vFORUM 2019

NS412

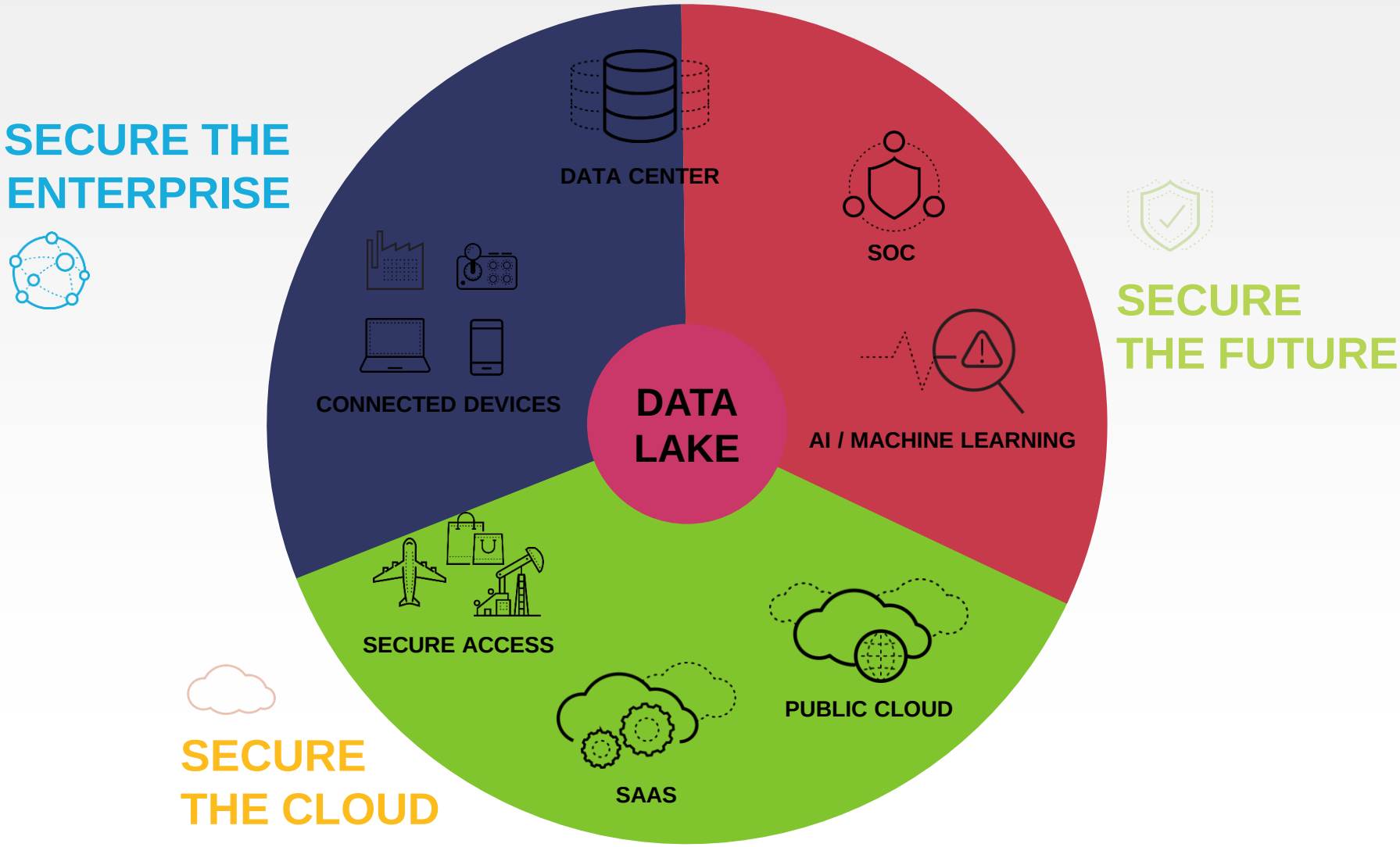
パロアルトネットワークスが貢献するゼロトラスト時代の真のサイバーセキュリティ対策

草川 秀人

パロアルトネットワークス株式会社
技術本部　コンサルティング　エンジニアリング
マネージャ

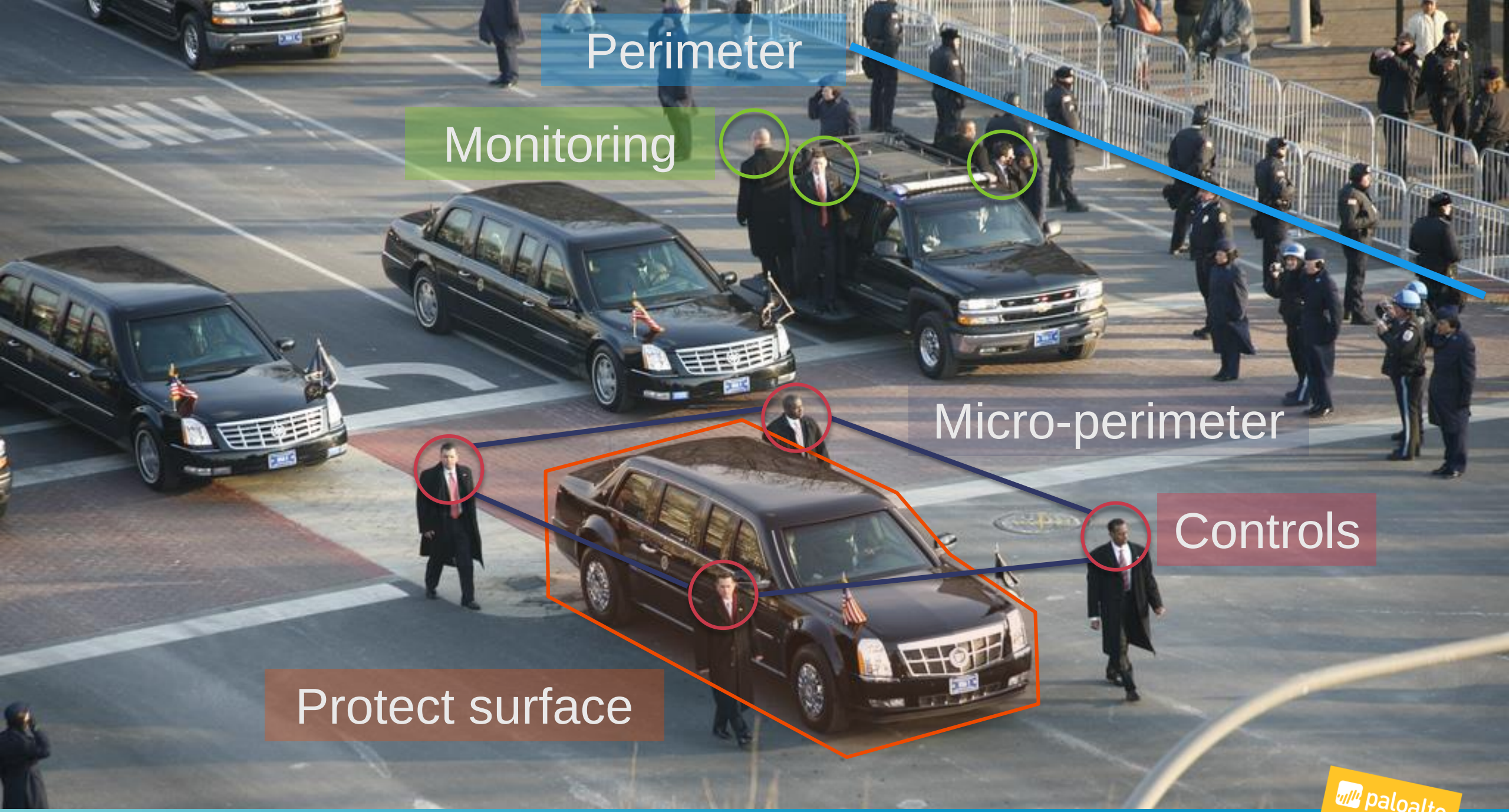
vmware

進化し続ける企業環境をよりセキュアに！

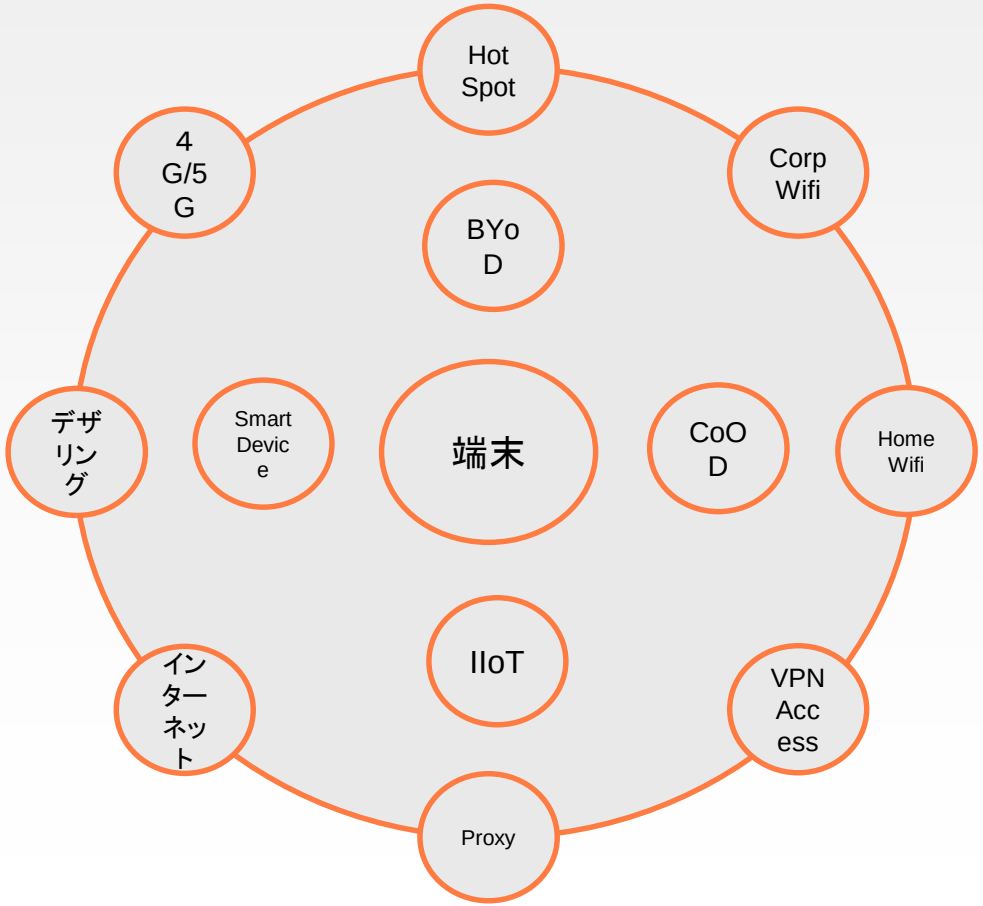


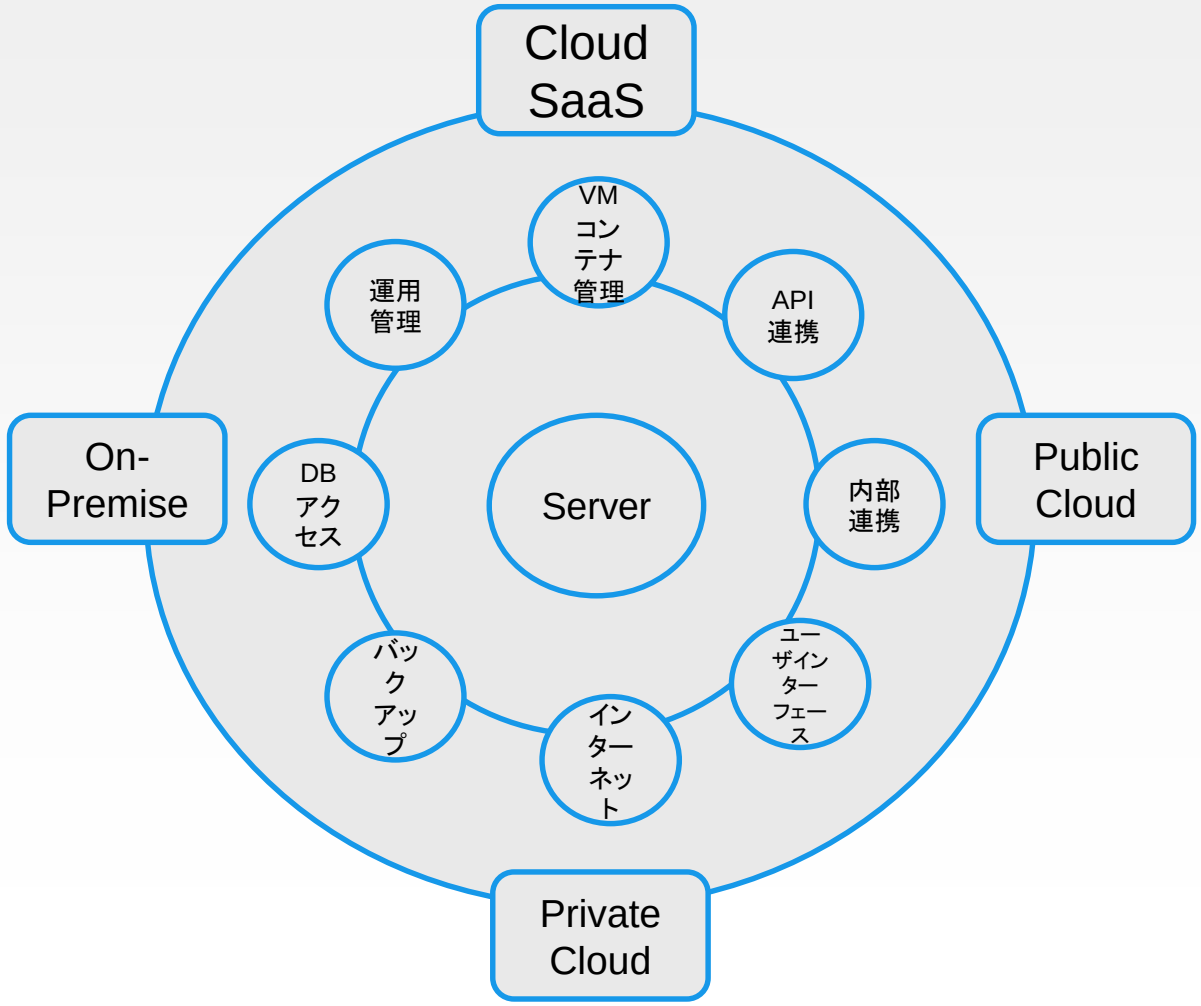
 |

ゼロトラストと企業ネットワークの取り巻く状況



端末とサーバ･システムの周辺要素は増える一方

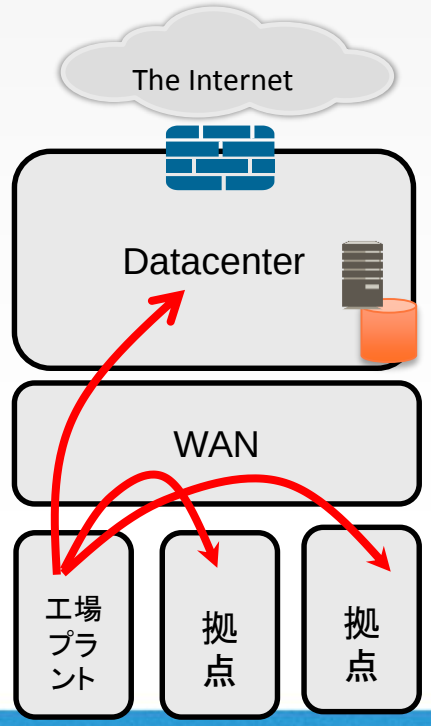




 |

拡散型マルウェア内部からの拡散

- 2017年5月12日（US時間）から世界的に感染被害が広がったランサムウェア。「EternalBlue」と呼ばれるMicrosoft WindowsのSMBプロトコルの脆弱性*CVE-2017-0144*を突いて、感染したエンドポイントから、ネットワーク上の他のシステムに感染を拡大する。



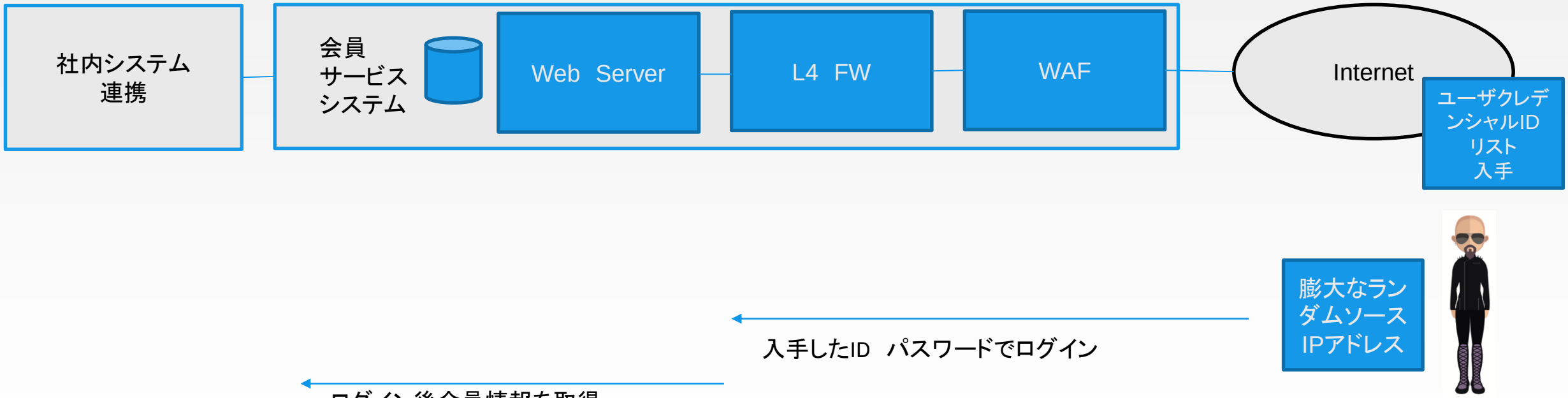
初期感染した端末が持ち込まれた拠点より拡散開始、内部向けに無防備であったサーバ、WANを超え別拠点内にも感染が拡大

業務の停止に追い込まれる

 |

標的攻撃例

- IDパスワードリストの攻撃の傾向



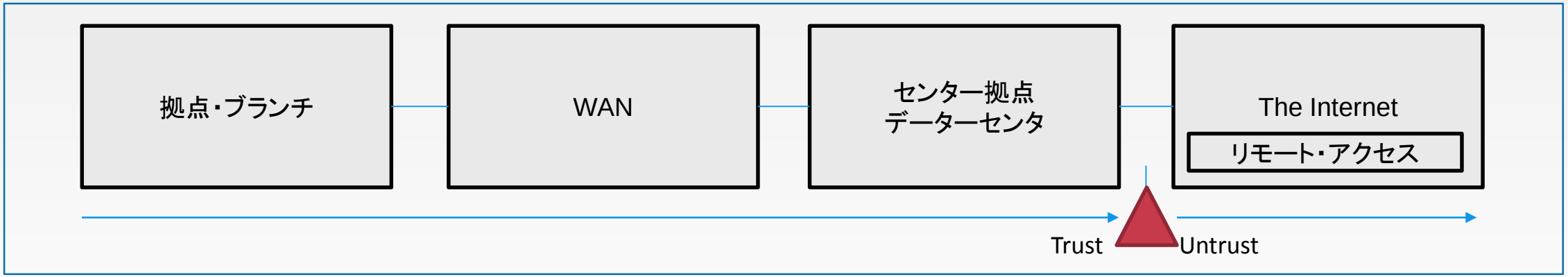
 |

MITRE ATT&CK™ にて紹介されるテクニック

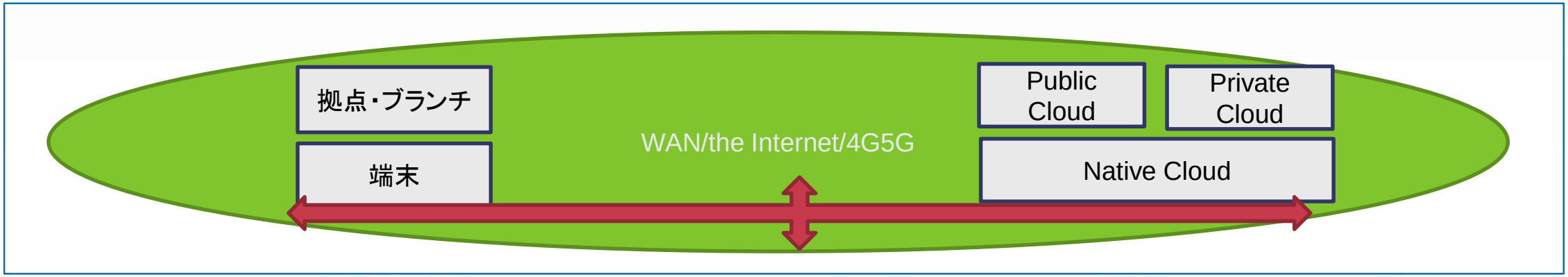
- MITRE ATT&CK™
  - Enterprise(244)
  - Mobile(67)
  - Pre-ATT&CK(174)
- Enterprise TechniquesはPost Exploitにターゲットを置いたフレームワーク
- Initial Access、Execution、Persistence、Privilege Escalation、Defense Evasion、Credential Access、Discovery、Lateral Movement、Collection、Command and Control、Exfiltration、Impact

全方位型のベクトル

- ゼロトラスト・内部セグメンテーション



境界でのセキュリティ対応から全方位 ゼロトラストモデルへ変遷



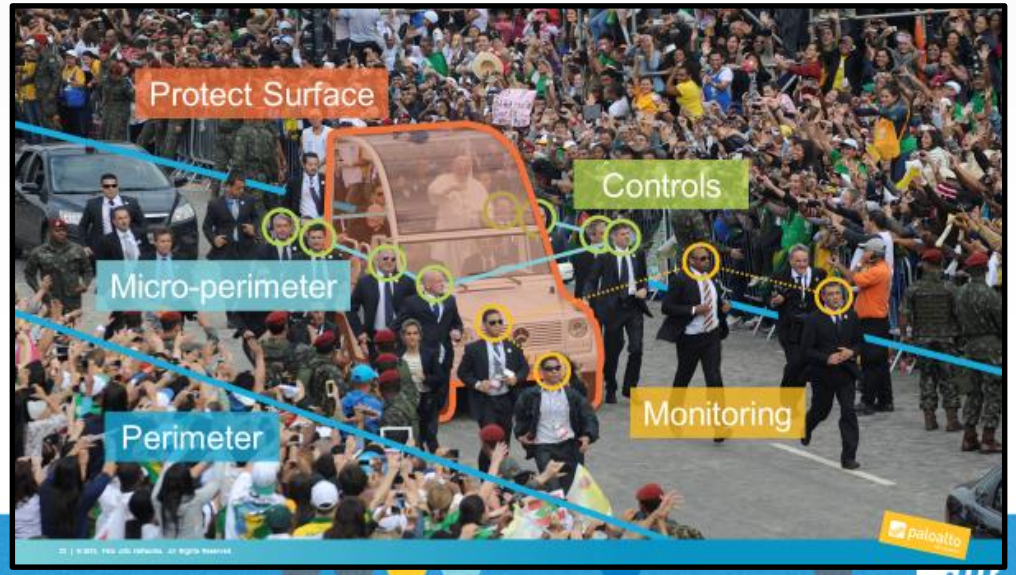
 |

ゼロトラストコンセプトから　セグメンテーション守るべきベクトルを抽出

1. プロテクトサーフェースとマイクロペリメーター＆コア
   - データセンター・クラウドコンピューティング環境、DevOpsからDevSecOpsへ
     - 仮想化、マイクロセグメンテーション、コンテナセキュリティ
     - N-S（クライアントサーバ間）
     - E-W（サーバ、サーバ間、システム、システム間）

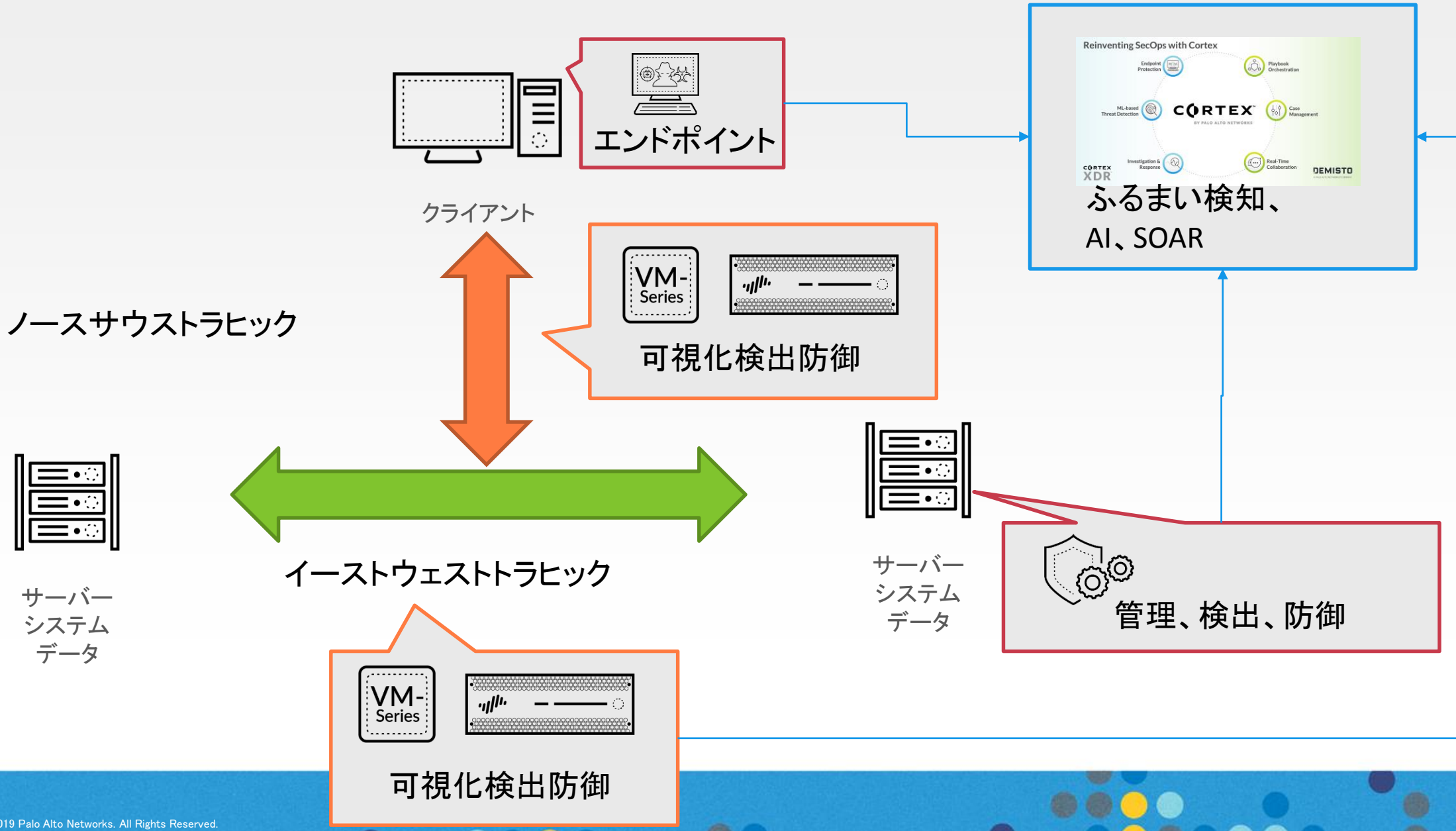
2. セグメンテーション
   - 認証情報の連携
   - ネットワークセグメンテーションとの連携
   - ファブリックマイクロセグメンテーションとの連携
   - アセット管理システムとの連携

3. ペリメータエクステンション
   - 企業WANからSD-WAN、クラウドへ



データセンタ仮想化のゼロトラスト対応

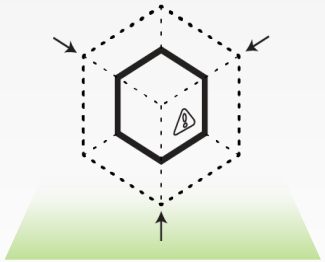
ノースサウスと イーストウェスト トラフィック



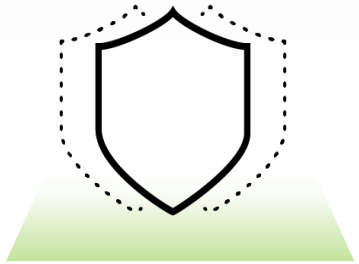
 |

パロアルトネットワークスで実現するセキュリティ機能

高次元な
可視化



多層
セグメンテーション



自動化された
脅威防御

URL Filter

Threat Prevention

Anti-Malware/Spyware

Segmentation Gateway
NGFW

DNS Security

SSL Decryption

Wildfire

Zero Trust

Workload Protection

Workload

Hypervisor

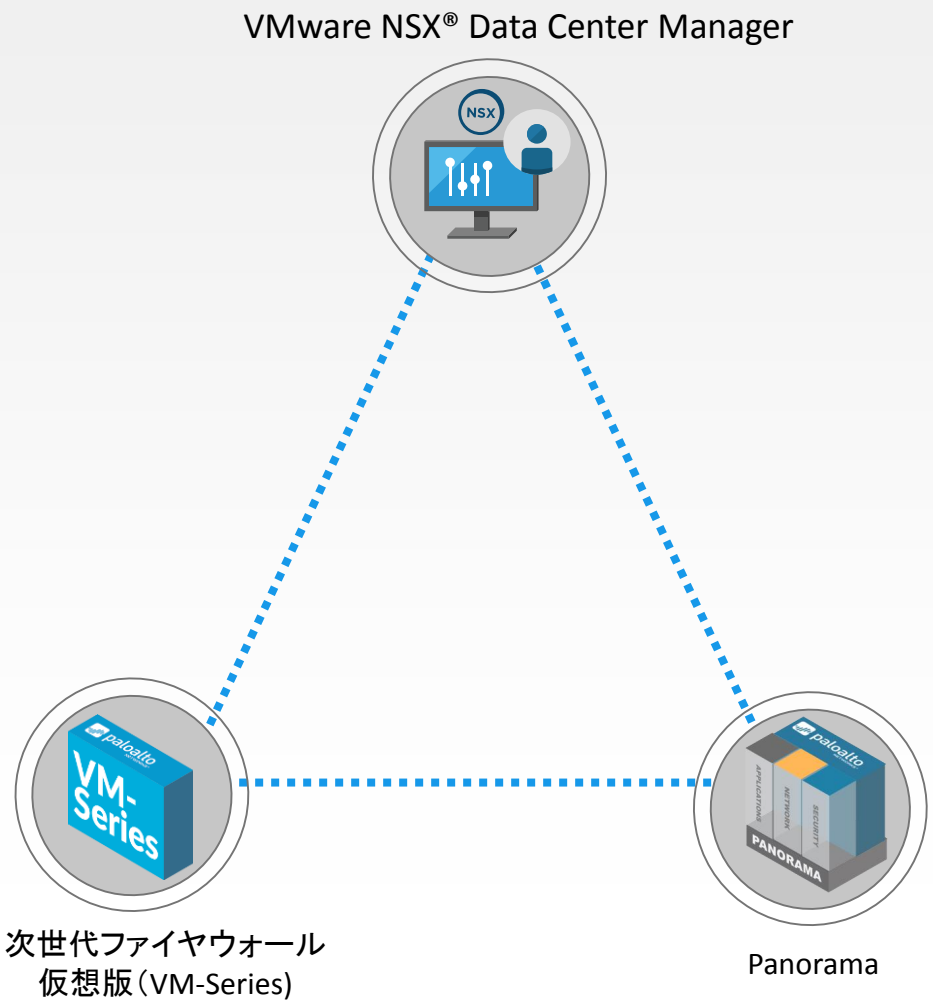
VSG

vSwitch

Switch

 |

パロアルトネットワークスで実現するVMware NSX® Data Center連携



セキュリテイサービス挿入の自動化

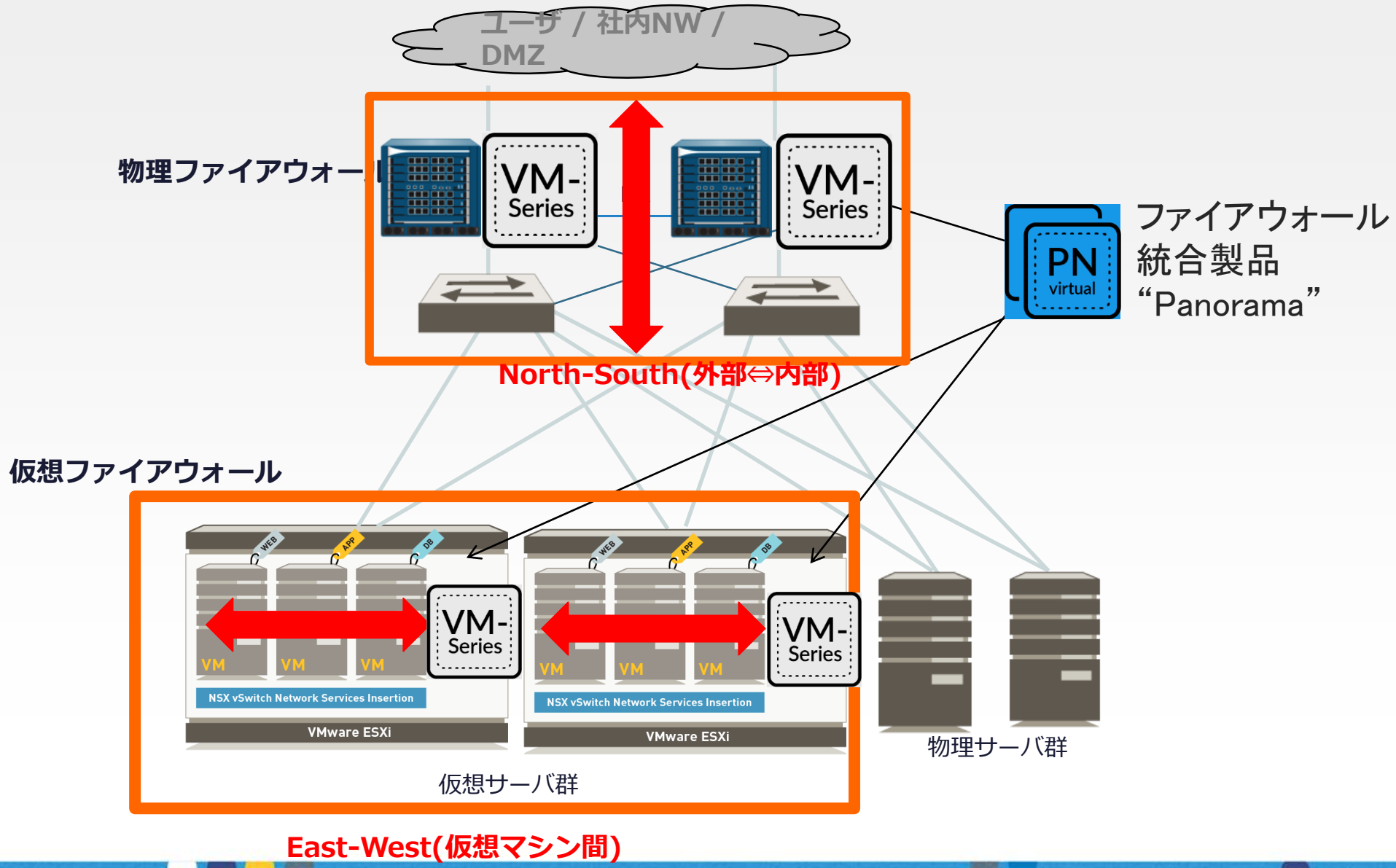
ダイナミックにセキュリティグループ・ポリシーを適応＊

アプリケーションのマイクロセグメンテーション化

脅威からデータとアプリーションの防御

＊NSX-Vインテグレーションにてサポート

トラフィックの可視化と防御と既存NGFWとの連携

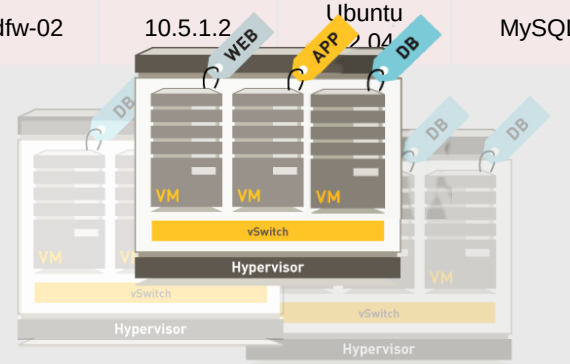


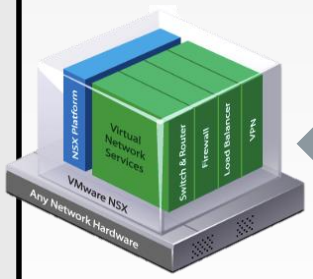
 |

ダイナミックにアドレス変更を追随するセキュリティーポリシー

VMware VMware vCenter® または VMware ESXi™

Name	IP	Guest OS	Container
web-sjc-01	10.1.1.2	Ubuntu 12.04	Web
sp-sjc-04	10.1.5.4	Win 2008 R2	SharePoint
web-sjc-02	10.1.1.3	Ubuntu 12.04	Web
exch-mia-03	10.4.2.2	Win 2008 R2	Exchange
exch-dfw-03	10.4.2.3	Win 2008 R2	Exchange
sp-mia-07	10.1.5.8	Win 2008 R2	SharePoint
db-mia-01	10.5.1.5 -> 10.5.1.19	Ubuntu 12.04	MySQL
db-dfw-02	10.5.1.2	Ubuntu 12.04	MySQL





自動連携

ホストのアドレスが変わっても、変更がダイナミックグループに反映され、継続じて同じセキュリティポリシーが適用される

PAN-OS ダイナミックアドレスグループ

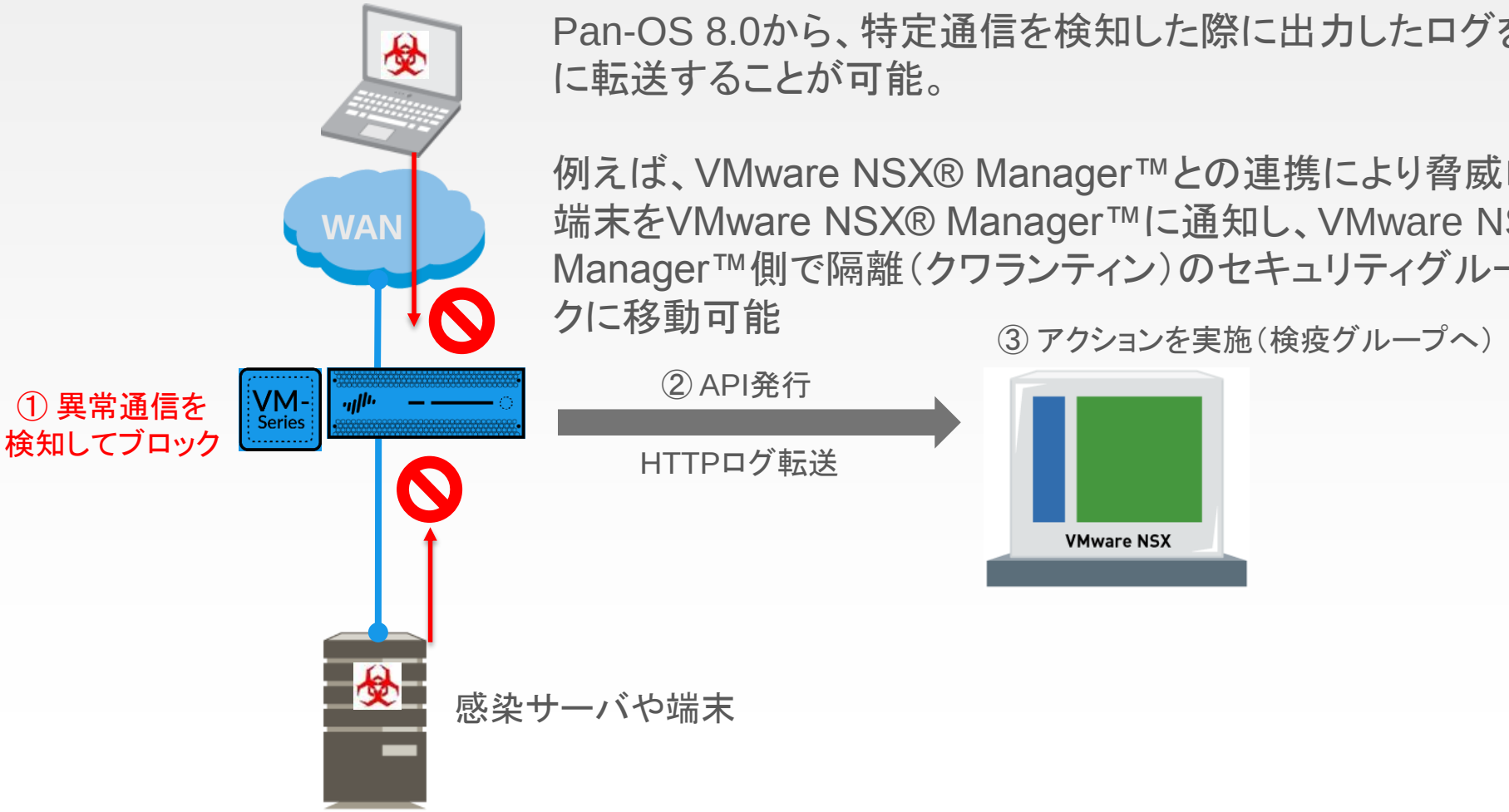
Name	Tags	Addresses
SharePoint Servers	SharePoint Win 2008 R2 “sp”	10.1.5.4 10.1.5.8
MySQL Servers	MySQL Ubuntu 12.04 “db”	~~10.5.1.5~~ 10.5.1.2 10.5.1.9
Miami DC	“mia”	10.4.2.2 10.1.5.8 10.5.1.5
San Jose Linux Web Servers	“sjc” “web” Ubuntu 12.04	10.1.1.2 10.1.1.3

PAN-OS セキュリティポリシー

Source	Destination	Action
San Jose Linux Web Servers	SharePoint Servers	✔
MySQL Servers	Miami DC	⃠

＊NSX-Vインテグレーションにてサポート

脅威の検出とサーバ、端末の隔離の自動化



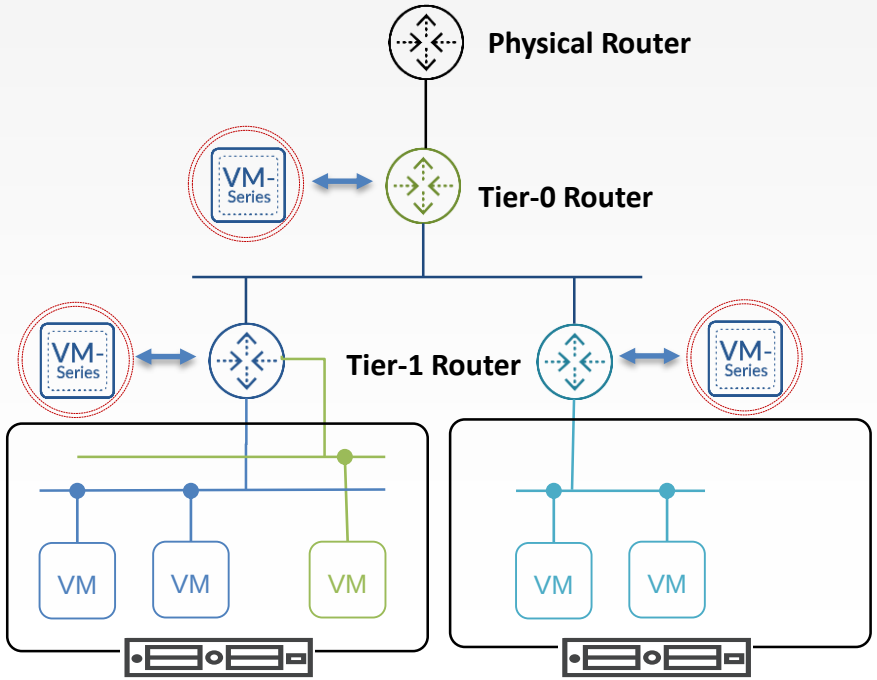
Pan-OS 8.0から、特定通信を検知した際に出力したログを、HTTPで外部に転送することが可能。

例えば、VMware NSX® Manager™との連携により脅威ログを検出した端末をVMware NSX® Manager™に通知し、VMware NSX® Manager™側で隔離（クワランティン）のセキュリティグループにダイナミックに移動可能

＊NSX-Vインテグレーションにてサポート

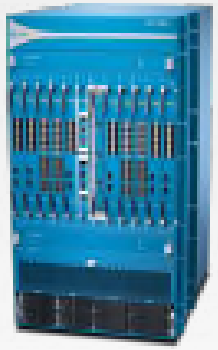
NSX-T North-South Service Insertion with VM-Series

NSX-T	PAN-OS	Panorama	NSX Plugin
2.4.0+	9.0.3+	9.0.3+	3.0.0



Benefits
Zero-Touch Provisioning • Automate the firewall deployment (with/without HA) • Auto connect to Panorama • Auto install the licenses
Protect the perimeter (Tier-0)
Protect the tenants (Tier-1)
Secure Kubernetes Namespaces
Secure “org” of Pivotal Application Services

パロアルトネットワークス　データセンターサーバー環境向け
次世代ファイヤーウォール



PA-7080

630 Gbps

PA-7050

380 Gbps

PA-52xx

68 Gbps

VM-50
VM-50 Lite

200 Mbps

VM-100

2 Gbps

VM-300/
VM-1000-HV

4 Gbps

VM-500

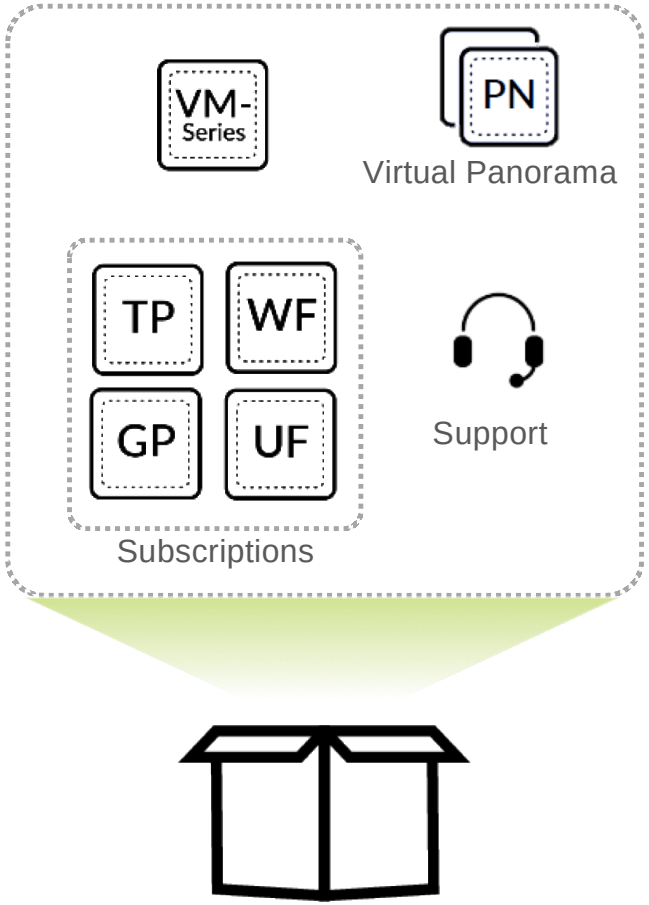
10 Gbps

VM-700

18 Gbps

 |

VM-ELA(Enterprise License Agreement)



- 契約期間：1年間および3年間のオプション
- 期限内に調整なしで無制限利用が可能
  - 3年契約の場合は、契約前半（折り返し）までは150%の成長上限（CAP)有り
- サポートされているすべての環境（プライベートクラウドとパブリッククラウド）で利用可能
- 複数のVM-Seriesモデルが含まれます
  （VM-50, VM-100, VM-300, VM-500, VM-700）
- ELA適用するための要件
- 無制限の仮想版Panoramaの利用
- 複数のカスタマーサービスポータル（CSP）アカウントに紐付け可能

エンタープライズクラスのセキュリティをマルチクラウド環境にシンプルに提供

ありがとうございます。