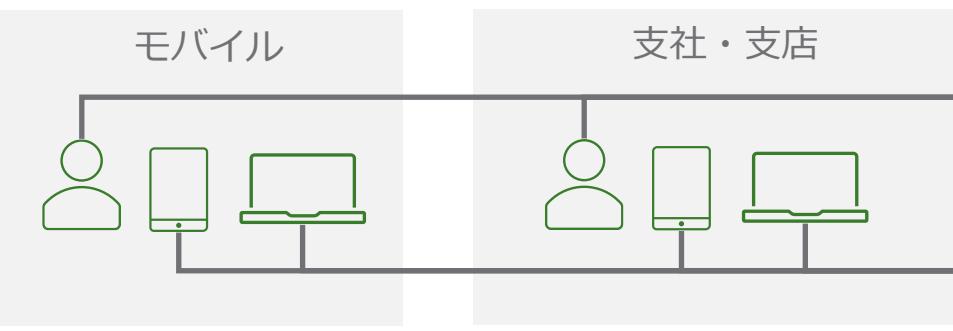
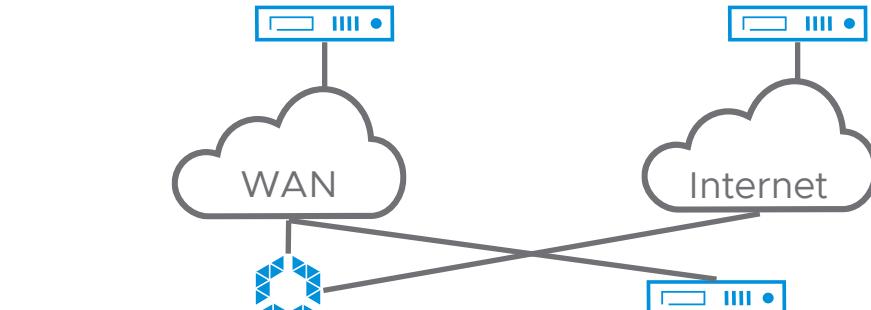
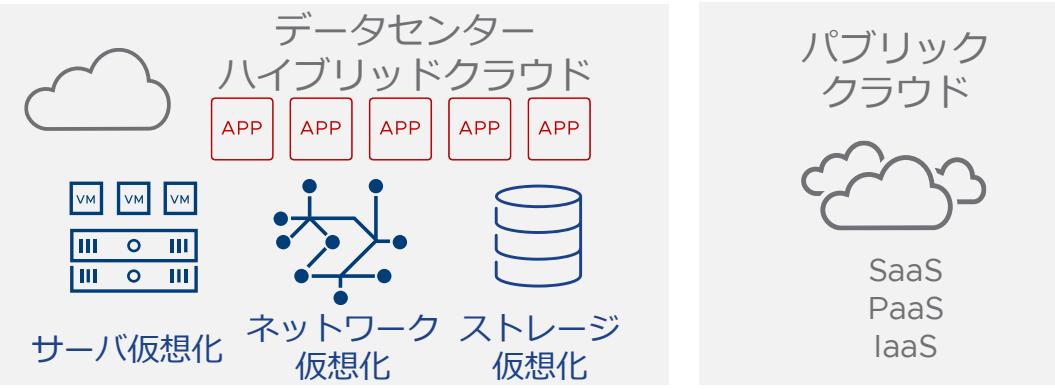
ゼロトラストと相性の良い
VMware のネットワークセキュリティを、
AI を活用してより強化

志茂野 利夫
ヴィ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 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

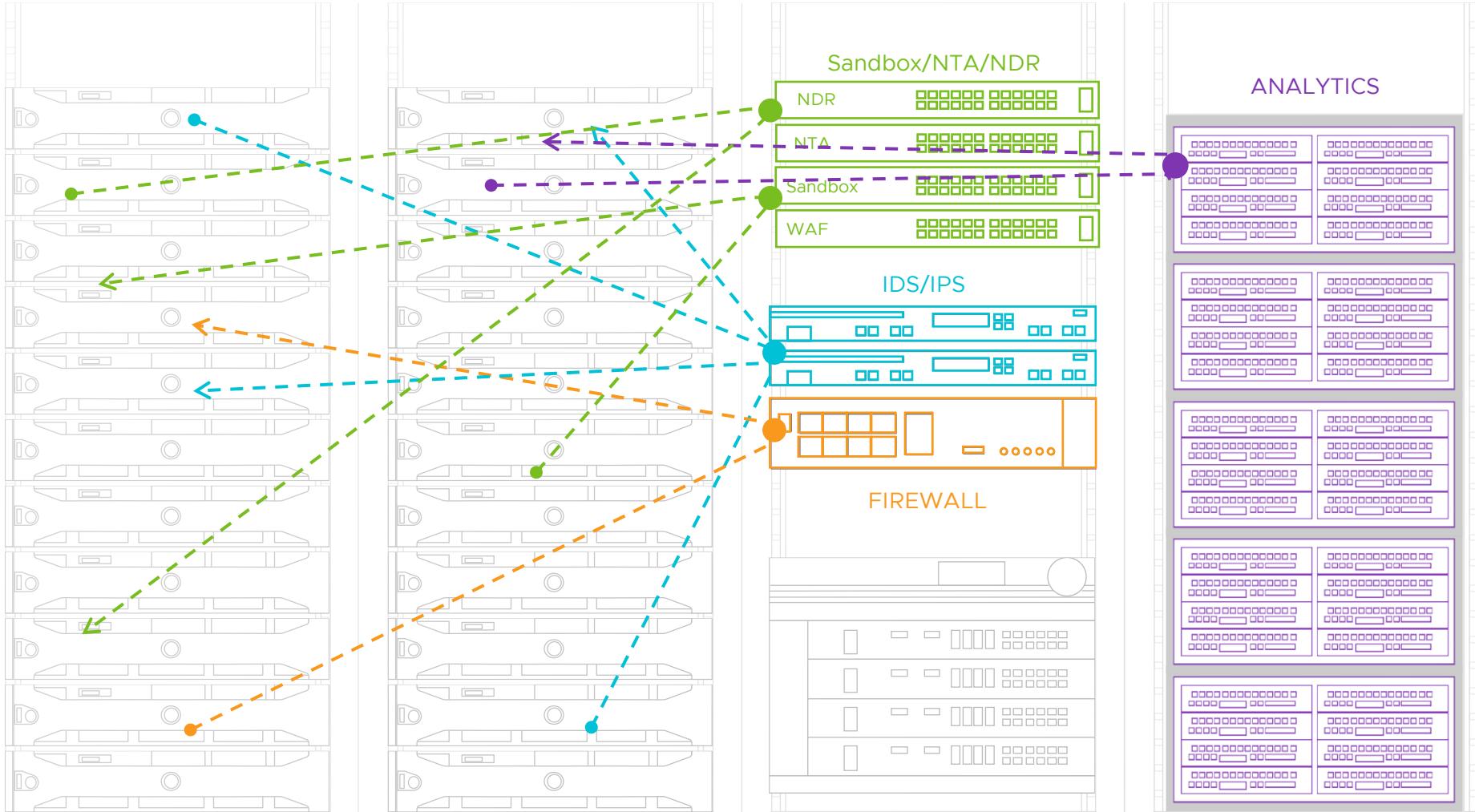


VMware ネットワークセキュリティソリューション

- 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

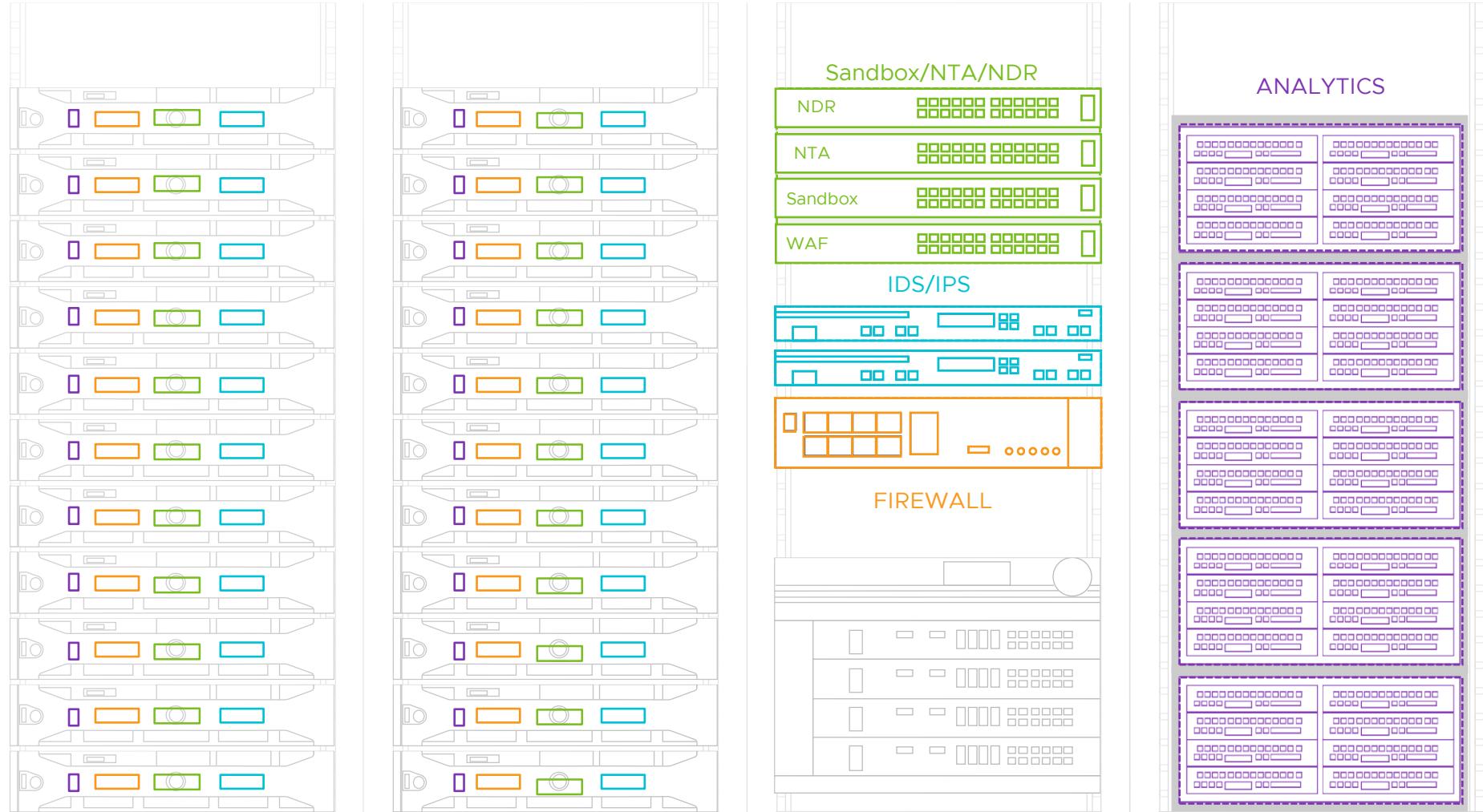
- ・全トラフィック検査は非現実的
- ・ヘアピントラフィック多発
- ・ブラインドスポットが発生
- ・柔軟なスケールアウトが困難
- ・非統一なセキュリティポリシー
- ・高価なCAPEX/OPEX (ハードウェアメンテナンス、電力、ケーブリング、ラックスペース...)

A collage of images illustrating the installation of surveillance cameras. The top half shows a wide-angle view of a red brick building facade with two white, bullet-style cameras mounted on black poles. The bottom half is a close-up of the same building's exterior, focusing on a single camera unit mounted on a pole next to a window. The camera is connected to a white electrical box with multiple black cables. The overall theme is the integration of modern security technology into a traditional architectural setting.

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)



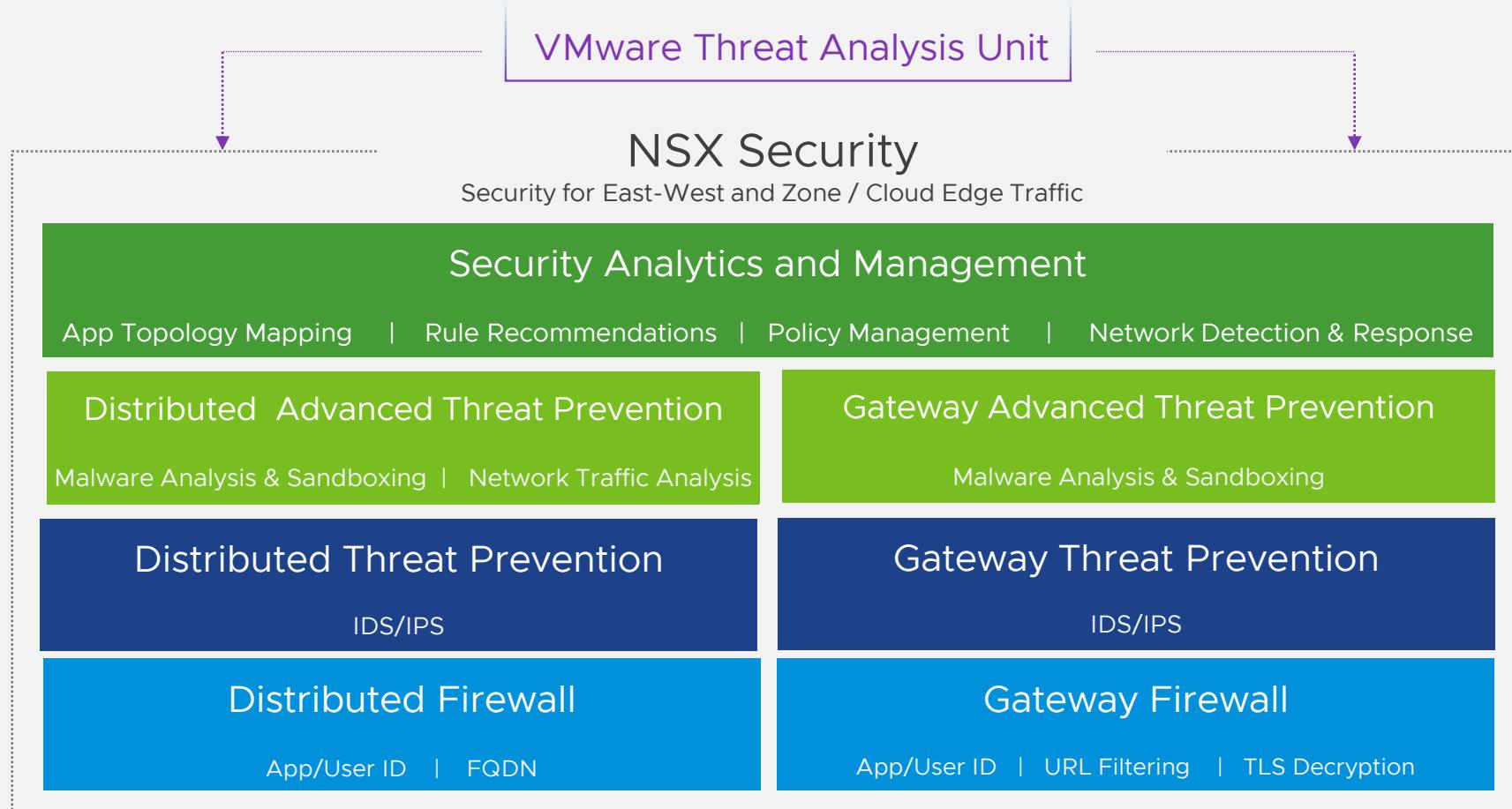
Built-in Surveillance

Built-in... Differently.

Built-in Fire Egress

Built-in Security

NSX Security: Modern Network Defense



VMs



Physical Server



Containers

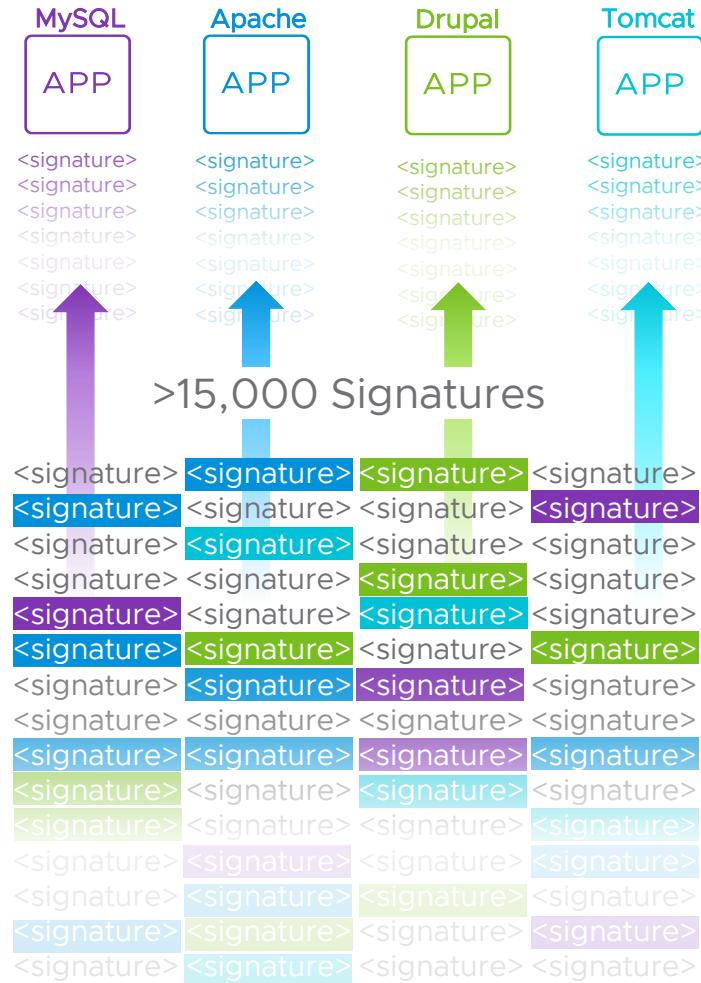


Multi-Cloud

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

既知の脅威—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

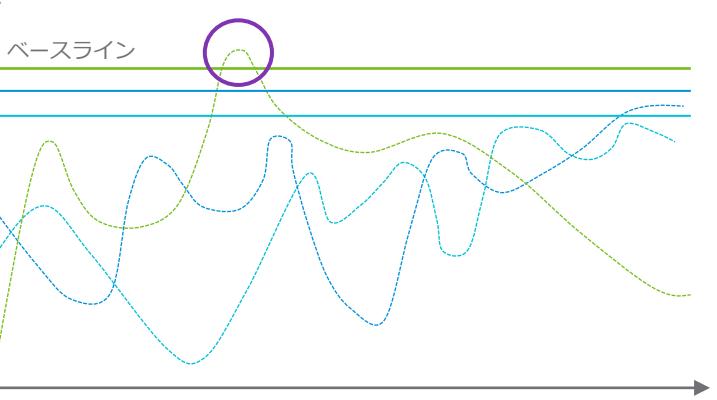
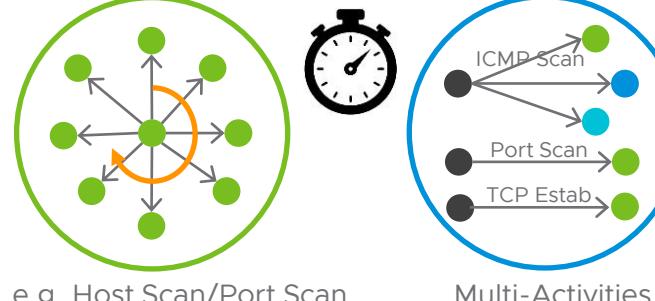


Behavioral IDSによる行動分析

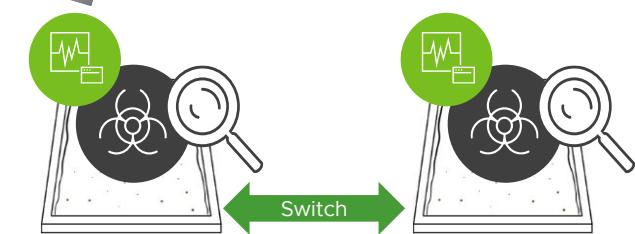
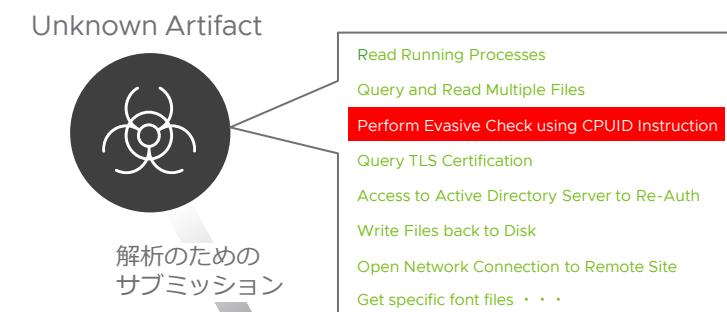
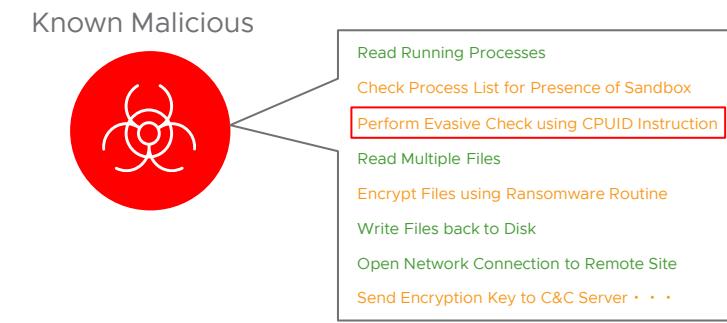
“ssh”トラフィックを検出したら、その後のトラフィック量を計測し異常を検出



Specific Duration

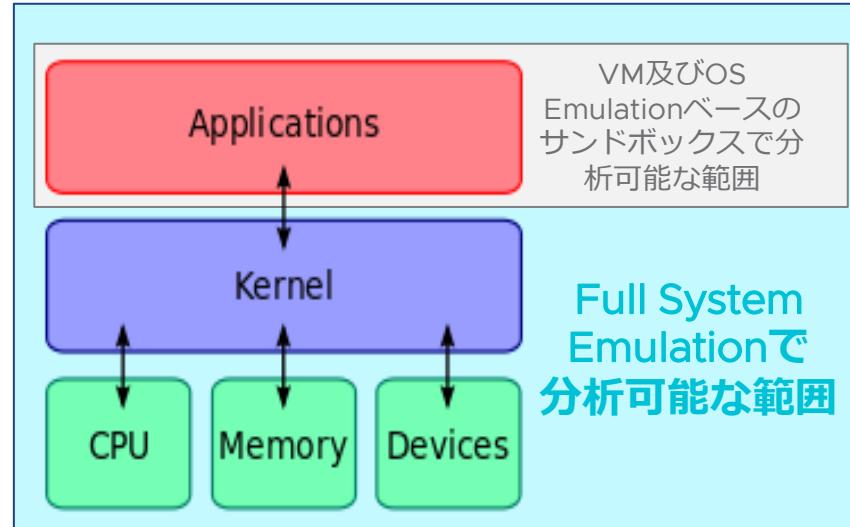
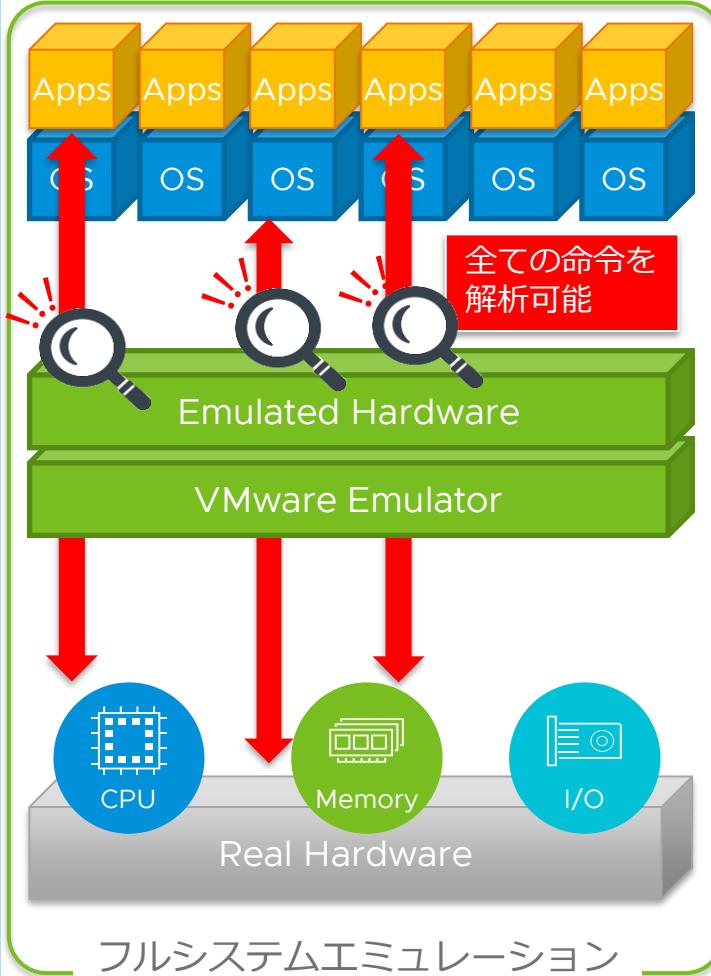


次の解析プロセスを決定づけるIDS

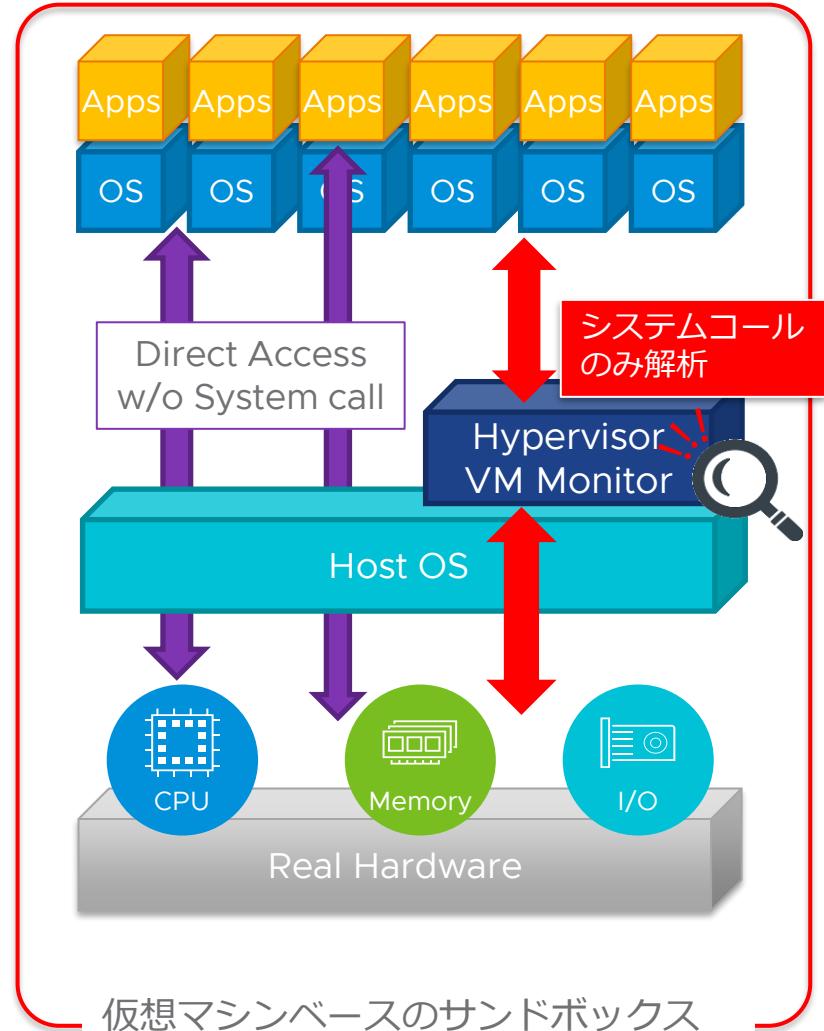


未知の脅威—サンドボックスによるマルウェア検知

Full System Emulation と Hypervisor Based



- ✓ 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



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



- 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説の精度が高い
- C2シグネチャのリアルタイム生成

トライ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

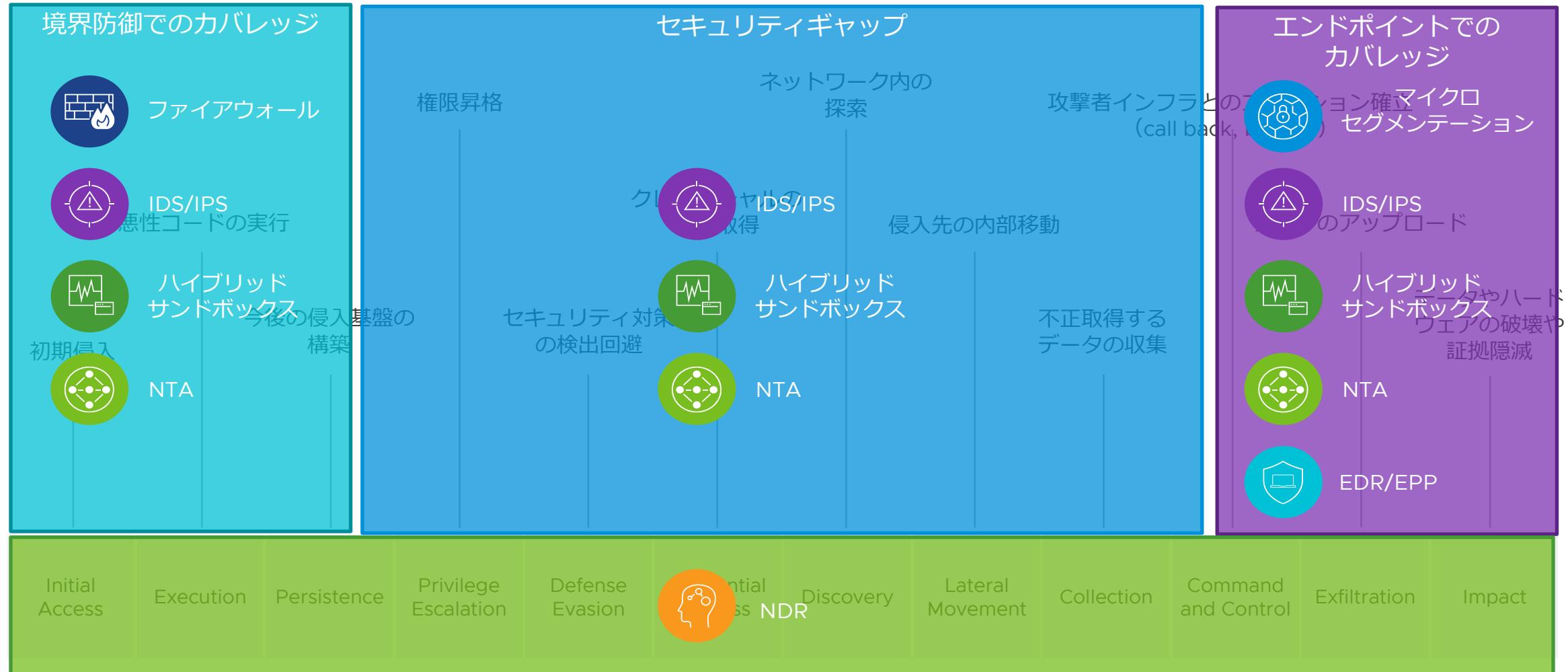
敵対者の戦術とテクニックのナレッジベース



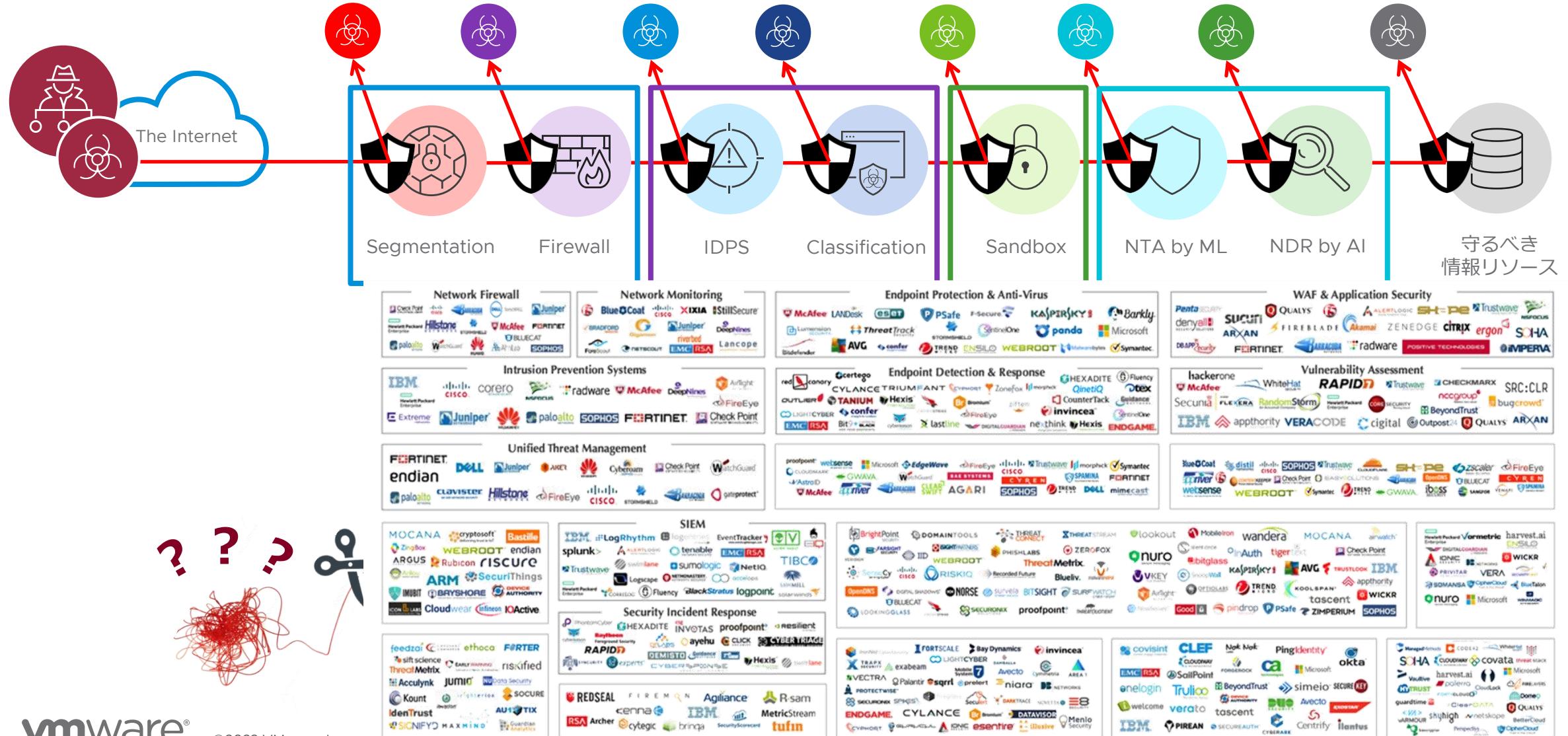
Tactics (戦術)	FW	IDPS	NTA	Sandbox
Initial Access (初期アクセス)	●	●		●
Execution (不正コード実行)				●
Persistence (永続性)		●	●	●
Privilege Escalation (特権昇格)	●	●	●	●
Defense Evasion (防御回避)	●	●		●
Credential Access (認証情報アクセス)		●		●
Discovery (検索)	●	●	●	●
Lateral Movement (水平展開)	●	●	●	●
Collection (情報収集)		●	●	●
Command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



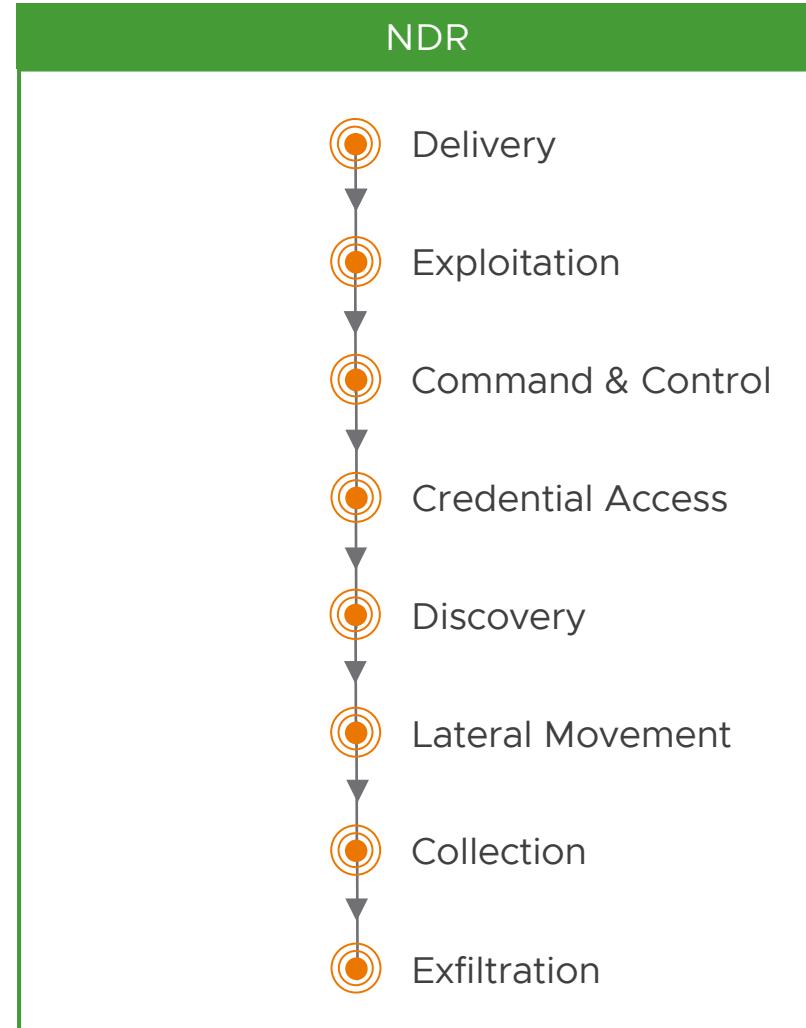
全イベントの相関関係と一連攻撃のMITRE ATT&CKマッピング

意味のある「コンテキスト」で攻撃全体を把握

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

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

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



攻撃キャンペーン全体を可視化—NDR 全体を網羅した可視化と統一した操作性

Overview Hosts Timeline History Evidence 攻撃ステージごとで検出したホスト概要

Threats and hosts

関与したホストや脅威の概要

9
THREATS

- Malicious File... 3 Hosts
- DGA activity 1 Host
- Empire Agent 2 Hosts
- CryptoWall 1 Host
- Magnitude EK 1 Host
- Dnscat 1 Host

[View threats details >](#)

3
HOSTS

- 192.168.20.151
- 192.168.100.181
- 192.168.20.211

[View hosts details >](#)

Impact: ● High ● Medium ● Low

Campaign blueprint

攻撃キャンペーンの全体の見取り図

The diagram illustrates a network of hosts connected by dashed lines, each associated with specific threat indicators:

- Host 91.250.34.89: Suspicious Kerberos AS_REQ RC4 Encryption
- Host 10.198.206.34: Dnscat, DGA activity
- Host 175.45.176.136: Malicious File Download
- Host 192.168.20.151: Suspicious Remote Task Scheduling, Empire Agent
- Host 192.168.20.211: Anomalous PSEXEC Interaction
- Host 192.168.100.181: Magnitude EK
- Host 34.102.136.180: CryptoWall
- Host 185.30.232.85: (No activity)
- Host 3a891f57: (No activity)

Legend (from left to right):

- Email address
- Email message
- Downloaded file
- Hostname
- Host
- FQDN has malicious reputation
- Info
- Analysis report
- Threat
- HTTP request

Overview	Hosts	Timeline	History	Evidence	攻撃キャンペーンの時系列アクティビティ		Show closed threats
				<div style="display: flex; justify-content: space-between;"> Sort by: Earliest (by start time) ▾ Search threats </div>			<input checked="" type="checkbox"/>
Feb 14, 01:15:48 - Feb 14, 01:15:48	> 192.168.100.181	05 MAGNITUDE EXI	EVIDENCE SUMMARY: 1 type: Signature	Latest stage Exploitation	OPEN	NEXT STEPS ▾	
Feb 14, 01:15:49 - Feb 14, 01:15:49	> 192.168.100.181	100 MALICIOUS FILE DOWNLOAD	EVIDENCE SUMMARY: 1 type: File download	Latest stage Delivery	OPEN	NEXT STEPS ▾	
Feb 14, 01:16:10 - Feb 14, 01:19:33	> 192.168.100.181	70 CRYPTOWALL	EVIDENCE SUMMARY: 1 type: Signature	Latest stage Command and Control	OPEN	NEXT STEPS ▾	
Feb 14, 01:22:53 - Feb 14, 01:40:27	> 192.168.100.181	25 ANOMALOUS PSEXEC INTERACTION	EVIDENCE SUMMARY: 1 type: Unusual behavior	Latest stage Lateral Movement	OPEN	NEXT STEPS ▾	
Feb 14, 01:43:06 - Feb 14, 01:43:06	> 192.168.20.211	75 EMPIRE AGENT	EVIDENCE SUMMARY: 1 type: Signature	Latest stage Command and Control	OPEN	NEXT STEPS ▾	
Feb 14, 01:45:07 - Feb 14, 01:45:07	> 192.168.20.211	100 MALICIOUS FILE DOWNLOAD	EVIDENCE SUMMARY: 1 type: File download	Latest stage Delivery	OPEN	NEXT STEPS ▾	
Feb 14, 01:45:31 - Feb 14, 01:54:25	> 192.168.20.211	20 SUSPICIOUS REMOTE TASK SCHEDULING	EVIDENCE SUMMARY: 1 type: Unusual behavior	Latest stage Lateral Movement	OPEN	NEXT STEPS ▾	
Feb 14, 01:45:34 - Feb 14, 01:45:34	> 192.168.20.211	20 SUSPICIOUS KERBEROS AS_REQ RSA ENCRYPTION	EVIDENCE SUMMARY: 1 type: Unusual behavior	Latest stage Credential Access	OPEN	NEXT STEPS ▾	
Feb 14, 01:49:48 - Feb 14, 01:58:41	> 192.168.20.151	20 SUSPICIOUS REMOTE TASK SCHEDULING	EVIDENCE SUMMARY: 1 type: Unusual behavior	Latest stage Lateral Movement	OPEN	NEXT STEPS ▾	
Feb 14, 02:04:03 - Feb 14, 02:04:03	> 192.168.20.151	75 EMPIRE AGENT	EVIDENCE SUMMARY: 1 type: Signature	Latest stage Command and Control	OPEN	NEXT STEPS ▾	
Feb 14, 02:06:07 - Feb 14, 02:06:07	> 192.168.20.151	100 MALICIOUS FILE DOWNLOAD	EVIDENCE SUMMARY: 1 type: File download	Latest stage Delivery	OPEN	NEXT STEPS ▾	
Feb 14, 02:06:26 - Feb 14, 02:06:55	> 192.168.20.151	65 ENIGMA	EVIDENCE SUMMARY: 1 type: Signature	Latest stage Exfiltration	OPEN	NEXT STEPS ▾	
No activity: Feb 14, 02:06:55 - 02:50:52 - (44 minutes)							
Feb 14, 02:50:52 - Feb 14, 03:04:05	> 192.168.20.151	80 DSA ACTIVITY	EVIDENCE SUMMARY: 1 type: Anomaly	Latest stage Command and Control	OPEN	NEXT STEPS ▾	

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



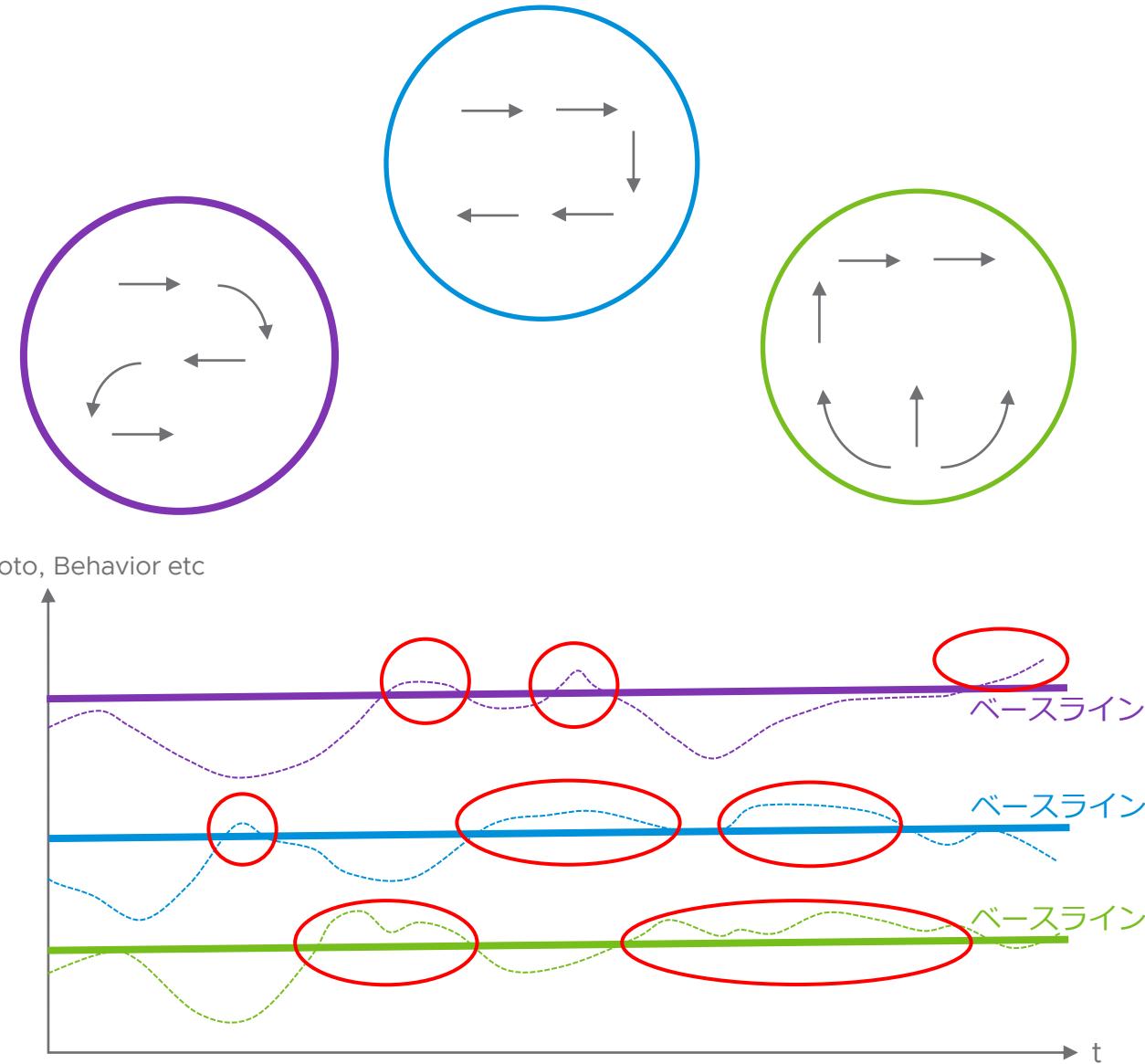
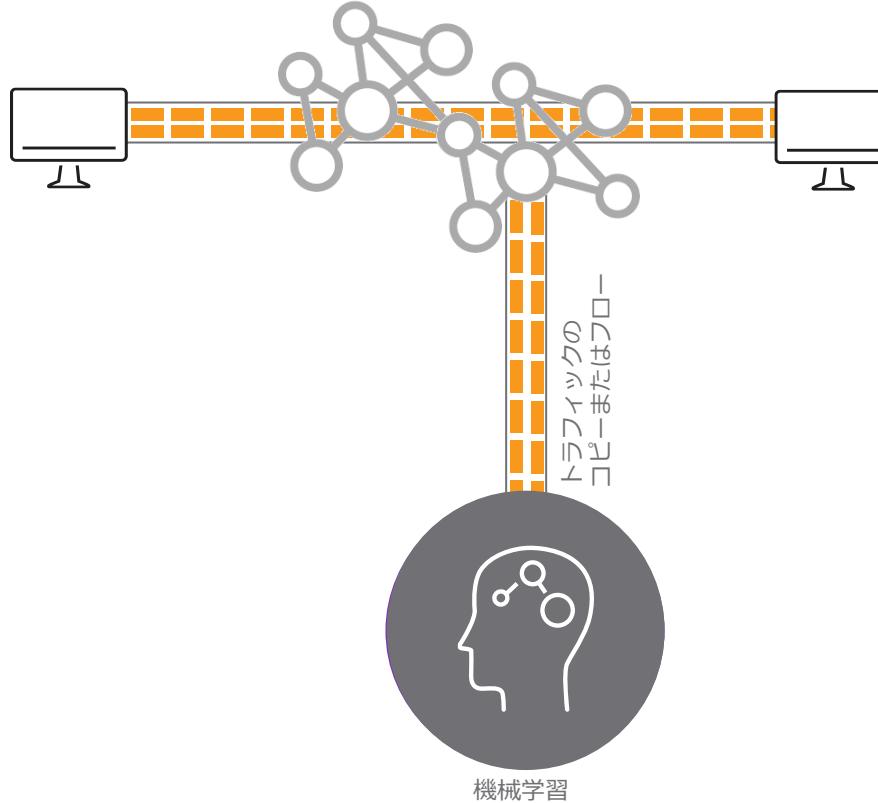
The screenshot shows a search results page for 'Network Detection and Response' on Gartner peer insights. The header includes the Gartner logo, a search bar, and navigation links for Write a Review, Categories, Log In, and For Vendors. The main content area displays a list of reviews with columns for Rating, Vendor, Product, and Market Name. At the bottom, there are links for EMAIL PAGE and PDF.

What is Network Detection and Response?

NDR solutions primarily use non-signature-based techniques (for example, machine learning or other analytical techniques) to detect suspicious traffic on enterprise networks. NDR tools continuously analyze raw traffic and/or flow records (for example, NetFlow) to build models that reflect normal network behavior. When the NDR tools detect suspicious traffic patterns, they raise alerts. In addition to monitoring north/south traffic that crosses the enterprise perimeter, NDR solutions can also monitor east/west communications by analyzing traffic from strategically placed network sensors. Response is also an important function of NDR solutions. Automatic responses (for example, sending commands to a firewall so that it drops suspicious traffic) or manual responses (for example, providing threat hunting and incident response tools) are common elements of NDR tools.

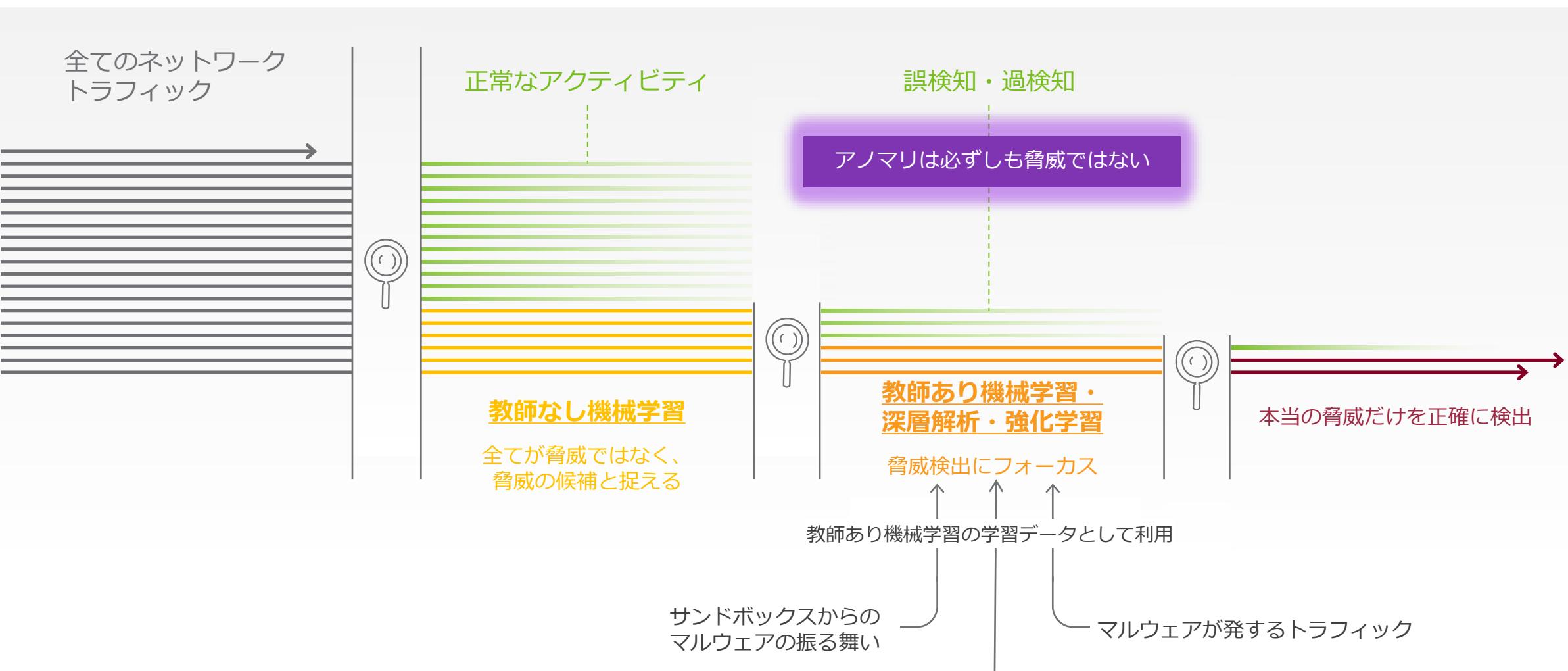
NTA

Network Traffic Analysisとは



AIによる NDR

フォルスポジティブの排除



「適切なレスポンス」に必要なもの

NTA / 一般的 NDR

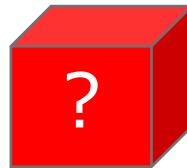
シグネチャを利用せずに、不審なトラフィックを検出する



シグネチャ



機械学習



ロジックが
見えない箱



普通ではないようだ....が根拠不明...



証拠不十分・詳細不明

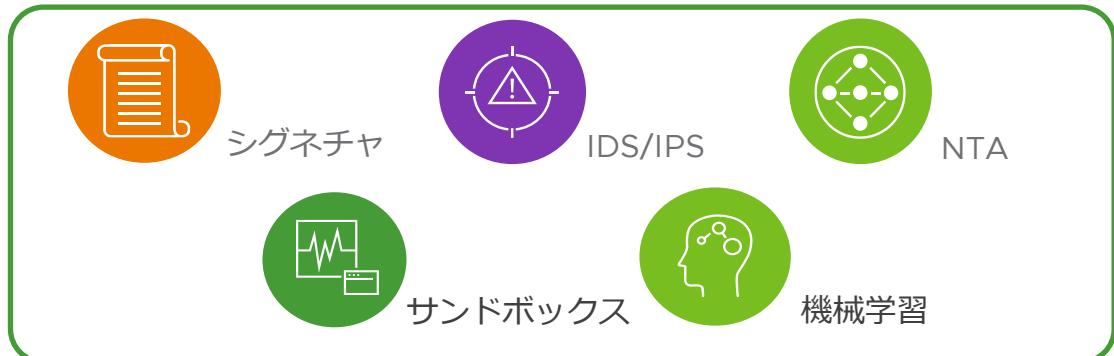


適切な対処困難

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」



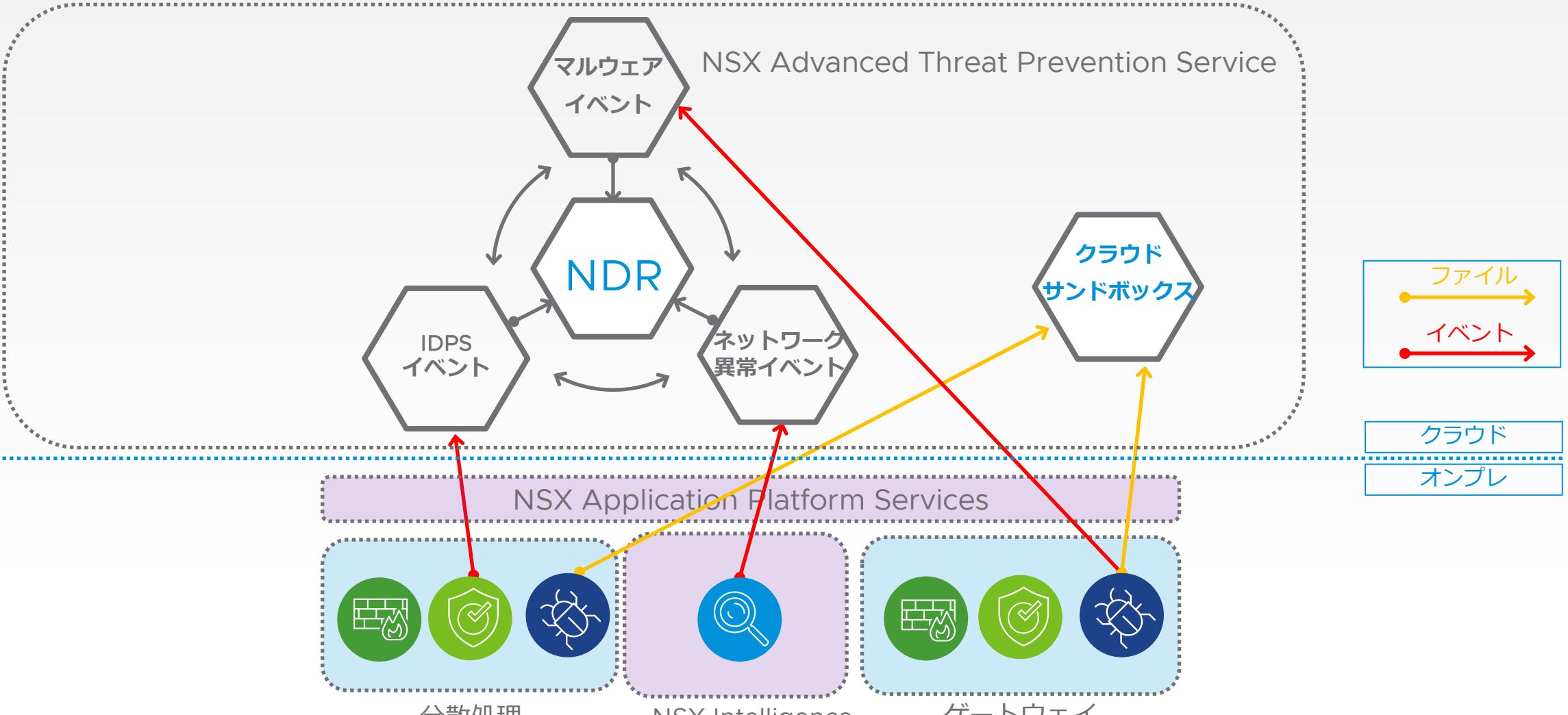
- ✓ シグネチャ
- ✓ パケット
- ✓ 3ウェイハンドシェイク
- ✓ HTTPレスポンスコード など



適切な対処

NDR

イベントの関連付け – 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			
 A circular seal with "SE Labs" at the top and bottom, "AAA" in the center, and "AUGUST 2021" at the bottom. The text "Network Detection & Response" is curved along the bottom edge.			
Total Rating	100%	100%	100%
Detection Accuracy	100%	100%	100%
Legitimate Accuracy	100%	100%	100%

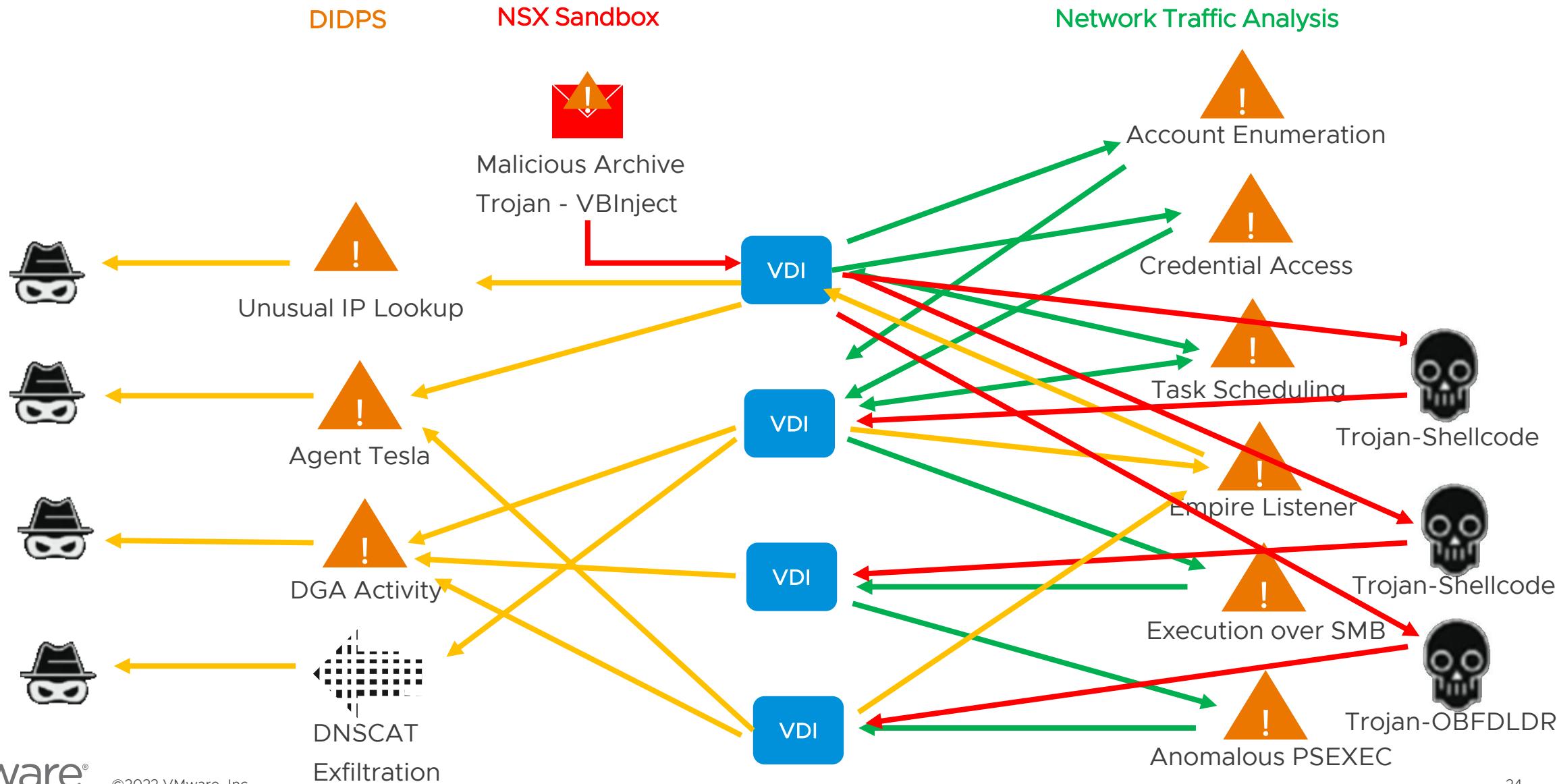
LEGITIMATE ACCURACY			
False Positives		0%	

THREAT RESPONSE DETAILS			
Threat	Target	Score	Overall Score
FIN7 & Carbanak	🛒	100%	100%
OilRig	\$	100%	100%
APT3	⚡	100%	100%
APT29	🏛️	100%	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 focuses on achieving detailed results, integrity in the testing process, useful threat intelligence and test innovation.

Licensed for republication by VMware, Inc.
© 2021 SE Labs Ltd

Oilrig APT (APT34) のアクティビティ



デモ

NSX

Not secure | https://nsx-demo-atp-1/nsx/#/app/home/overview

vmw NSX-T

Home Networking Security Inventory Plan & Troubleshoot System

Search What can I search?

Overview Alarms Monitoring Dashboards Documentation

NETWORKING

- 1 Tier-0 Gateway
- 8 Segments
- 4 NAT Rules
- 0 EVPN Tenants
- 0 Advanced LB Virtual Services
- 3 Tier-1 Gateways
- 0 Distributed Port Groups
- 0 VPN Services
- 0 Load Balancers

SECURITY

- 12 Distributed FW Policies
- 0 Endpoint Policies
- 0 Network Introspection NS Policies
- 0 IDS/IPS Gateway Policies
- 2 Malware Prevention Gateway Policies
- 5 Gateway Policies
- 1 Network Introspection EW Policy
- 2 IDS/IPS Distributed Policies
- 1 Malware Prevention Distributed Policy

INVENTORY

- 36 Groups
- 22 Virtual Machines
- 0 Physical Servers
- 411 Services
- 66 Context Profiles
- 2 L7 Access Profiles

SYSTEM

- 2 Transport Zones
- 1 Edge
- 1 Edge Cluster
- 1 NSX Management Node ⚠️ 3 node cluster recommended
- 1 Service Deployment
- 12 Roles
- 3 of 3 Hosts Configured
- 1 Host Cluster
- 12 Users

Preparing more Hosts or Edges? Visit [QUICK START](#)

The screenshot shows the VMware NSX-T Management interface. The top navigation bar includes Home, Networking, Security, Inventory, Plan & Troubleshoot, System, a search bar, and user information. Below the navigation is a search bar and a placeholder 'What can I search?'. The main content area is divided into four sections: Networking, Security, Inventory, and System. The Networking section shows 1 Tier-0 Gateway, 8 Segments, 4 NAT Rules, 0 EVPN Tenants, 0 Advanced LB Virtual Services, 3 Tier-1 Gateways, 0 Distributed Port Groups, 0 VPN Services, and 0 Load Balancers. The Security section shows 12 Distributed FW Policies, 0 Endpoint Policies, 0 Network Introspection NS Policies, 0 IDS/IPS Gateway Policies, 2 Malware Prevention Gateway Policies, 5 Gateway Policies, 1 Network Introspection EW Policy, 2 IDS/IPS Distributed Policies, and 1 Malware Prevention Distributed Policy. The Inventory section shows 36 Groups, 22 Virtual Machines, 0 Physical Servers, 411 Services, 66 Context Profiles, and 2 L7 Access Profiles. The System section shows 2 Transport Zones, 1 Edge, 1 Edge Cluster, 1 NSX Management Node (with a warning for a 3-node cluster), 1 Service Deployment, 12 Roles, 3 of 3 Hosts Configured, 1 Host Cluster, and 12 Users. A note at the bottom of the System section says 'Preparing more Hosts or Edges? Visit [QUICK START](#)'. A yellow callout box highlights the '1 NSX Management Node' entry.



Thank You