VMware の IT チームによるゼロトラストの実践

弊社におけるゼロトラスト実現に向けた取組事例

Craig Savage

VMware, Inc

Information Security Strategy Director

クレイグ・サヴェージの紹介

VMware 情報セキュリティ戦略担当ディレクター

CISSP（認定情報システム セキュリティ プロフェッショナル）、
ISSMP（情報セキュリティ システム管理プロフェッショナル）

- 主な担当業務：
  情報セキュリティ関連の働きかけとコミュニケーション
- 経験豊かなトランスフォーメーション コンサルタント
- セキュリティの簡素化を提唱

免責事項

- 本セッションには、現在開発中の製品/サービスの特長または機能を含む、VMware Inc. の秘密情報と専有情報が含まれています。
- これは、内部使用のみを目的として参加者に提供されているものです。
- 本セッションで紹介する新しいテクノロジーについて、VMware が製品/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、発注書/注文書、または販売契約書にも規定されないものとします。
- 技術的な問題と市場の需要により、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。
- ここで言及および提示されている新しいテクノロジーまたは機能の価格とパッケージは、決定されたものではありません。
- 参加者は、この資料を、その一部か全体かにかかわらず、だれとも共有しないものとします。ただし、ほかのあらゆる目的について拘束性のある機密保持契約を締結済みである参加者所属企業の従業員との間を除きます。
- 資料で紹介されている第三者の商標（ロゴとアイコンを含む）はすべて、引き続きそれぞれの権利者に帰属する財産として存続します。

アジェンダ

01 VMware IT

02 ゼロトラストについて

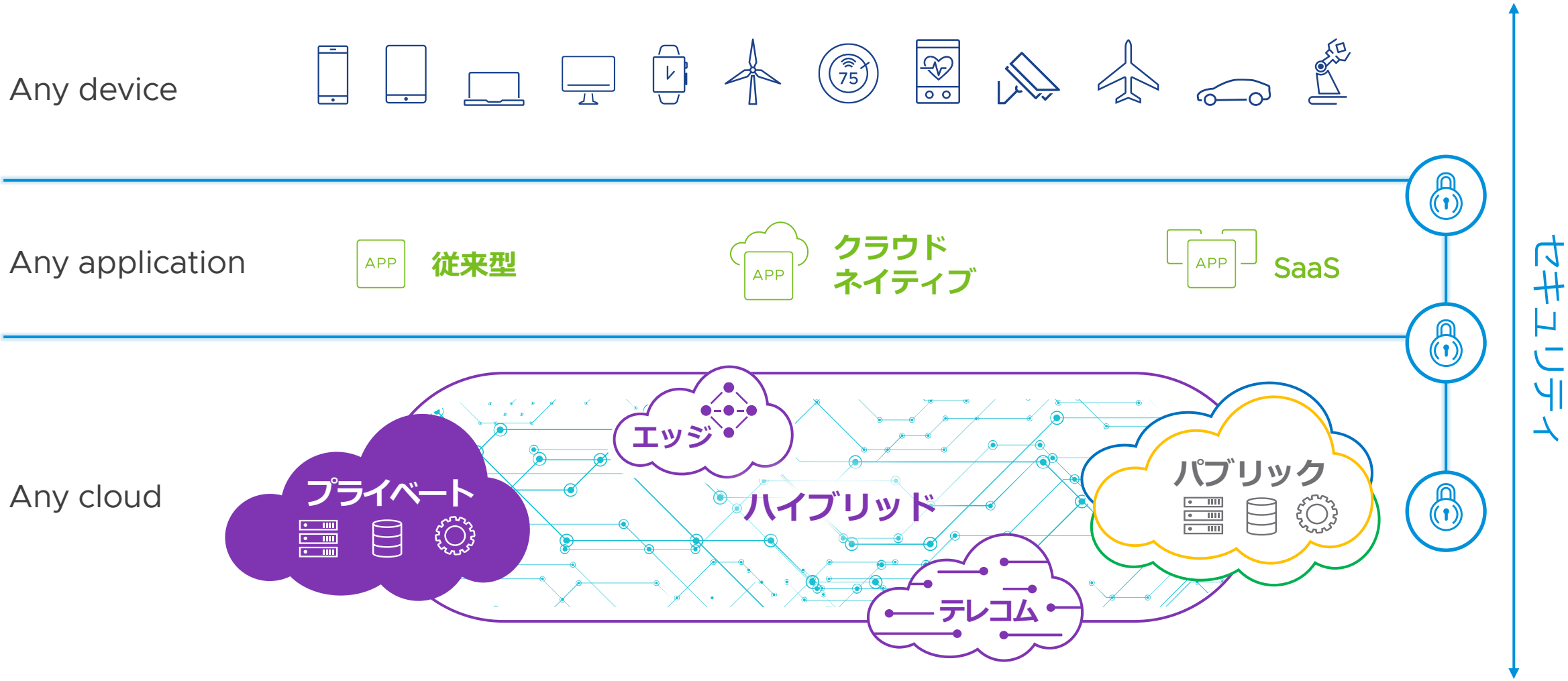
03 環境の保護

04 まとめ

05 Ask the Speaker (セッション終了後)

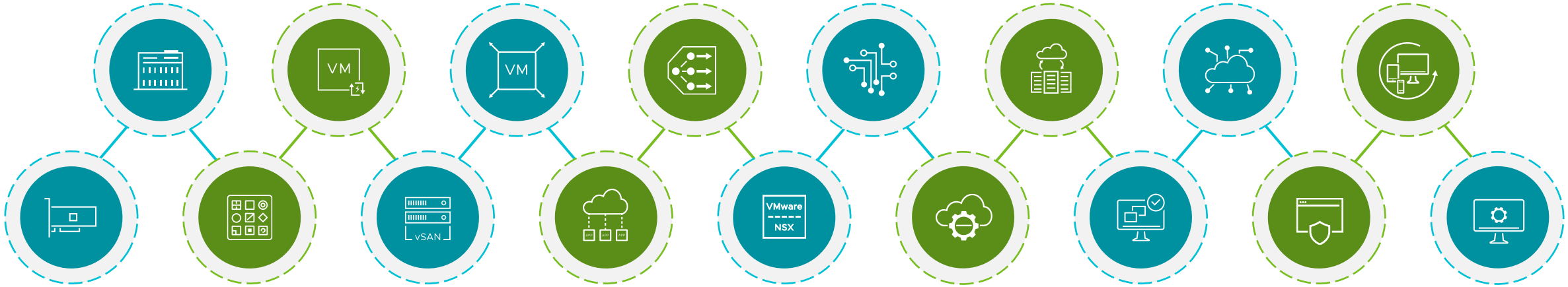
VMware が提供するデジタル基盤

あらゆるアプリケーションのビルド（構築）、実行、管理、接続、保護をあらゆるクラウド、あらゆるデバイスで実現



VMware 本番環境の概要：2022年5月時点

CIO、VES、情報セキュリティ チームによるマネージド環境

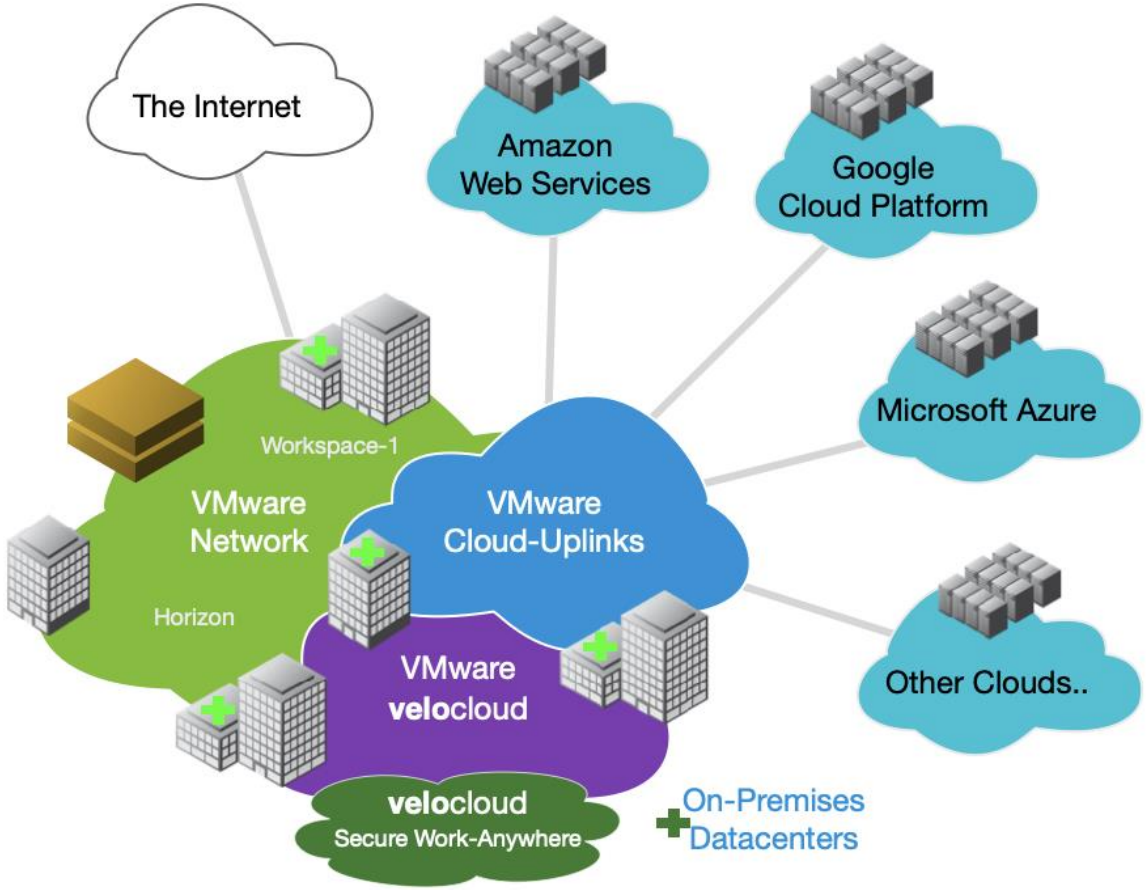


*DC:データセンター、WFH: Work from Home(テレワーク)

ネットワークの概要

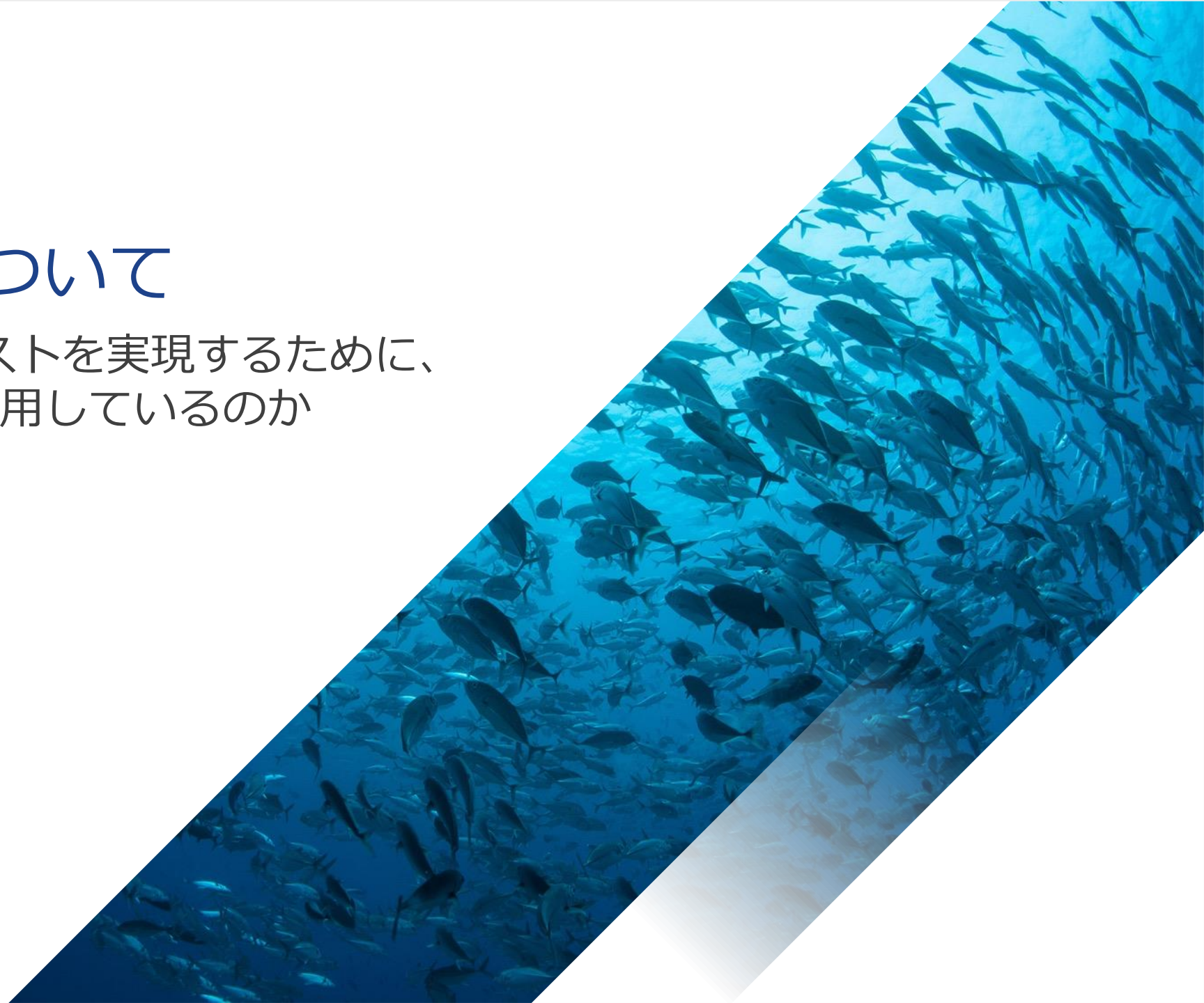
VMware のネットワークはハイブリッドクラウド（クラウドとオンプレミスのリソースを融合させたもの）である

- クラウドホスト型のデータセンターが従来型のオンプレミス データセンターと統合されている
- VMware のネットワークではマイクロセグメンテーションが必須。コード、製品ロードマップ、その他の知的財産は分離して管理する必要がある
- 2 要素認証、証明書、シングル サインオン（SSO）が必須。パスワードを唯一の認証手段にすることはできない
- VMware Horizon リモート デスクトップはリモート アクセスとパートナーからのアクセス用に提供



ゼロトラストについて

VMware IT がゼロトラストを実現するために、
自社製品をどのように利用しているのか



ゼロトラストの基礎となる基本的なサイバー ハイジーン

効果的なゼロトラストを実現するための基盤と 5 つの柱

暗号化

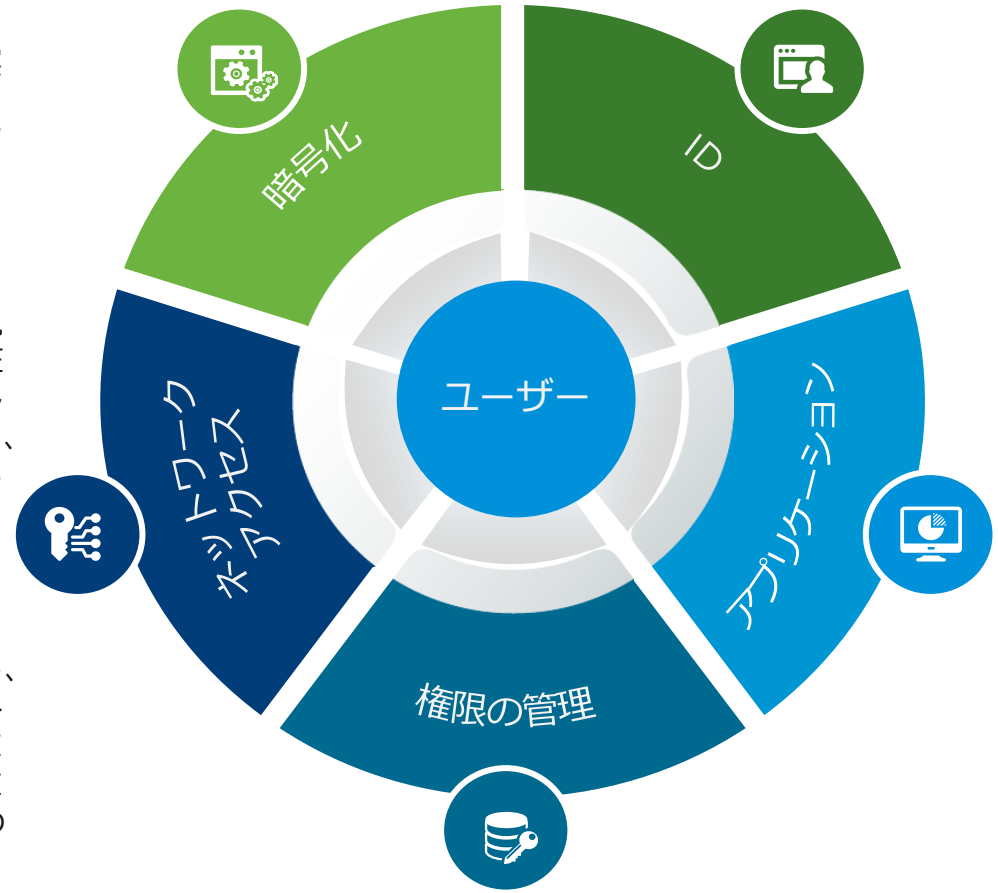
すべてのデバイスとデータ トラフックを確実に暗号化することで、デバイスを紛失したりネットワークに侵入されたりした場合のデータ侵害のリスクを低減できる

エンドユーザー

ゼロトラスト モデルへの効果的な移行を実現するには、ユーザーを理解し、ユーザーが現在どのような作業をしてなにを達成しようとしているかを把握する必要がある。そのために、先入観を持たず、多様なメンバーで構成されるチームを結成してこの問題に取り組む

ネットワーク アクセス

使用するネットワークの種類（イーサネット、Wi-Fi、VPN）にかかわらず、コア ネットワークに接続しなくても作業ができるようにする。コア ネットワークは重要なサービスにのみ使用し、その他のアクティビティは、他の領域で行う



ID

ユーザーの「認証」と「認可」の両方を正確に行えること。適切なユーザーが想定された活動をしていることを確認し、必要に応じて再確認できる機能が不可欠である

アプリケーション

企業向けアプリケーションやサービスを利用しやすくし、既知の不正なアプリケーションを阻止し、新しいアプリケーションやアップデートを簡単に展開できるようにする

権限の管理

エンドポイントへの特権資格情報の配置を許可しないこと。API の使用を推奨し、それができない場合は VDI アクセスを提供する。この 2 つの対策によって、有害なエラーの発生リスクを抑制し、悪意のある活動を制限できる

セキュリティとソリューションに関する VMware のビジョン

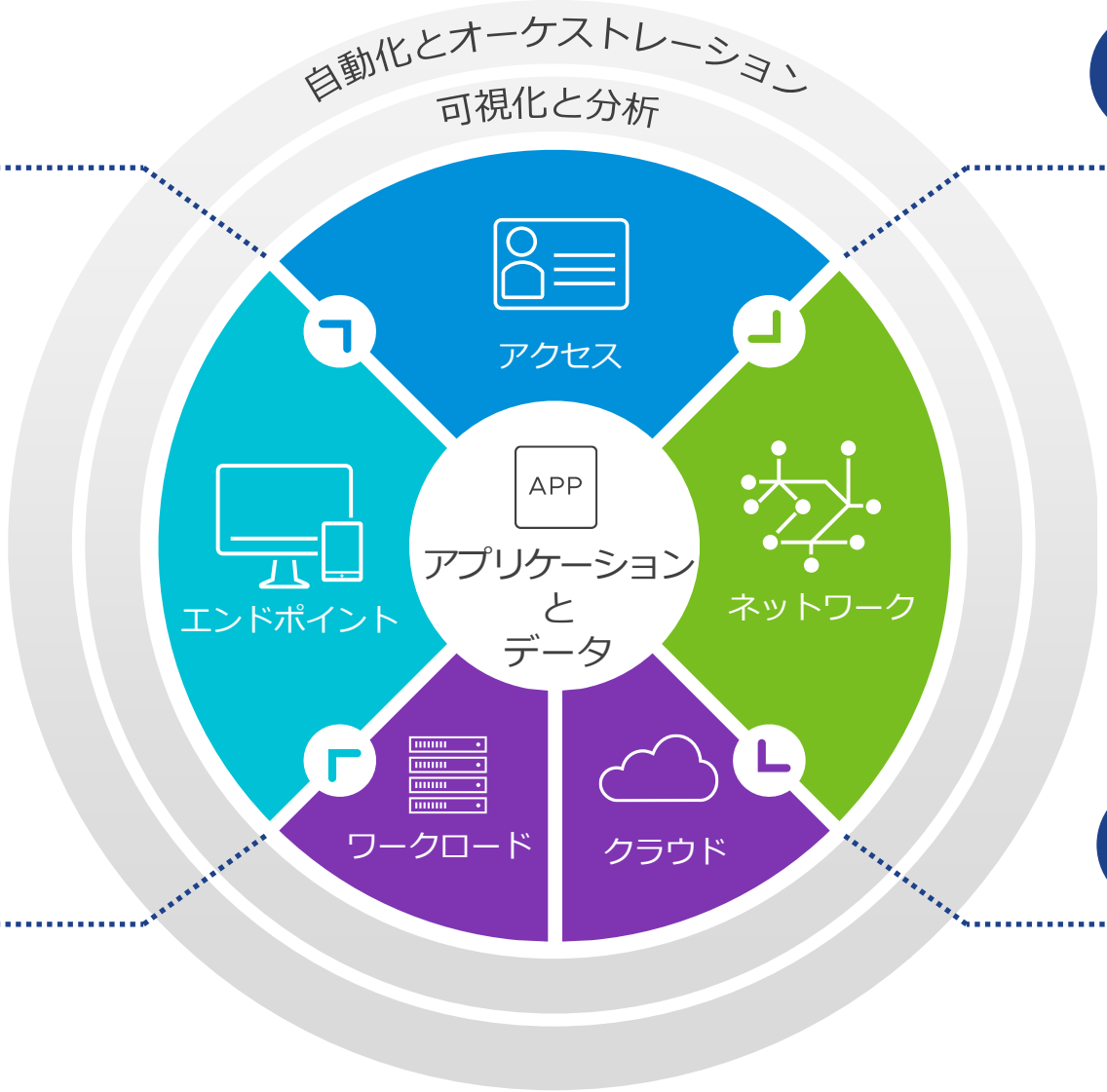
重要なアプリケーションとデータの保護

エンドユーザー サービス チーム

- デバイス/ユーザーの状態の管理
- アクセスの管理

ネットワーク チーム

- マイクロセグメンテーション
- ネットワーク アクセス
- ネットワーク保護



情報セキュリティ チーム

- リスクの特定/保護強化
- 防御
- 検知/対応

クラウド運用チーム

- セキュアなクラウド インフラストラクチャの構成

環境の保護

従業員を守り、アプリケーションやデータを
保護する

エンドポイント セキュリティ

デバイスの信頼	ユーザーの信頼	データの信頼	アプリケーションの信頼
• パッチ管理 • コンプライアンス状態 • AD ドメインレス運用 • EDR と マルウェア対策 • エンドポイント ファイアウォール	• 証明書ベースの認証 • 多要素認証(MFA) • 条件に基づいた アクセスと 最小権限アクセス	• ディスク全体の暗号化 • 情報漏洩防止対策 (DLP) • デフォルトでネット ワーク接続を暗号化	• シングル サインオン • マイクロセグメンテー ション • エンタープライズ アプリケーション管理 • 仮想デスクトップ インフラストラクチャ • アプリケーション 固有のトンネル

VMware Workspace ONE
VMware Carbon Black
ディスク全体の暗号化
情報漏洩防止対策

可視化と分析（SIEM、Log Insight）

自動化とオーケストレーション（SOAR）

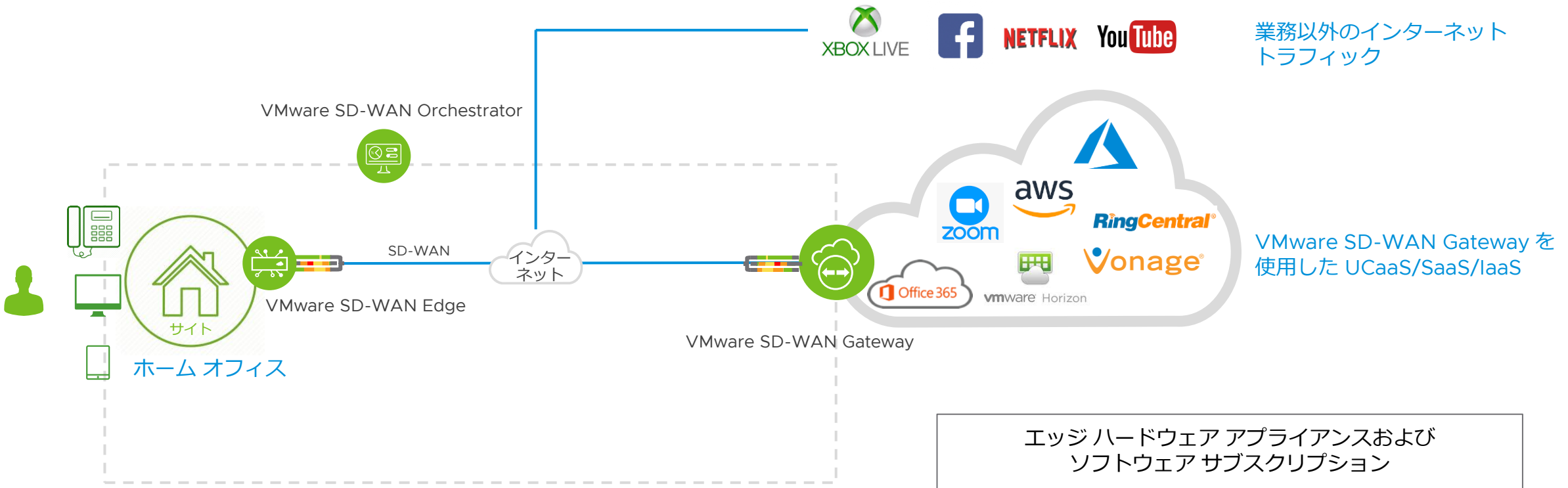
VMware IT による SD-WAN の活用

VMware SD-WAN を利用した従業員の業務環境の改善

信頼性の高い VOIP、UC、
コラボレーション、SaaS アクセス

ラスト ワンマイルの最適化による
従業員の業務環境の改善

接続の切断/不安定化の対策



エッジ ハードウェア アプライアンスおよび
ソフトウェア サブスクリプション

VMware IT による管理とサポート

VMware IT：Carbon Black がもたらした成果（2022 年 4 月）

アラート

セキュリティの強化

34,724 件のイベントを CB によって分析

- 26,039 のポリシーを適用
- 8,685 件の注意が必要な異常を検知

改善率

運用の俊敏性

着実な改善：バイパス ルールを最大 35% 削減

より厳格にルールを適用

- 48% Windows
- 15% macOS

保護の範囲

保護したシステムの数

18,051：Windows Server

22,650：Windows デスクトップ

3,856：VDI（Win OS）

22,796：macOS

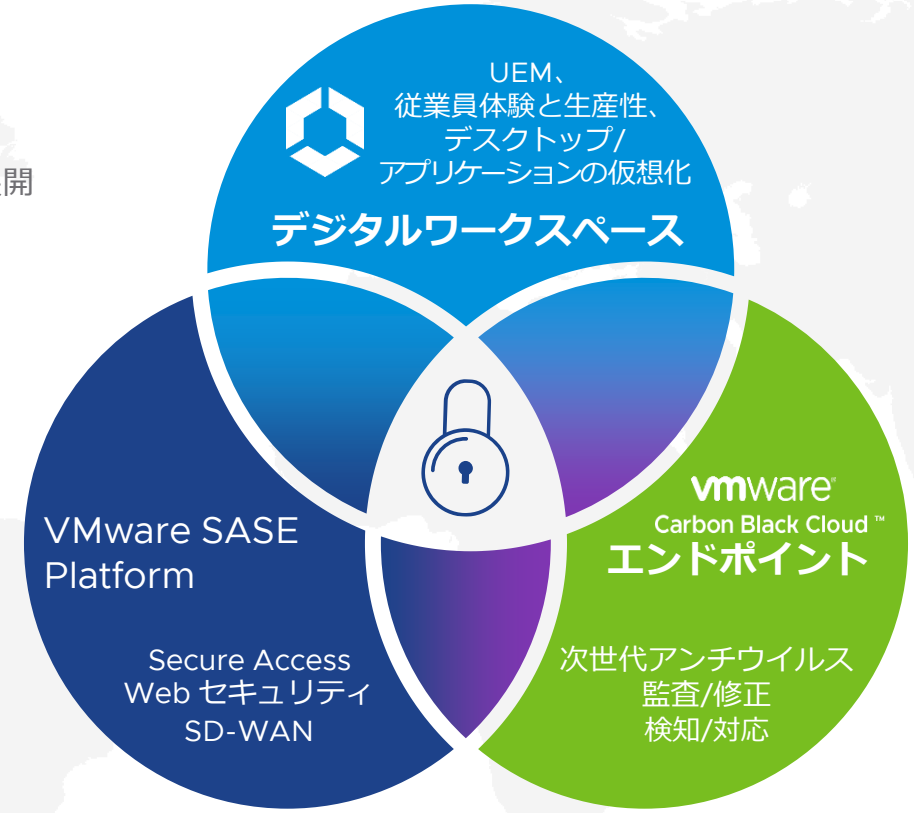
4,601：Linux

従業員の保護

デジタルワークスペース
- デバイスの健全性確認
- VPN に依存せず VDI とFAT PC を活用
- 集約、管理された企業アプリケーション展開
- エンドユーザー デバイスのパッチ管理

Secure Access
- 迅速なオンボーディング
- Workspace ONE
  - 暗号化/ファイアウォール管理
  - CB Cloud の導入
  - OS のパッチ管理
  - 条件に基づいたアクセス

SD-WAN
- 1,000 名を超えるテレワーカーの業務環境の改善
- テレワーカーの業務環境に関する、1000 を超える改善点



Carbon Black Cloud Endpoint Advanced
- 次世代アンチウイルス（防御）
- Live Query/Live Response（即座に端末全体にクエリを行って検出された問題を修正）

Carbon Black Cloud Enterprise EDR
- 検知、対応、脅威ハンティング
- 包括的で詳細なテレメトリ

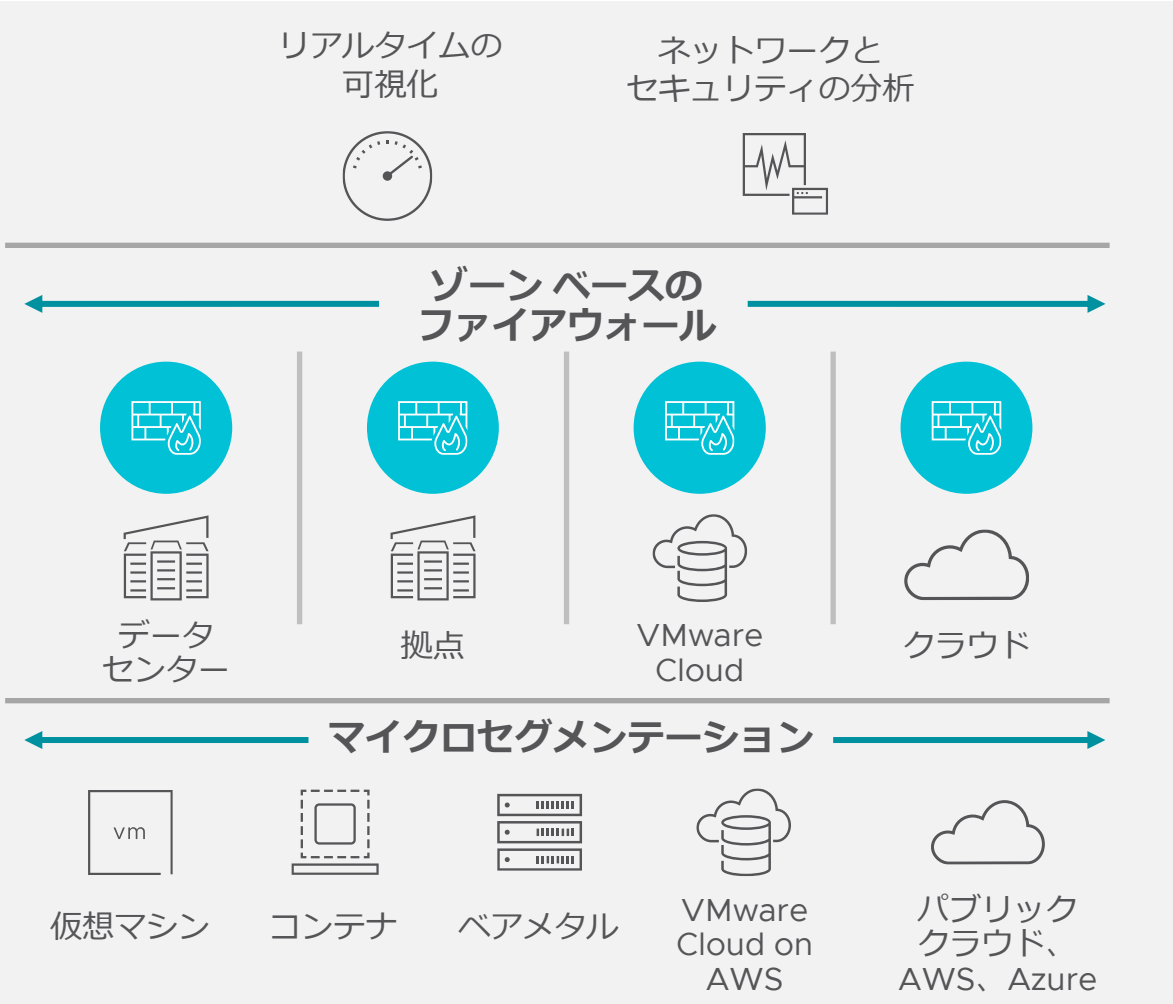
Carbon Black Cloud でのデバイス管理
- USB 書き込み保護
- USB 許可デバイス管理

NSX のセキュリティ

ネットワーク レベルでの知的財産に対するアクセスの制御

主なポイント

- ネットワークのマイクロセグメンテーションによるメリット：
  - 双方向のデータ フローの制御により、知的財産へのアクセスを制限
  - マルウェア伝播の可能性の低減
  - 社内のデータ フローの可視化により、機密データを常にあるべき場所に保管
- マイクロセグメンテーションにより、最新の管理機能に対応できないレガシー環境もサポート
- ログはすべてアグリゲータを通じて中央のセキュリティ情報イベント管理（SIEM）ソリューションに返送される



VMware IT によるゼロトラストの導入

第 1 段階

- VDI のセグメンテーション
- VDI のマイクロセグメンテーション
- 100 以上のアプリの
  マイクロセグメンテーション
- 境界内境界の設置

第 2 段階

- East-West トラフィックに対する
  ワンクリックの IDS/IPS デプロイ
- Network Detection and Response
  のデプロイ

今後追加が予定されている機能

- ID ベースの内部ファイアウォール
- タップレスでのネットワーク
  トラフィック分析
- 仮想パッチ適用

VMware IT：これまでの成果

500

Gbps の
トラフィックを保護

セキュリティの強化

- ワークロードに合わせて
  セキュリティを拡張
- ゼロトラスト アーキテクチャ

90%

のセキュリティ
ポリシーを削減

運用の俊敏性

- IP/ポート/プロトコルの
  ポリシーの代わりに
  セキュリティ グループを活用
- ポリシーの自動化によって
  古いポリシーを排除

40

時間/月の
メンテナンス作業を削減

コスト削減

- ポリシーの自動化をワーク
  ロードのライフサイクルに
  関連付け
- ネットワークの変更が不要

ネットワーク、アプリケーション、クラウドの保護

Carbon Black Cloud Container Security
- Kubernetes クラスタの構成/違反のアセスメント

Carbon Black Cloud Workload Protection（CWP）
- vCenter インスタンス内のすべての仮想マシンの CB Cloud Sensor（EndPoint Standard + EDR）を検証
- VC インスタンス内で実行されているワークロード（仮想マシン）の脆弱性評価を実施

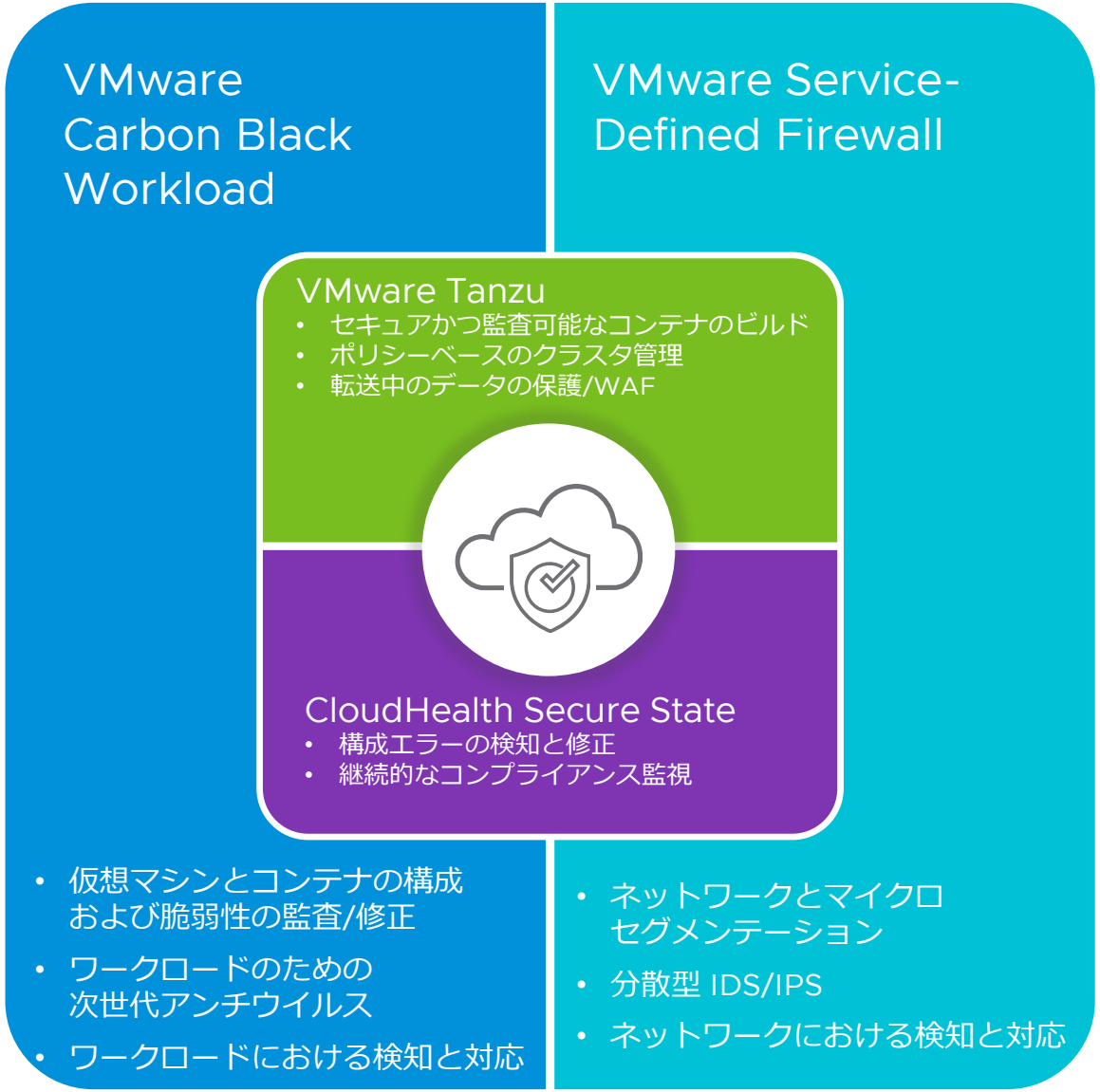
Carbon Black App Control
- 2,000 以上の Windows サーバを対象としたオンプレミス型のアプリケーション制御

CloudHealth Secure State
- VMware クラウドのワークロードのモニタリングおよびコンプライアンス追跡

NSX Firewall
- VMware のネットワークの（およびアプリケーション/サービスごとの）マイクロセグメンテーション

vRealize Network Insight
- ネットワーク セキュリティによる検知、検証、調査

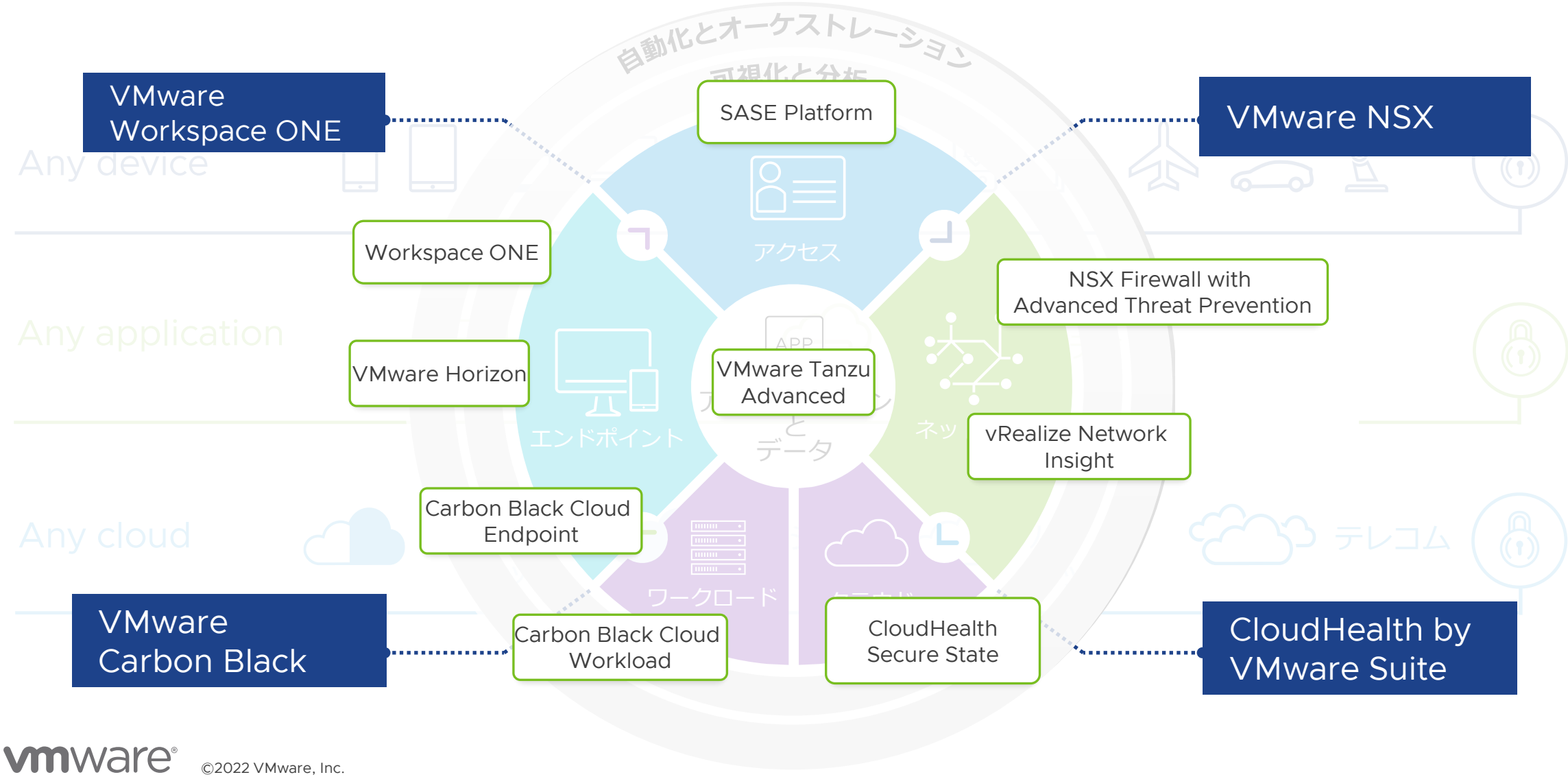
NSX Network Detection and Response（旧 Lastline）
- トラフィックをアプライアンスにミラーリングし、トラフィック分析を実行
- 次世代型 AI による侵入検知



まとめ

セキュリティとソリューションに関する VMware のビジョン

重要なアプリケーションとデータの保護



VMware on VMware プログラム リソース

vmwonvmw@vmware.com

https://blogs.vmware.com/vov/about/

https://www.vmware.com/jp/company/vmware-on-vmware

@vmwonvmw

ありがとうございました