

vFORUM 2019

NS144

堅牢な SDDC を実現する

- VMware セキュリティソリューション -

vSphere Platinum と NSX による ゼロトラスト セキュリティ

ヴァイムウェア株式会社

ソリューションビジネス本部

ネットワーク & セキュリティ技術部

シニアスペシャリストエンジニア 長門石 晋

Make Your Mark

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

情報セキュリティをとりまく状況の変化

SDDCによる効果的なセキュリティ対策の基本要素

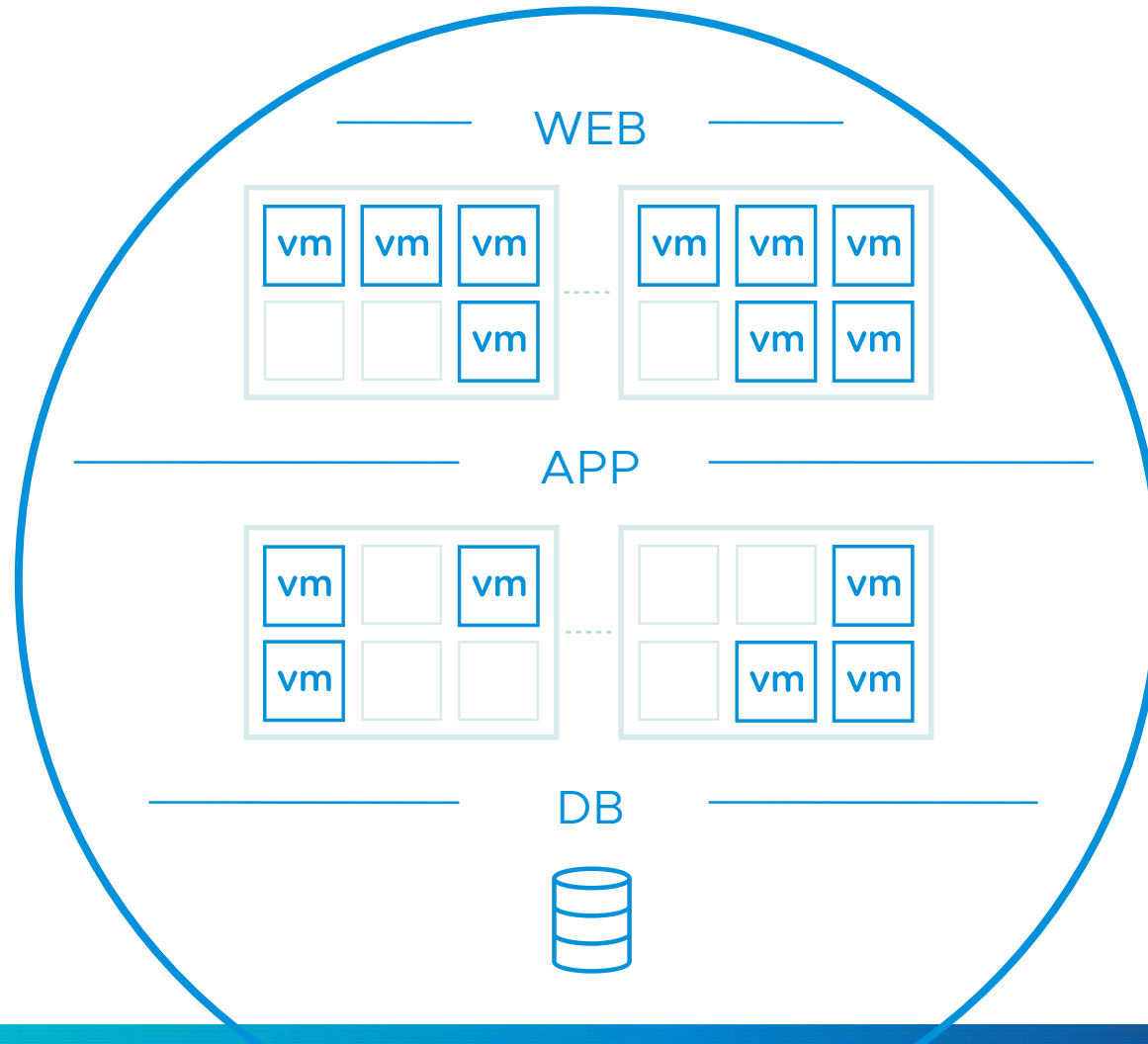
- サイバーハイジーンの基本原則の実装
- マイクロセグメンテーション + 他社連携による対策の高度化
- vSphere 組み込み型セキュリティ機能
- 高度なセキュリティ機能 : AppDefense / vSphere Platinum / NSX Intelligence

まとめ

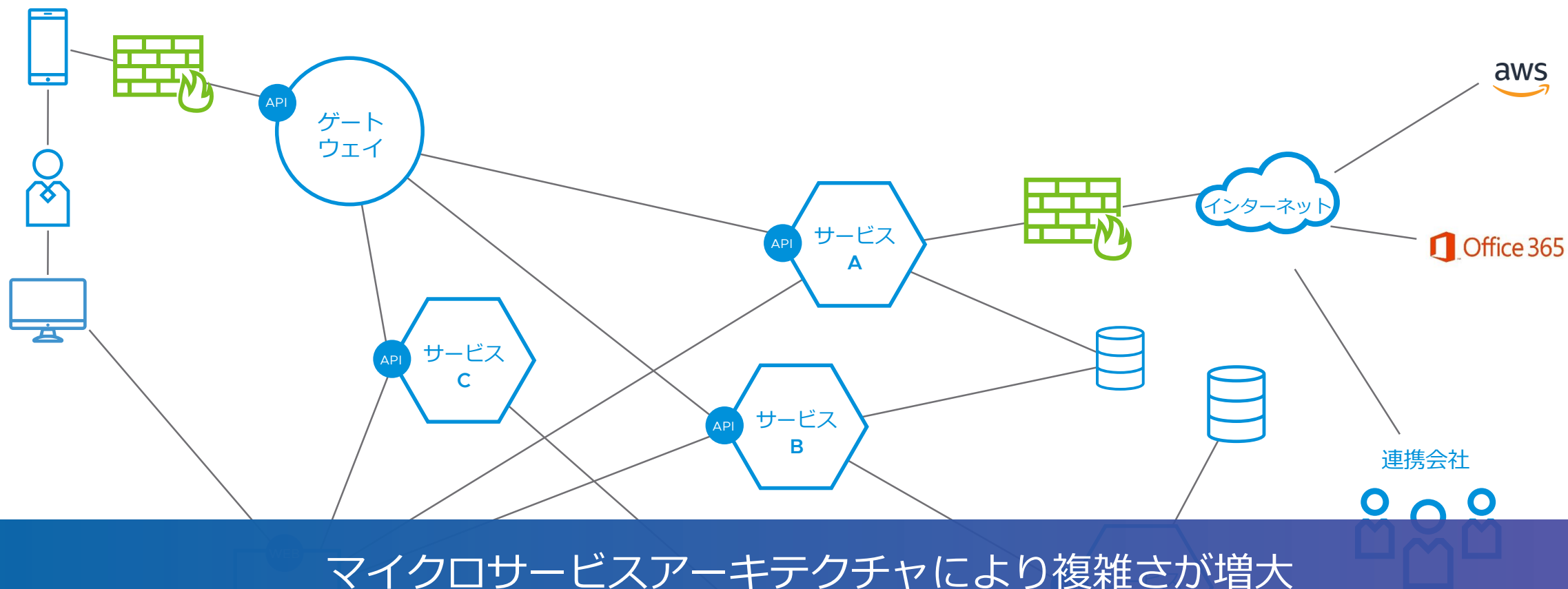
業務システム



階層化分割



クラウドネイティブ アプリケーション



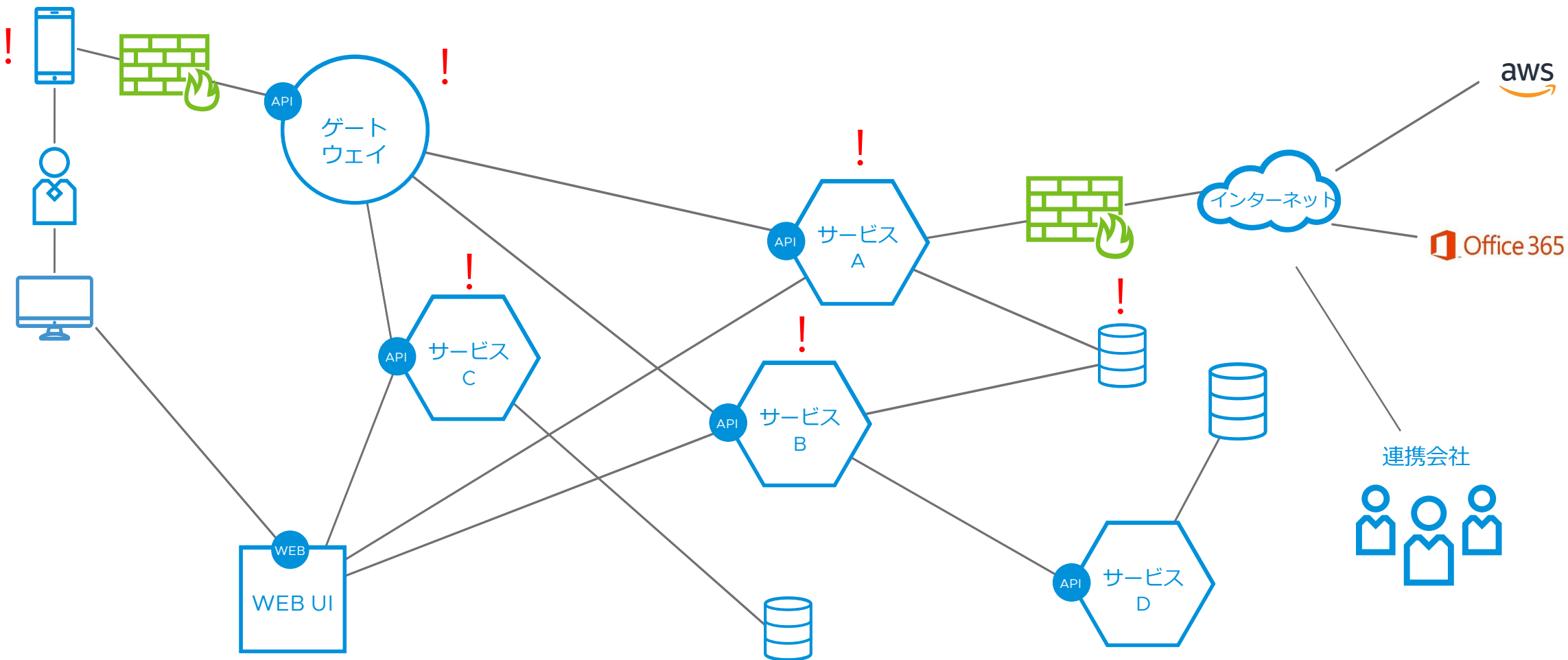
マイクロサービスアーキテクチャにより複雑さが増大

管理が分散した
セキュリティ対策

分散
アプリケーション

10-100-1000 規模
のサービス管理

短時間に変更される
サービスの短命さ



内部対策としての E-W セキュリティは
依然として大きな課題に...

従来型セキュリティによる内部対策の難しさ

数字によるセキュリティの実態

～ 3 ヶ月

攻撃者のシステム内に留まり、
滞在(潜伏)する平均期間
(2018年)

#1

もっとも窃取された情報
クレデンシャル
(2018年)

386万ドル

約 4 億円

情報えいによる
被害金額の平均
(2018年)







75

企業内で使われる
セキュリティツール数(平均)

国内のセキュリティ被害の実態

過去 10 年の平均と比較して..

個人情報漏えいインシデント 概要データ





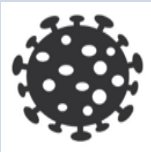
漏えい人数		519万8,142人
インシデント件数		386件
想定損害賠償総額		1,914億2,742万円
一件あたりの漏えい人数		1万4,894人
一件あたり平均想定損害賠償額		5億4,850万円
一人あたり平均想定損害賠償額		2万3,601円

出展：JNSA「2017年 情報セキュリティインシデントに関する調査報告書
～個人情報漏えい編～」のデータを元に作成

<https://www.jnsa.org/seminar/2018/0612/data/A1-2incident.pdf>

セキュリティインシデントは発生し続けている
・・・なぜ？

高度なサイバー攻撃の背景

	妨害行為	ハクティビズム (思想・信条動機)	犯罪	諜報活動	戦争行為
目的	 侵入・増殖	 誹謗中傷、 圧力行為、政策批判	 金銭窃取	 経済、 政策的優位性	 破壊行為
例	ボットネット・ スパムメール	ウェブサイトの 改ざん	クレジット情報、 ランサムウェア	標的型攻撃	重要インフラの 破壊
標的型		✓	✓	✓	✓
特性	機械的 自動的	自意識の高い 人目を引く行為	機を見て対処	しつこく何度も 繰り返す	対立関係 が推進

可能性
深刻度

サイバー攻撃の高度化・巧妙化により既知の攻撃への対処
では対応しきれない状況となっている

IT 環境をとりまく状況の変化

攻撃対象の側面が多角化・拡大し、サイバーセキュリティの脅威はより高度・複雑に

組織を取り巻く IT 環境の変化

グローバル化の進展
と
競争激化

インフラ・
アプリケーションの
クラウド移行

業務での
スマートデバイス活用

テレワーク

一般社会への
IT の浸透
(スマートシティ、IoT)

情報セキュリティにおける課題

組織的犯罪の増加

セキュリティ
境界線の変化

攻撃手段の巧妙化

利用者側の
セキュリティ意識
の低さ

あらかじめこうした変化を前提として
セキュリティを考慮した IT 基盤の構築がより求められる

「セキュリティ対策は突破される可能性がある」

「脅威は侵入し得る」という前提

従来のセキュリティ モデル

アクセス制御・ID / クレデンシャル・デバイス・ワークロード
IP アドレス・プロトコル・システム衛生状態・利用状況, etc..

組織のネットワーク内にあるものは
すべて**信頼できる**という前提

ゼロトラストのセキュリティ モデル

組織のネットワーク内にあるものは
すべて**信頼しない**という前提

なにも信頼せず、すべてを**確認**するモデル

VMware SDDC は、効果的なセキュリティ対策に活用できる？

効果的なセキュリティ対策を 実現するための基本技術要素

サイバーハイジーンの基本原則の実装

サイバーハイジーンの基本原則

VMware が提唱する 5 つの要素

VMware の考える「サイバーハイジーン」の定義

サイバー攻撃から重要な資産を守るために、
組織が備えておく必要のある基本的な要素

最小限
の権限



パッチ
適用



多要素認証



マイクロ
セグメン
テーション



暗号化

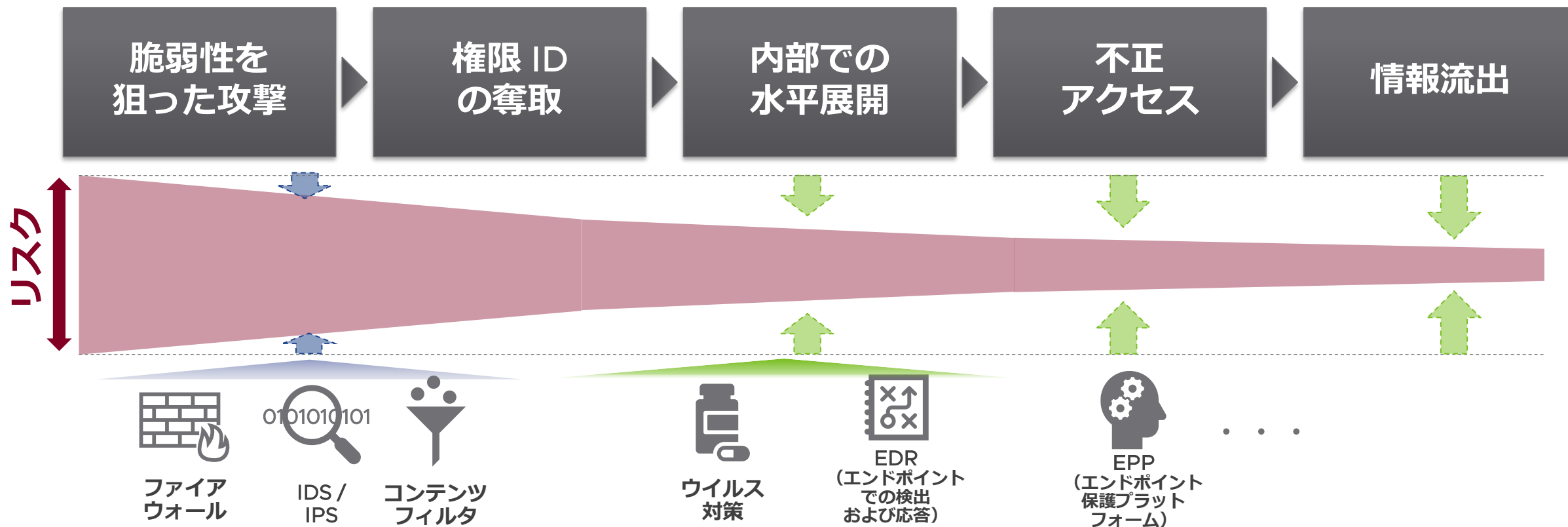


新しい概念というよりも、より効率的なセキュリティの実現に大きな影響を持つ要素

NIST サイバーセキュリティ フレームワーク などの確立されたフレームワークをベースにした テクノロジー ニュートラルな原則

標的型攻撃の流れとサイバーハイジーンの要素

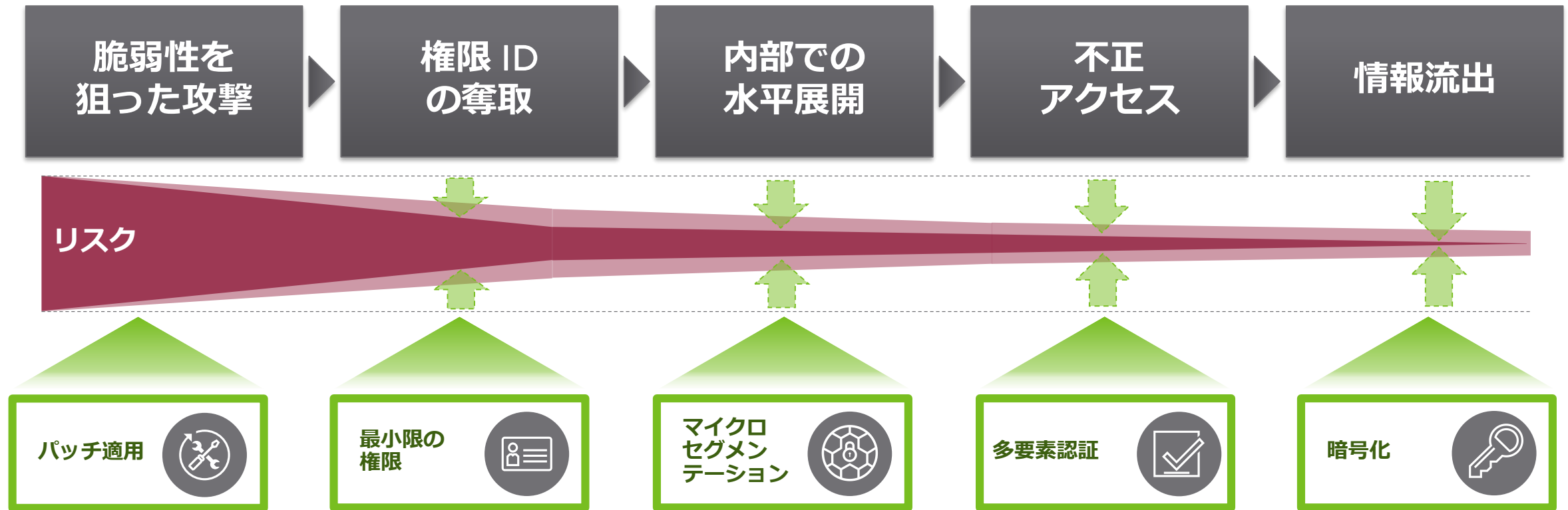
標的型攻撃の流れと5つの要素との対応



サイバーハイジーンの要素を実現することで
人手をかけることなくより効果的に攻撃コストを上げることが可能

標的型攻撃の流れとサイバーハイジーンの要素

標的型攻撃の流れと5つの要素との対応



サイバーハイジーンの要素を実現することで
人手をかけることなくより効果的に攻撃コストを上げることが可能

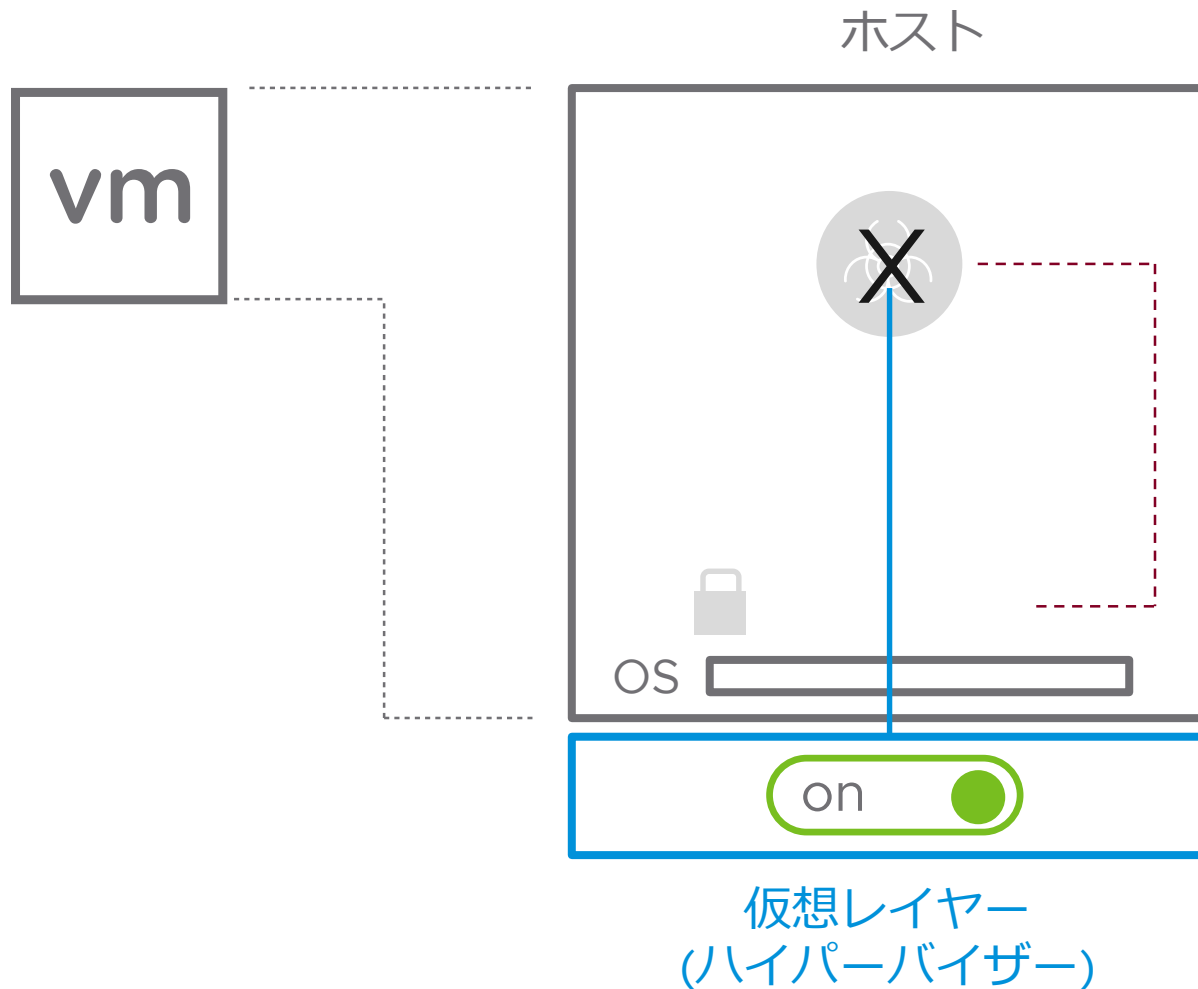
効果的なセキュリティ対策を 実現するための基本技術要素

実現を下支えする基礎技術を解説

VMware NSX Data Center セキュリティ
マイクロセグメンテーション

VMware マイクロセグメンテーション - 分散技術によるポリシーの強制

Root 権限の1つ上の機構から、より強固な保護機能を提供



一般的なエージェント依存のアプローチ

Linux ipsets/iptables、Windows Defender Firewall
のルールに反映させることで アクセス制御を実施
(ゲスト OS レベルでの対策)

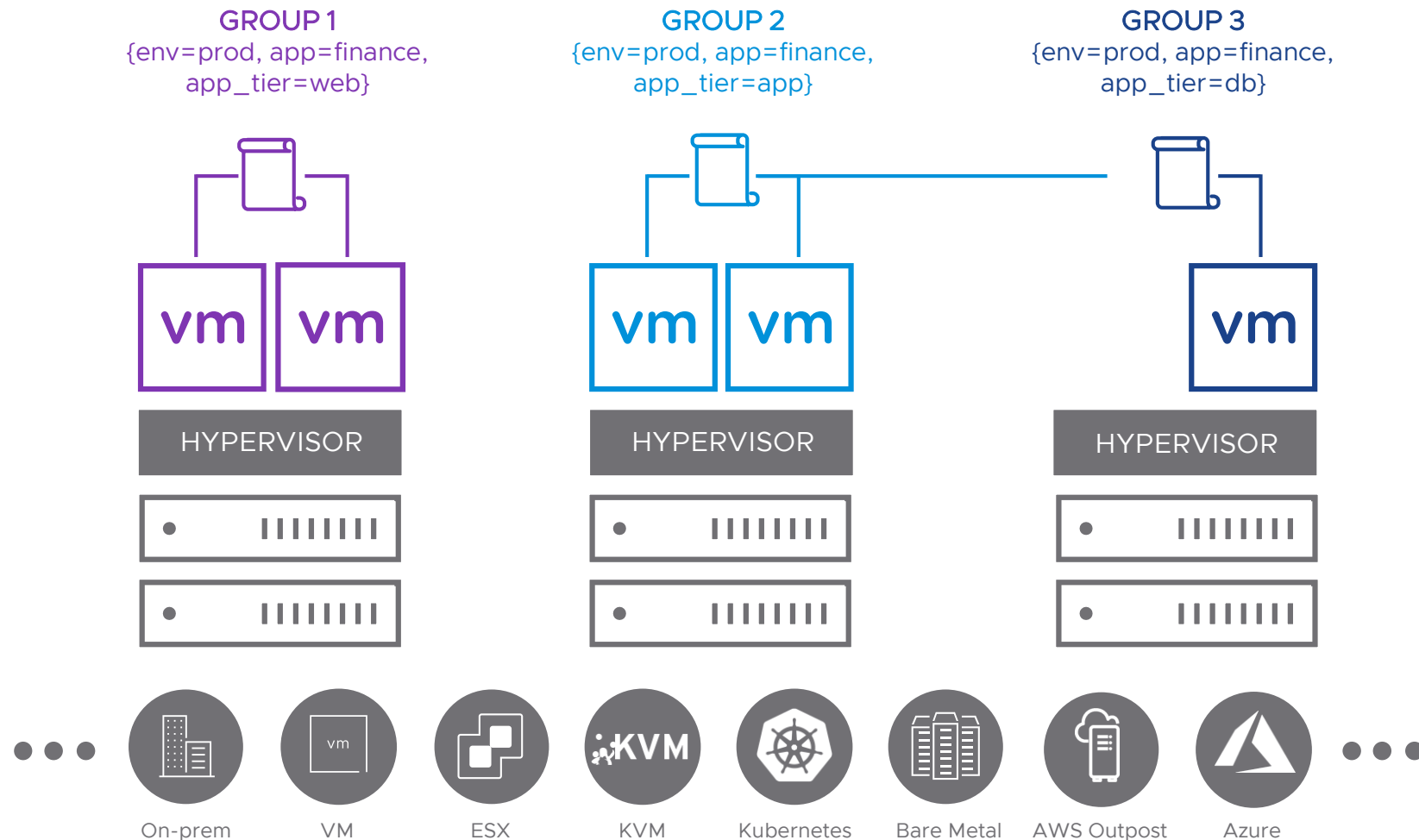
一度 Root 権限が奪取されると、
仮想レイヤーによるアクセス制御の強制
エージェントによる保護が解除された状態に
攻撃に対して、OS 非依存型で効率的かつ確実な防御が可能
エージェントが OS を効果的に保護することは事実上不可能

分散ファイアウォール のアプローチ

ワークロード単位でファイアウォールポリシーを適用
より粒度の細かいセグメンテーションを実現
(仮想化レイヤーでの対策)

VMware マイクロセグメンテーション - リアルタイム制御

リアルタイムにワークロードの変化へ追従



透過型 Stateful Firewall を提供

アプリケーション毎に
セグメンテーション (グループ化)

ワークロードの変化に追従した
リアルタイムな保護

AV など 3rd Party 製品連携で
検知と保護の連携の自動化

トポロジーフリーでシンプルな
ファイアウォールルール (ポリシー)
で運用が可能に

分散ファイアウォール - East-West サービスインサーション

vNIC に適用する 3rd パーティ ネットワークサービスインサーション

Palo Alto Networks, Fortinet, Check Point



FORTINET



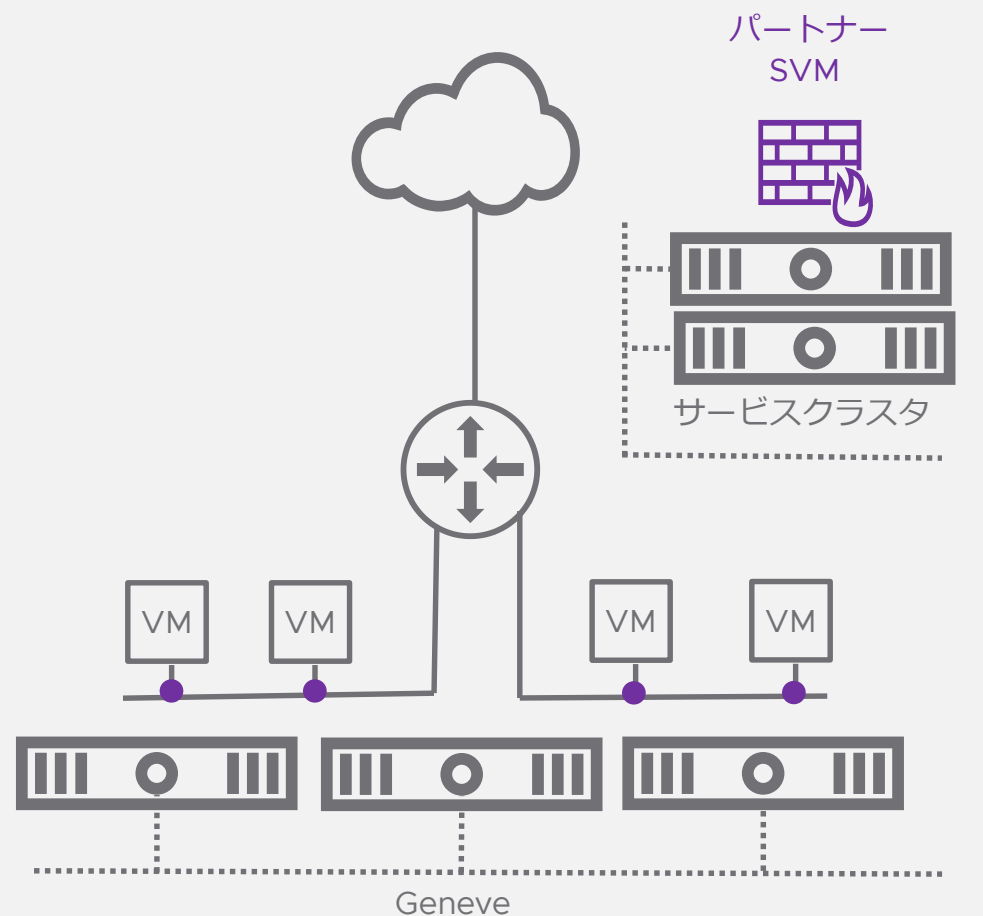
NETSCOUT

vStream *

* Coming Soon!

vmware®

©2019 VMware, Inc.



East-West トラフィックに対する
高度なセキュリティサービスの挿入

分散ファイアウォールと連携して、
vNIC を通過するパケットをインターセプト

ネットワークトポロジーに
依存しないサービスインサーション

弊社パートナーが提供する
高度なセキュリティ機能と併用可能
(IP レピュテーション, URL フィルタリング,
パケットキャプチャ、等)

VMware NSX-T™ Data Center の
組み込みの仕組みに
セキュリティ機能のアドオンが可能

基盤構築後も、無理な変更なく
透過的にサービス挿入がいつでも可能

従来型ファイアウォール - トラフィックのヘアピンによる対策

効率性の低い複雑なアーキテクチャ

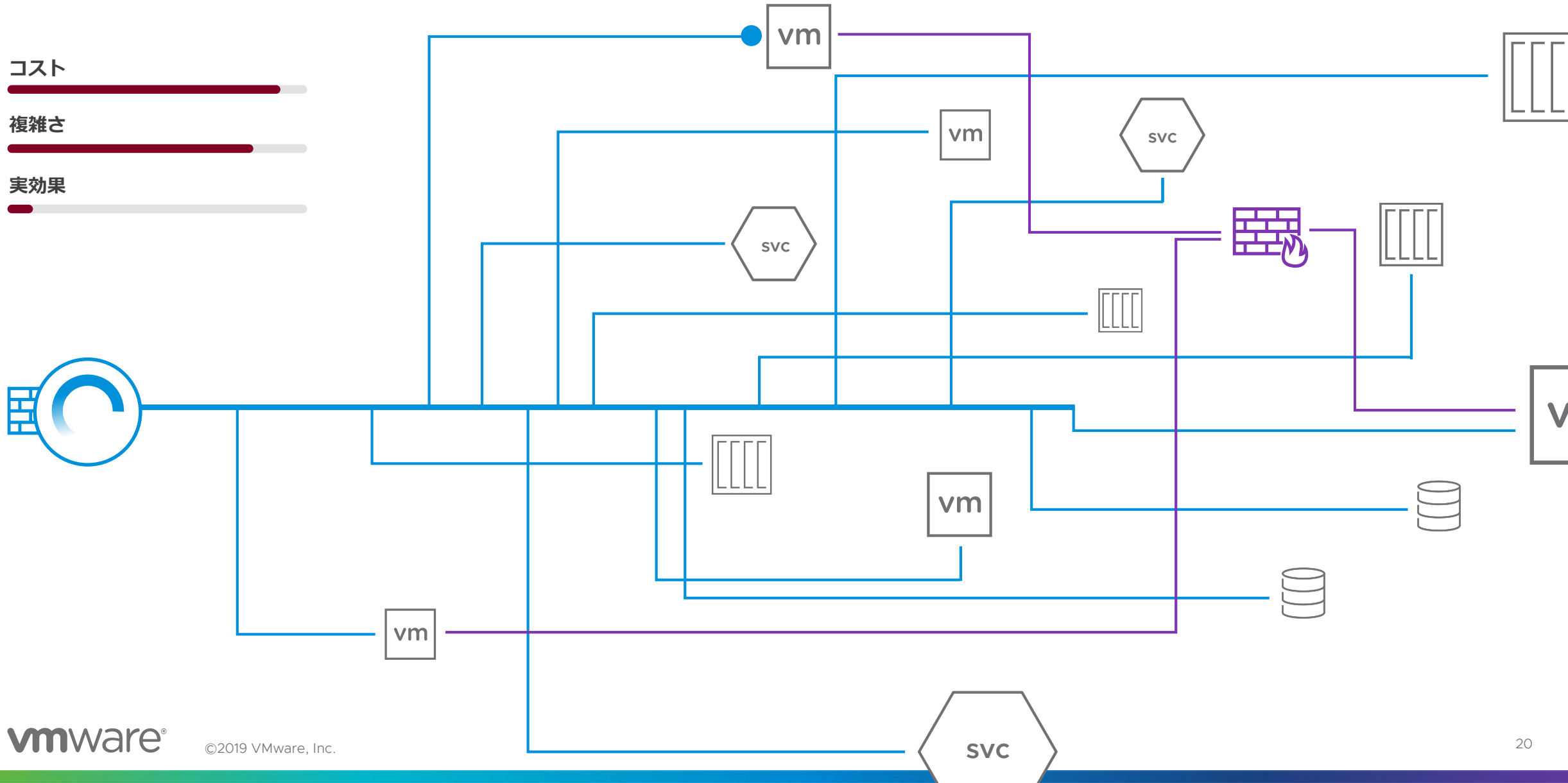
コスト



複雑さ



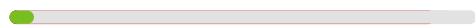
実効果



分散ファイアウォール – 分散技術によるポリシー強制

全てのパケットをインスペクション – 全ワークロードを攻撃からの保護対象に

コスト



複雑さ



実効果

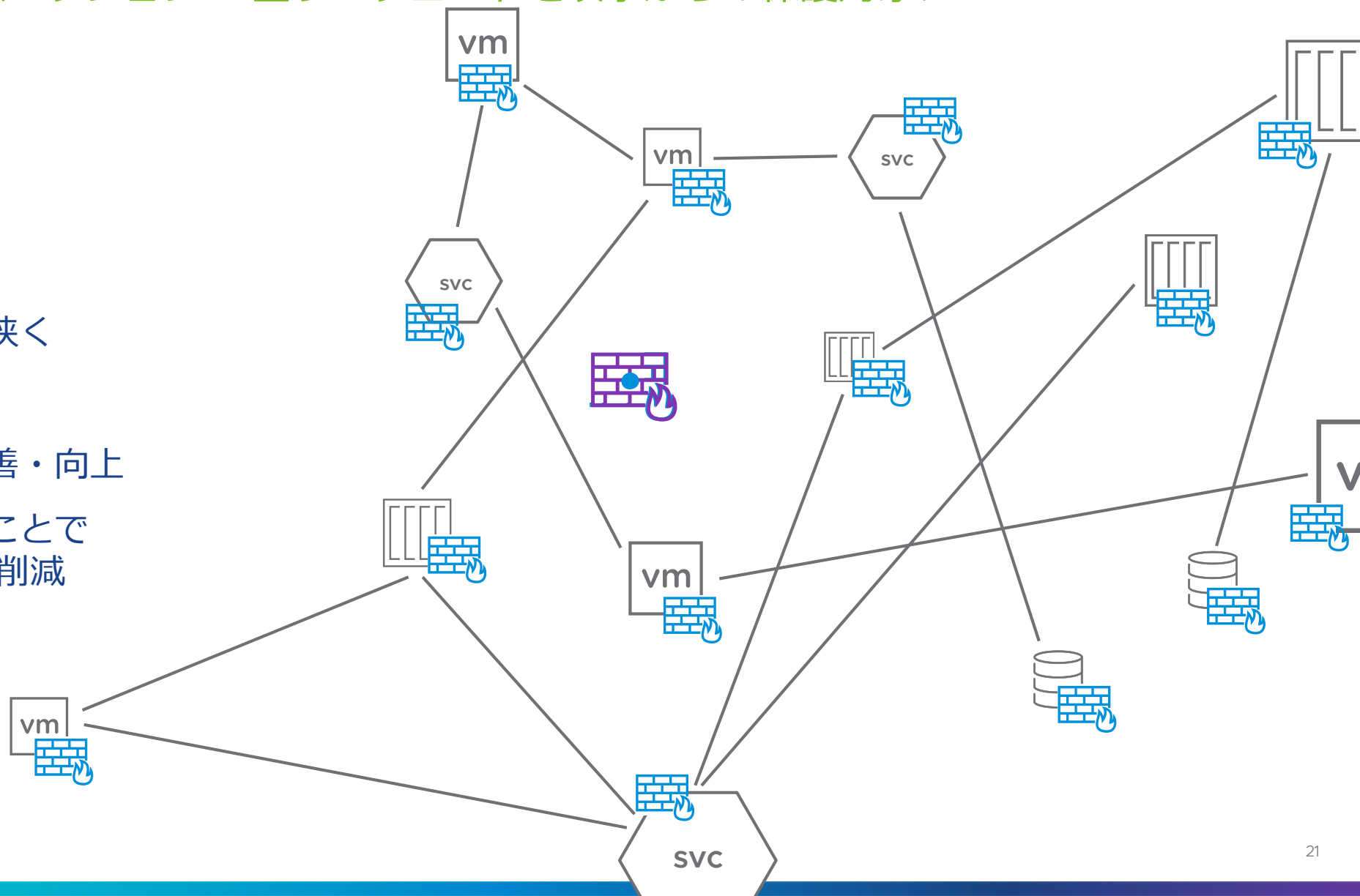


攻撃対象の側面を限りなく狭く

保護機能はよりシンプルに

ネットワーク処理性能の改善・向上

組み込みの技術を活用することで
CapEx を最大で 60 % まで削減



効果的なセキュリティ対策を実現するための基本技術要素

実現を下支えする基礎技術を解説

vSphere 組み込み型セキュリティ機能

高度なセキュリティ機能

- AppDefense / vSphere Platinum

ハイパーバイザーベースの防御 – 仮想基盤の信頼性向上

ハイパーバイザーベースの防御

ハイパーバイザーによる OS の完全性・整合性のチェックと情報保護



UEFI による
セキュアブート

VMware ESXi™ と
ゲスト OS の
起動時に、デジタル署名を
用いて完全性を検証

ルートキットや
マルウェアの定着から保護



Virtualization
Based
Security
(VBS)

Device Guard, Credential
Guard, HVCI の利用

Pass-the-Hash 攻撃から
クレデンシャル情報を保護



VM Encryption

XTS-AES で
仮想マシンデータを暗号化

仮想マシンのディスクやファイルも保護
暗号化機能でマルチクラウド環境での
vMotion などをセキュアに実行可能

整合性・完全性レポート

対象の VM から検出された OS / ドライバーの不正操作や改ざんチェック

日本語表示対応

vm vSphere Client

Menu Search in all environments Administrator@VSPHERE.LOCAL

jenny-win-2008-new2

Summary Monitor Configure Permissions Datastores Networks Updates

Issues and Alarms
All Issues
Triggered Alarms

Performance
Overview
Advanced

Tasks and Events
Tasks
Events
Utilization

AppDefense
Guest Integrity
Guest Monitoring
Vulnerabilities

Guest Integrity

VM belongs to scope windows and service 1.

DELETE

	Sev	Process	Event Sub Type	Last Received At	Last Remediation Action
<input type="checkbox"/>	⚠	logger	Guest Integrity Code	Feb 5, 2019, 4:02:47 AM	Action taken: Appdefense - Alert
<input type="checkbox"/>	⚠	systemd-cgroups-agent	Guest Integrity Code	Feb 5, 2019, 4:01:36 AM	Action taken: Appdefense - Alert
<input type="checkbox"/>	⚠	flock	Guest Integrity Code	Feb 5, 2019, 3:16:40 AM	Abandoned: Appdefense - Power Off
<input type="checkbox"/>	⚠	chronyd	Guest Integrity Code	Feb 4, 2019, 4:24:25 AM	Abandoned: Appdefense - Suspend

検出されたアラートに対して、隔離・サスペンドなどのアクションが可能

仮想マシンの OS とロードされているすべてのドライバーの整合性・完全性を確認
セキュリティイベントは VMware vCenter Server® 管理者に警告が表示され、追加調査へ繋ぐことが可能

脆弱性レポート - Gest OS で検出された脆弱性

対象の VM から検出された脆弱性を OS / アプリ毎にリスト

OS/アプリベンダー、バージョンに加え、該当の脆弱性のCVEコードや、外部参考リンクを VMware vCenter® からまとめて確認

日本語表示対応

Search in all environments



Administrator@VSPHERE.LOCAL



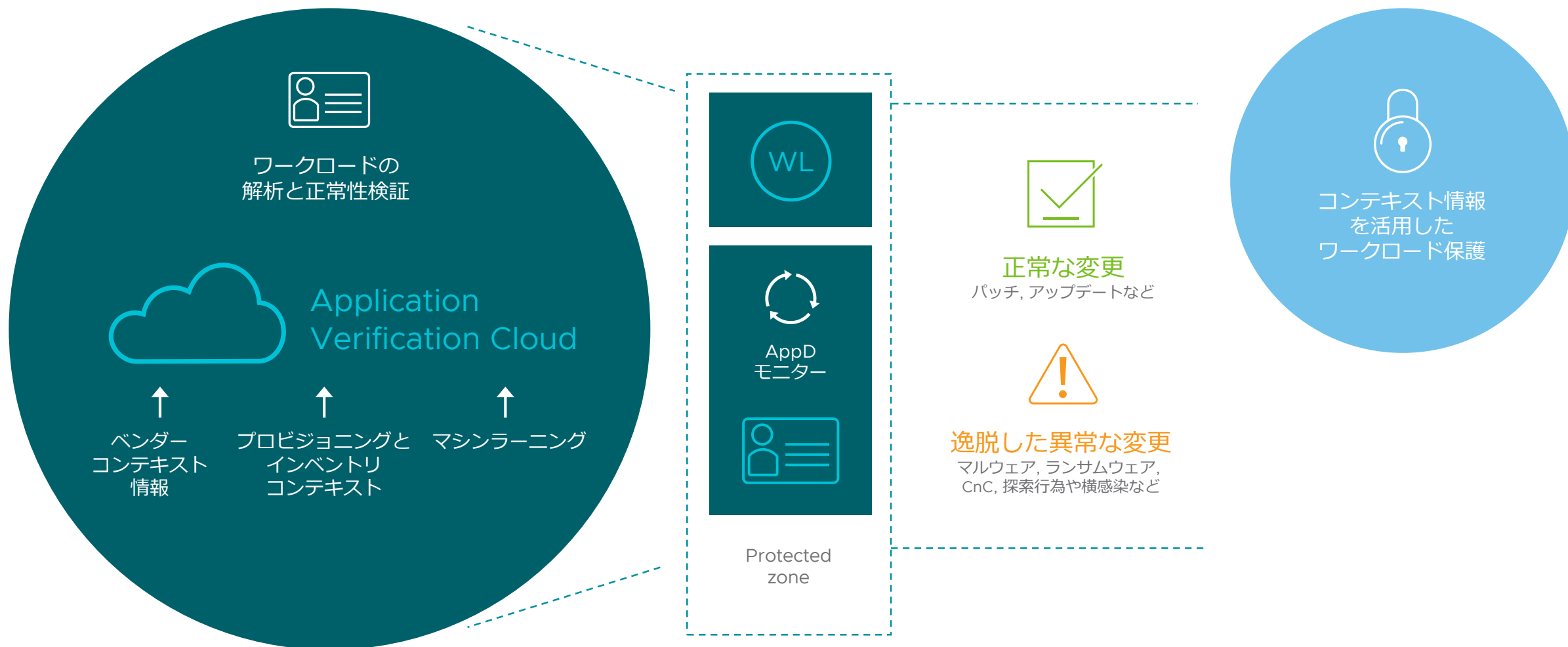
The screenshot shows the VMware vCenter AppDefense interface. On the left, a list of VMs is displayed, with 'jenny-win-2008-new2' selected. The main panel shows the 'Vulnerabilities' section for this VM. The 'OS' tab is selected, showing a bar chart with 86 vulnerabilities. The table below lists the vulnerabilities, including their severity, vendor, product name, version, CVE ID, and risk score.

Severity	Vendor	Product Name	Version	CVE Id	Risk Score	Fixed By
Important	Microsoft Corporation	Internet Explorer	11.00.14393.2007	CVE-2019-0541	8.4	
<p>Description: A remote code execution vulnerability exists in the way that the MSHTML engine improperly validates input, aka "MSHTML Engine Remote Code Execution Vulnerability." This affects Microsoft Office, Microsoft Office Word Viewer, Internet Explorer 9, Internet Explorer 11, Microsoft Excel Viewer, Internet Explorer 10, Office 365 ProPlus.</p> <p>Solution: N/A</p> <p>Important Links: National Vulnerability Database</p>						
Moderate	Microsoft Corporation	Internet Explorer	11.00.14393.2007	CVE-2019-0752	6.1	
Moderate	Microsoft Corporation	Microsoft® .NET Framework	4.6.1586.0	CVE-2019-0613	4.5	
Moderate	Microsoft Corporation	Microsoft® .NET Framework	3.5.30729.8763	CVE-2019-0613	4.5	
Moderate	Microsoft Corporation	Microsoft Teams	1.2.00.19260	CVE-2019-5922	4.4	
Moderate	Microsoft	Microsoft Teams	1.4.4.0	CVE-2019-5922	4.4	

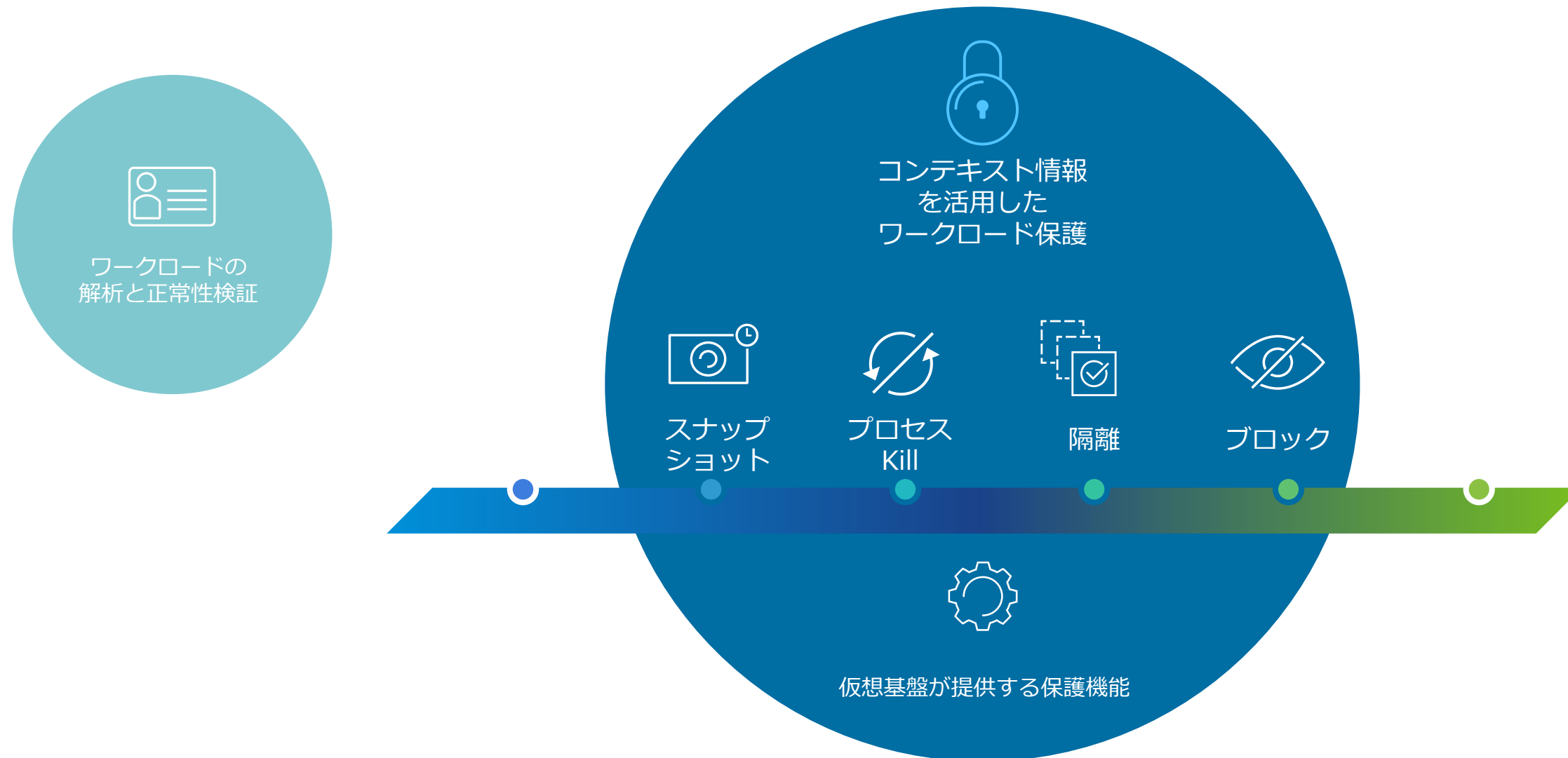
1-15 of 69 Vulnerabilities

ワークロードのコンテキスト情報を解析、より高度な可視性を提供

常にワークロードの状態と振る舞いを解析することでベースラインリファレンスを確立でき、そこから逸脱した不審な動きがあれば早期に確認/検知することが可能に

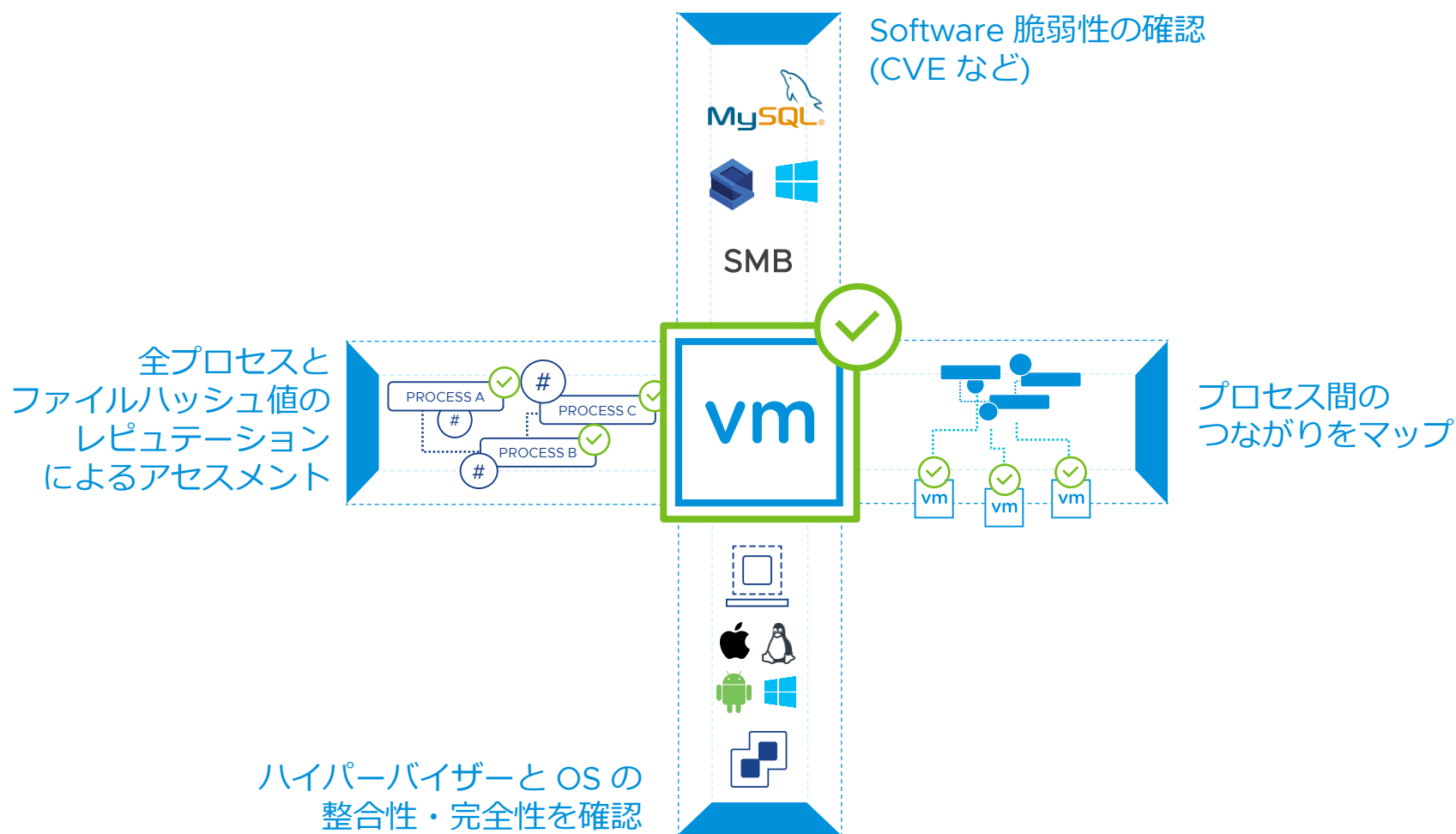


コンテキスト情報を活用したワークロード保護機能を提供 レスポンス



vSphereでワークロードのリアルタイム解析

脆弱性と完全性を可視化・対策を通した衛生管理の運用サイクルを実施



VMware vSphere® を活用したセキュリティ対策

エージェントソフトウェア不要

リアルタイムにワークロードの脆弱性有無と脆弱性リスクアセスメント

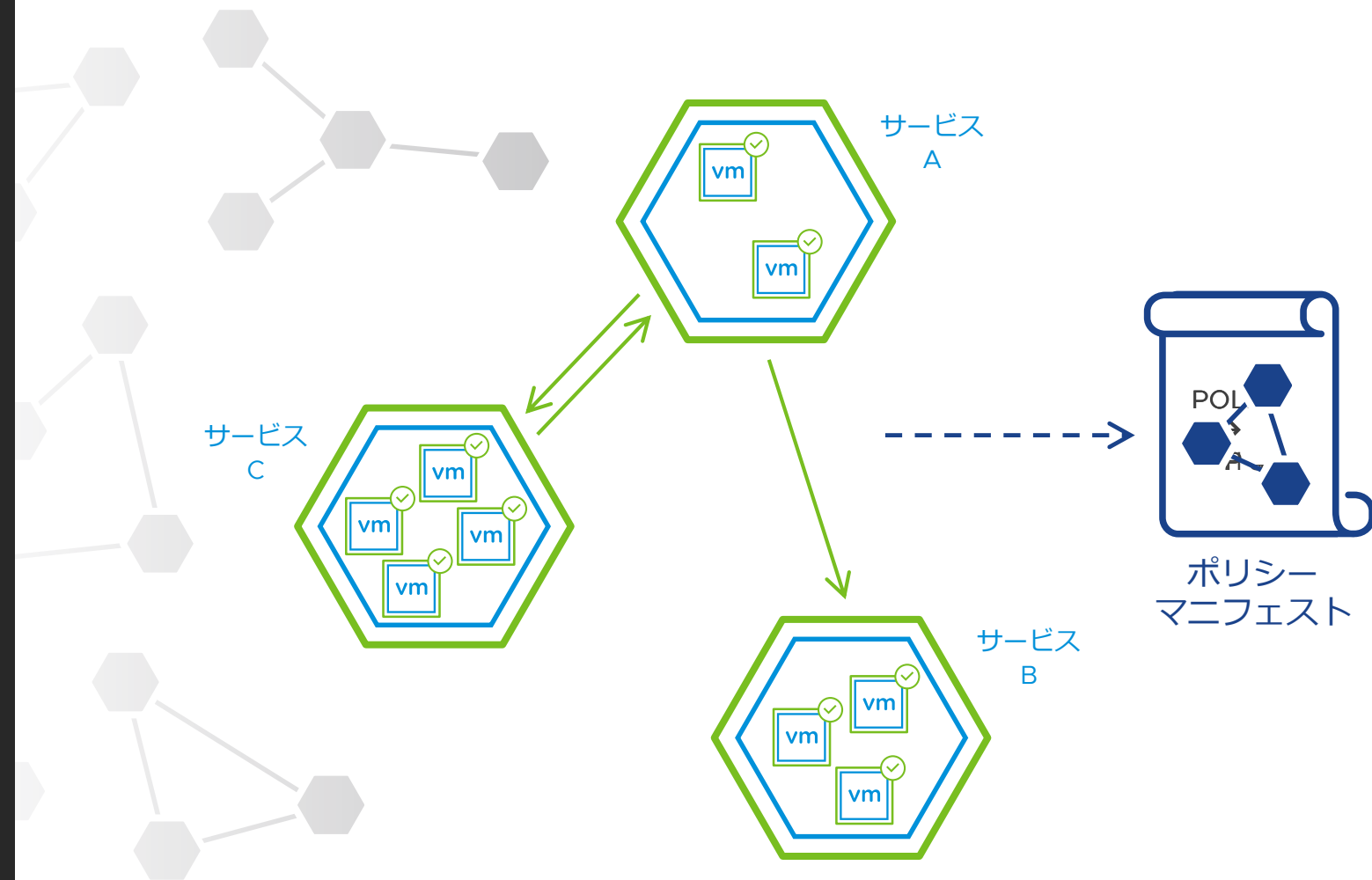
VM やコンテナのプロセスが生成する通信フロー情報を全て収集することでプロセスやファイル I/O からどのプロセスがどのポートでどのアプリケーションと通信しているかを追跡

どれとどれが連携しているのかといった通信状況を全て把握

脆弱性を突く攻撃による通信や内部での不審なコマンド実行なども確認/検知できる基盤へ

ネットワークで通信フローのリアルタイム解析

リアルタイムなアクセス制御で衛生管理の運用サイクルを実施



VMware NSX Intelligence

VM・コンテナにエージェントソフトを介さず、
刻々と変わるアプリケーションの状況や
ネットワークに流れるパケットを収集し
機械学習技術を用いて解析

↓
その場に適したホワイトリストを自動生成

定められた範囲内に動作を
封じ込められるように
より粒度の細かいマイセグを適用可能に

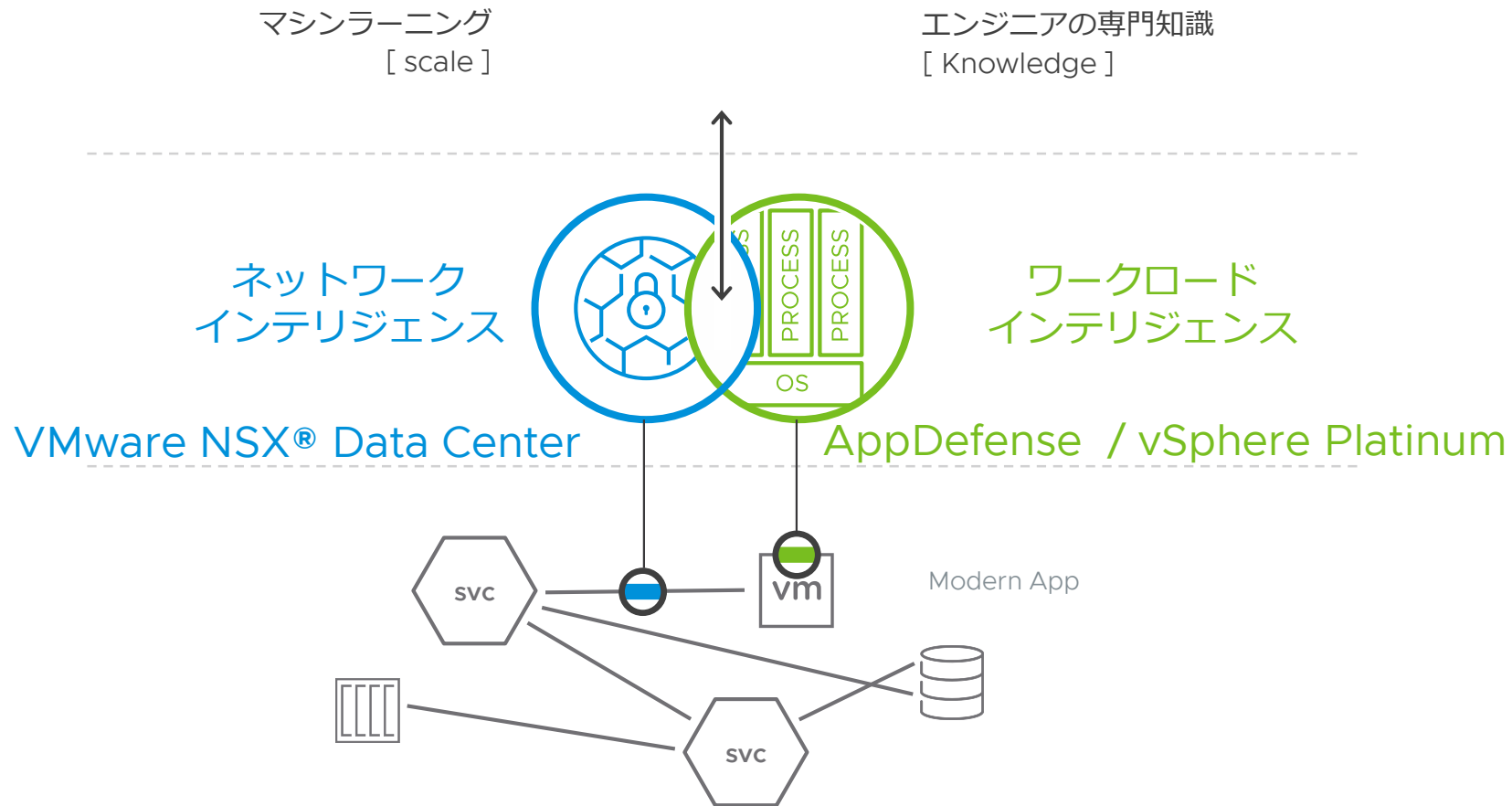
常にトラフィックを解析することで
ベースラインを確立
逸脱した**内部での不審な動き**があれば
異常を確認/検知することが可能

運用時の通信フロー全てに対して
信頼性を常に確認できる基盤へ

より高度な VMware ビルトインセキュリティの実現

ビルトイン技術による透過的なエージェントレスアプローチ

NSX INTELLIGENCE
CLOUD



ラーニング・可視化

アプリのコンピュートと
ネットワークレベルの
振る舞いを学習

エンフォース

仮想レイヤーから
アクセス制御を強制

アダプト

インフラとアプリの状況変
化にリアルタイムに追従

後追い（付け足し）ではなく、あらかじめ SDDC にビルトインされた形で実現することが重要

効果的なセキュリティ対策を 実現するための基本技術要素 まとめ

仮想化レイヤーを活用したセキュリティ対策

信頼性を確保、攻撃対象の側面を減らし、侵害を封じ込め

ワークロードとネットワークの可視化



何が展開されていて



何が稼働しているか

アプリケーションの設定内容や
システムコンポーネント間で
想定される相互処理を**常時確認**



©2019 VMware, Inc.

エージェントレス & 論理境界



アプリケーションやサービスの周りに
論理境界を設ける

自動化されたレスポンス



ワークロードの変更や不正行為の検知を
受けて、重要なデータやアプリケーション
へのアクセス制御を自動的に適用

VMware の考える仮想基盤セキュリティのまとめ

注目を集める前からゼロトラストと同様のアプローチを提唱してきた VMware SDDC の強み

パッチ適用



最小限の
権限



マイクロ
セグメン
テーション



多要素認証



暗号化



新たな IT 環境に合わせたセキュリティを実現する上で、
ゼロトラストというアプローチは不可欠

ホワイトリストによるワークロード制御 や **脆弱性可視化、整合性・完全性の担保** といった、
ネットワークとワークロードのホワイトリスト制御を活用することで
日常のシステムでの衛生管理 が可能な “無理のない” 運用へ

常に通信やワークロードを解析するということは「**正常時**」を**把握**でき、
仮に **そこから逸脱した “内部での不審な動き”** があれば早期に気が付ける基盤に

脆弱性を突く攻撃による通信や不審なコマンド実行などにも **気が付ける**
ゼロトラストのアプローチを **基盤に透過的に導入**することが可能

VMware Vision

The Essential, Ubiquitous Digital Foundation

Any Device



Any Application



Traditional

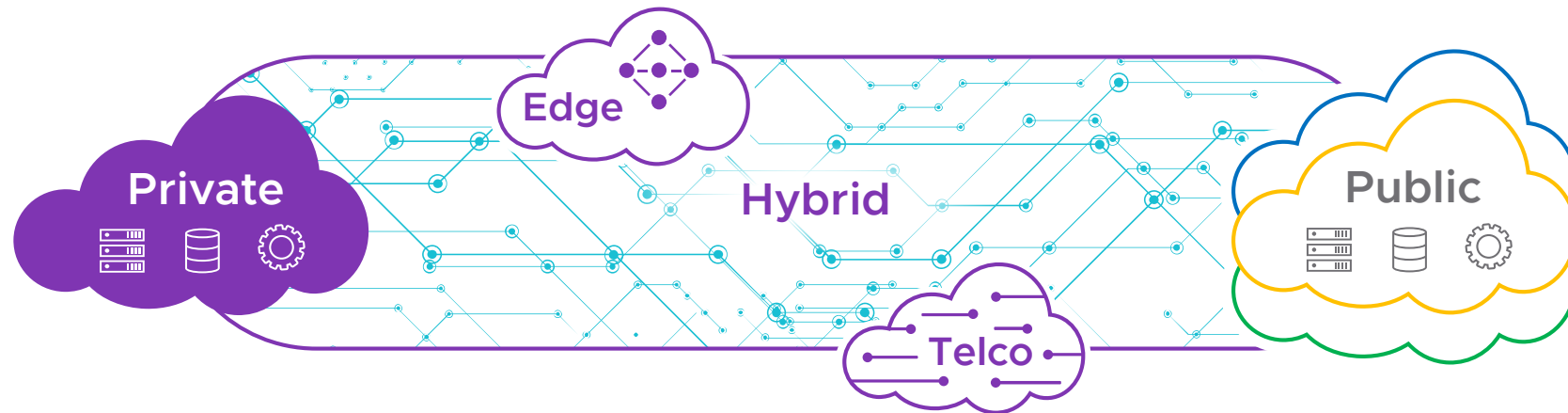


Cloud Native



SaaS

Any Cloud





Thank You