

利便性とセキュリティの 両立したテレワーク環境を実現

Workspace One と Carbon Black 連携による
運用の効率化

世羅 英彦

ヴィエムウェア株式会社

セキュリティ事業部

シニアソリューションエンジニア

井本 玲雄

ヴィエムウェア株式会社

エンドユーザーコンピューティング事業部

シニアスペシャリストエンジニア



ユーザ利便性 vs セキュリティ

ユーザに管理者権限を与えていませんか？

管理者のジレンマ

ユーザがアプリを自由に
インストールできる必要がある

ユーザ利便性

重要なセキュリティ設定が
無効化されていないだろうか？

リスクのあるアプリが
インストールされている
かもしれない。。

管理者権限を付与したこと
で
マルウェアに感染。。



セキュリティ

どこでも安全に業務が出来る環境でしょうか？

攻撃を防ぎ、原因の特定と復旧の迅速化し早期の業務復旧

場所を問わず安全に業務を
継続出来るようにしたい

ユーザ利便性

ランサムウェアによる攻撃が
心配だ。。

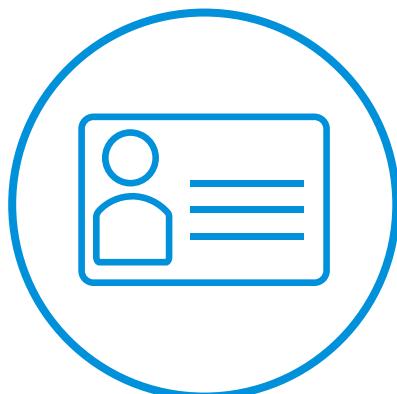
攻撃を食い止めるのも大事だが、
原因を特定し被害を最小限に
とどめたい。。

セキュリティ

被害からの復旧し再発防止を
早急に行いたい。。



感染から機密情報搾取まで



PowerShellなど悪意のある
スクリプトの実行

- Officeドキュメントなどを開くことで自動実行
- 管理者権限で脆弱性を悪用しセキュリティ機能を無効化

パスワードクラッキング

- ブルートフォース攻撃
- 辞書攻撃
- パスワードリスト攻撃

他のPC、サーバへ侵入

- 機密情報の搾取

管理者権限を剥奪することによるリスクの軽減

2017年02月27日 20時00分

Microsoft製品の脆弱性の94%は管理者権限をオフにすることで回避可能であることが判明



By public domain

コンピューターのソフトウェアにまつわる脆弱性は常にユーザーを惑わせる問題ですが、セキュリティ関連企業の調査によると、Windowsに関する脆弱性の大部分はOSやアプリケーションの管理者権限を編集することで回避できることが明らかになりました。

94% of Microsoft vulnerabilities can be easily mitigated | Computerworld

<http://www.computerworld.com/article/3173246/security/94-of-microsoft-vulnerabilities-can-be-easily-mitigated/>

出典: Gigazine(2017/2) <https://gigazine.net/news/20170227-94-percent-microsoft-vulnerability-mitigated/>

The screenshot shows a news article from Security IT News. The header includes the site's logo with binary digits, the word "Security", and "IT News". Below the header is a navigation bar with links: HOME, SECURITY (which is underlined), CLOUD, DEVOPS, IOT, AI, and ENDPOINT. A breadcrumb trail says "YOU ARE AT: Home > Security > News > BeyondTrust Finds 56 Percent of Critical Microsoft Vulnerabilities can be Mitigated by Removing Admin Rights". The main content features a large circular graphic with a blue border, showing "2021年" at the top and "56%" in the center. The background of the graphic is a blue-toned image of gears and digital icons.

| BeyondTrust Finds 56 Percent of Critical Microsoft Vulnerabilities can be Mitigated by Removing Admin Rights

管理者権限を剥奪すると、脆弱性を悪用したリスクを軽減可能

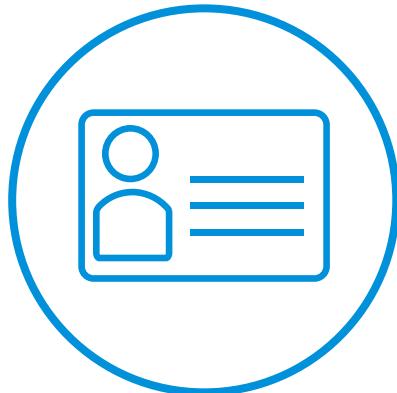
出典: Security IT News(2021/3)<https://digitalitnews.com/beyondtrust-finds-56-percent-of-critical-microsoft-vulnerabilities-can-be-mitigated-by-removing-admin-rights/>

感染から脅威へのリスク軽減



感染

- PowerShellや脆弱性を悪用し侵入



管理者権限剥奪

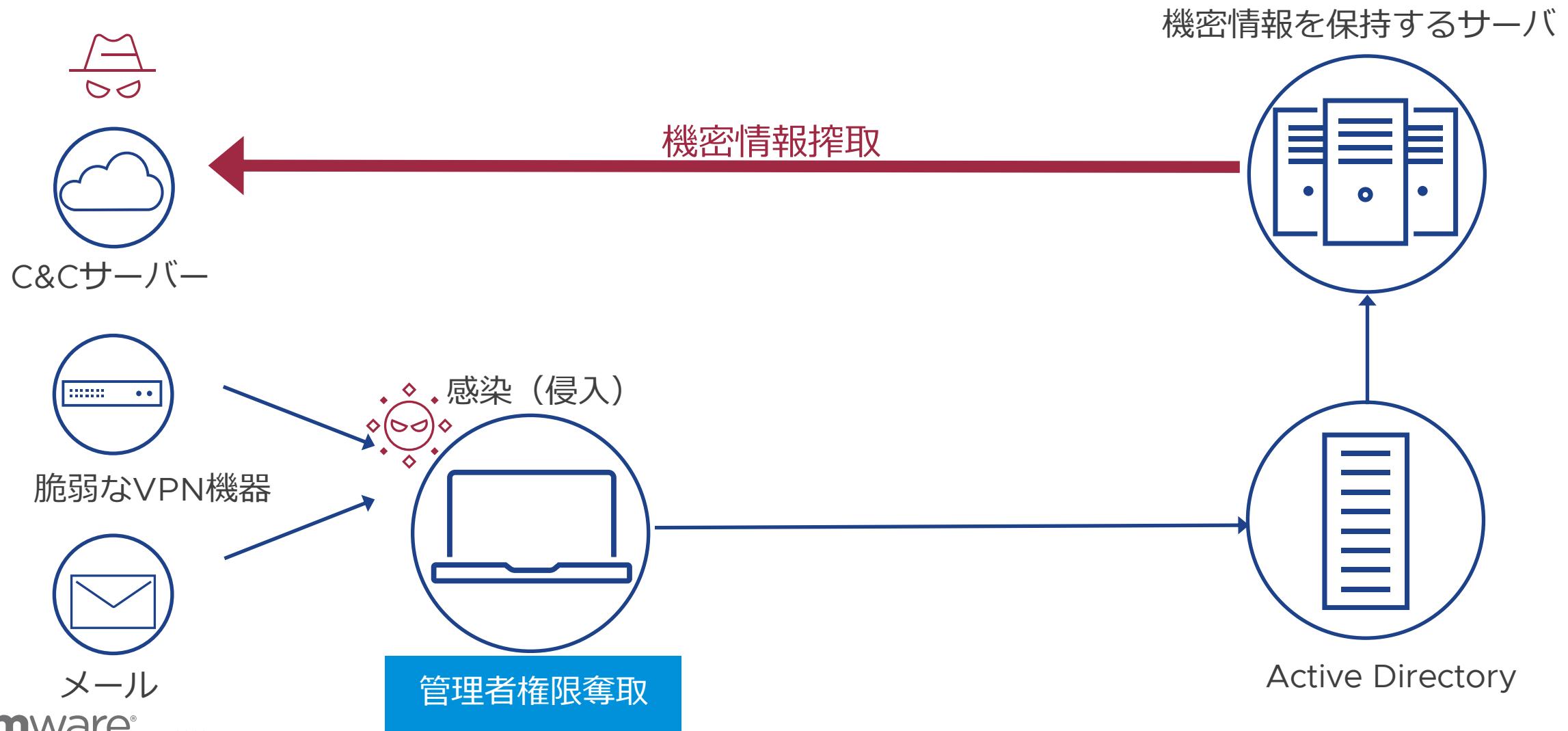
- 感染の影響範囲の緩和
- 組織のシステム根幹を容易に狙えない



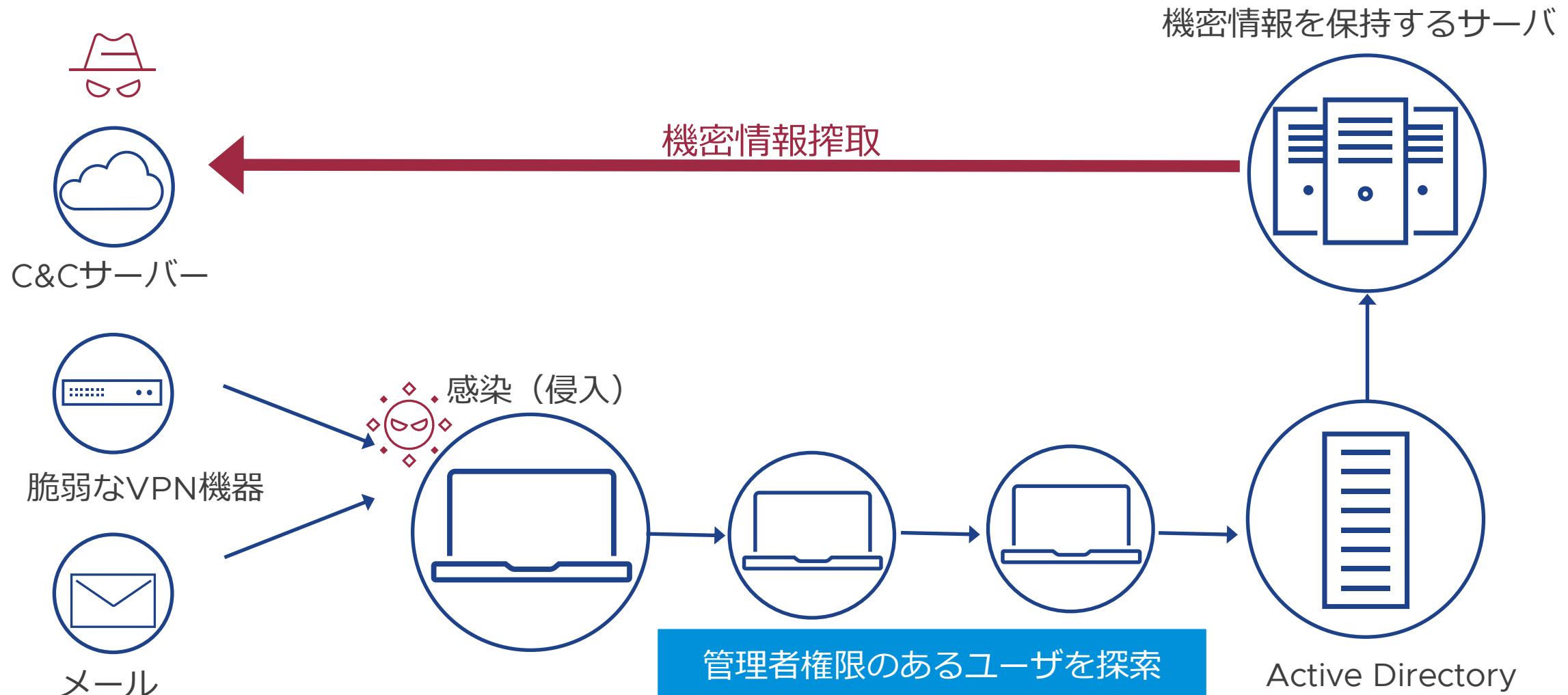
脅威

- 管理者権限を悪用したリスクを軽減

攻撃されたユーザが管理者権限を持っている場合



攻撃されたユーザが管理者権限を持っていない場合



両方のバランスが取れるとしたらいいかがでしょうか？

ユーザ利便性



セキュリティ

Workspace ONE とは



Workspace ONE ができること

本日、頭の片隅に覚えて帰っていただきたい3つのポイント

認証基盤を構築できる



ID & アクセス管理

さまざまなデバイスを
インターネット下で一元管理できる



統合エンドポイント管理

デバイス情報を可視化して
利活用できる



可視化 & 自動化



Workspace ONE®
Intelligent Hub



SAMSUNG
Knox



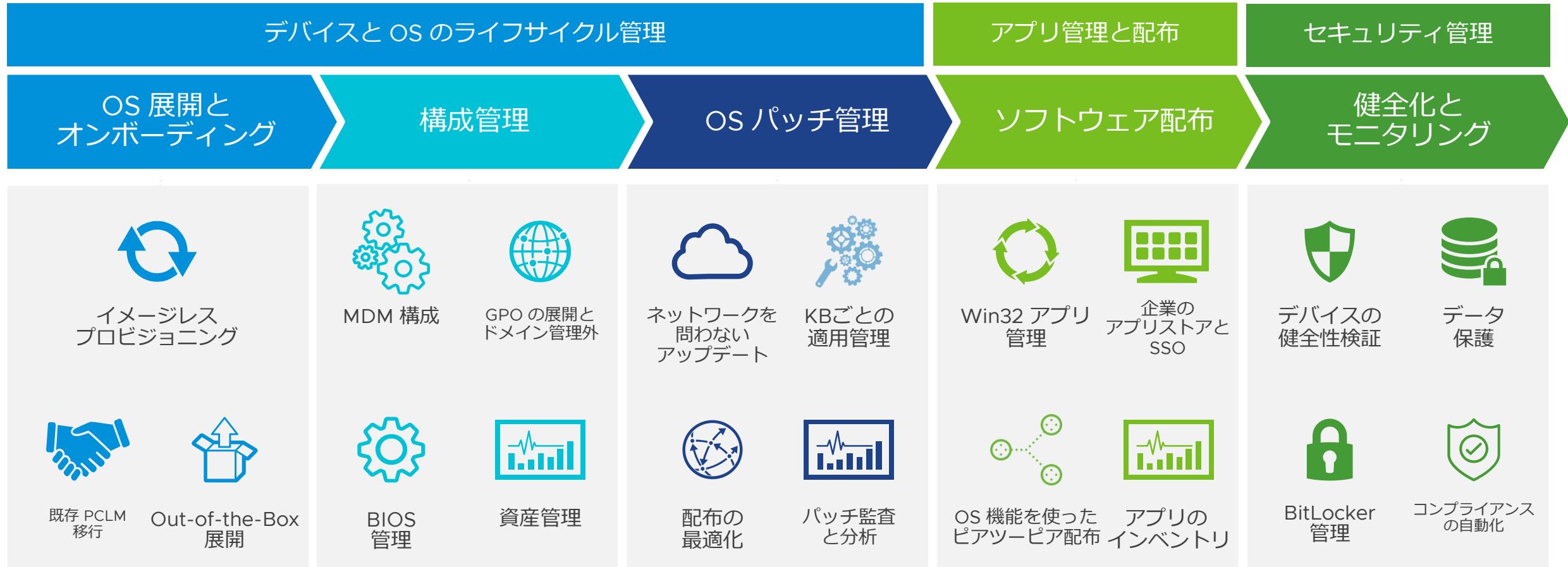
macOS



Desktop, Mobile, Rugged, Virtual, IoT

PC ライフサイクル管理を実現する Workspace ONE

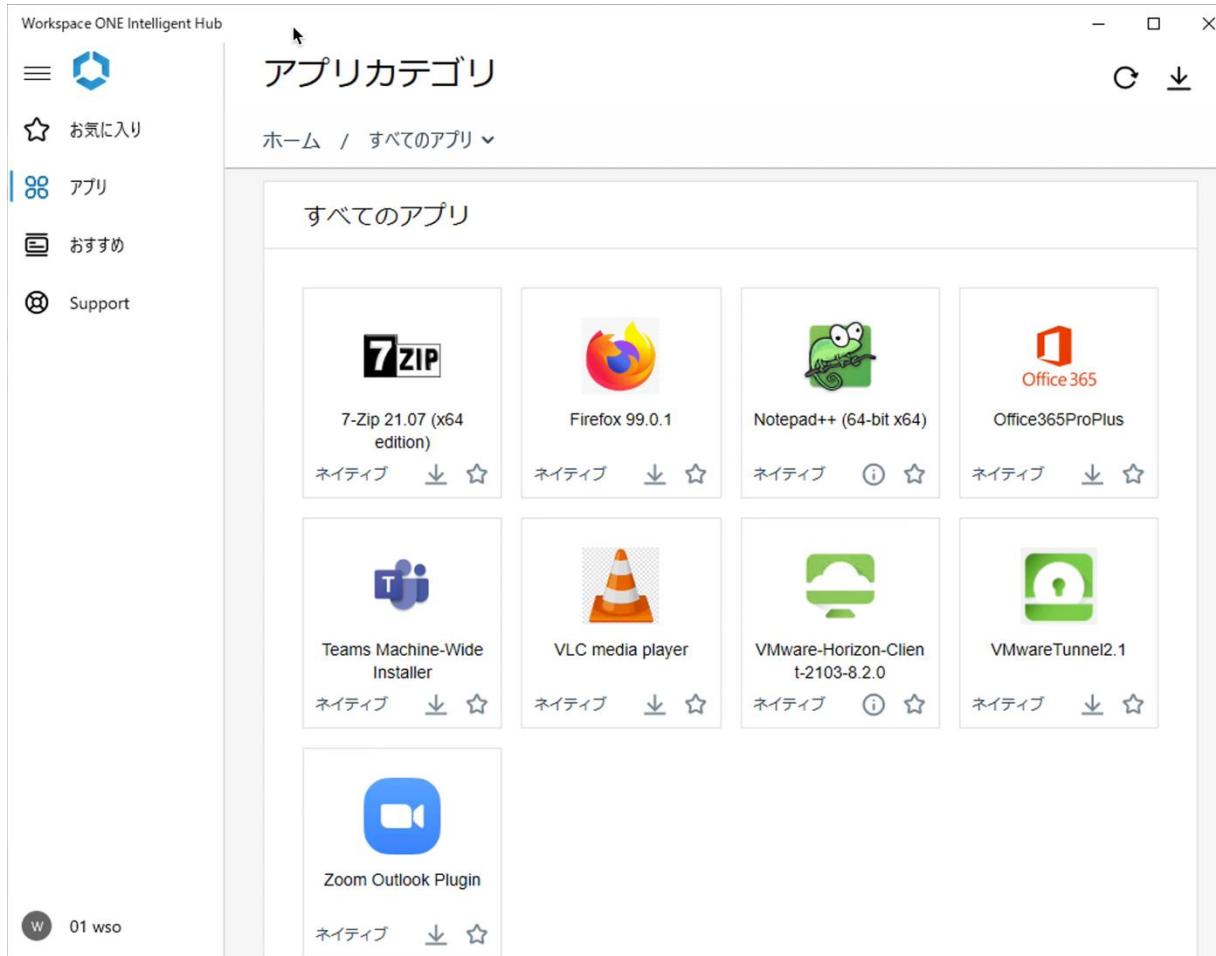
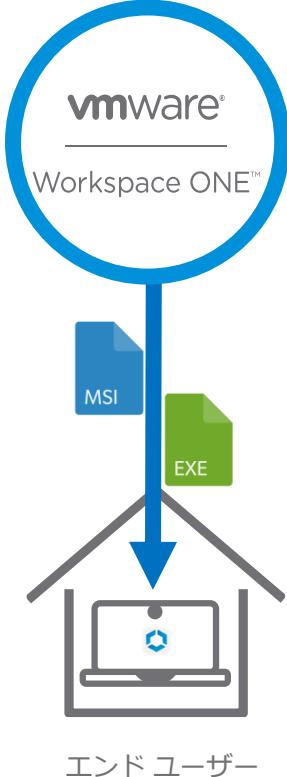
Windows デバイスに対する管理ソリューション



インテリジェント・インサイトとルールエンジン

アプリケーション配信

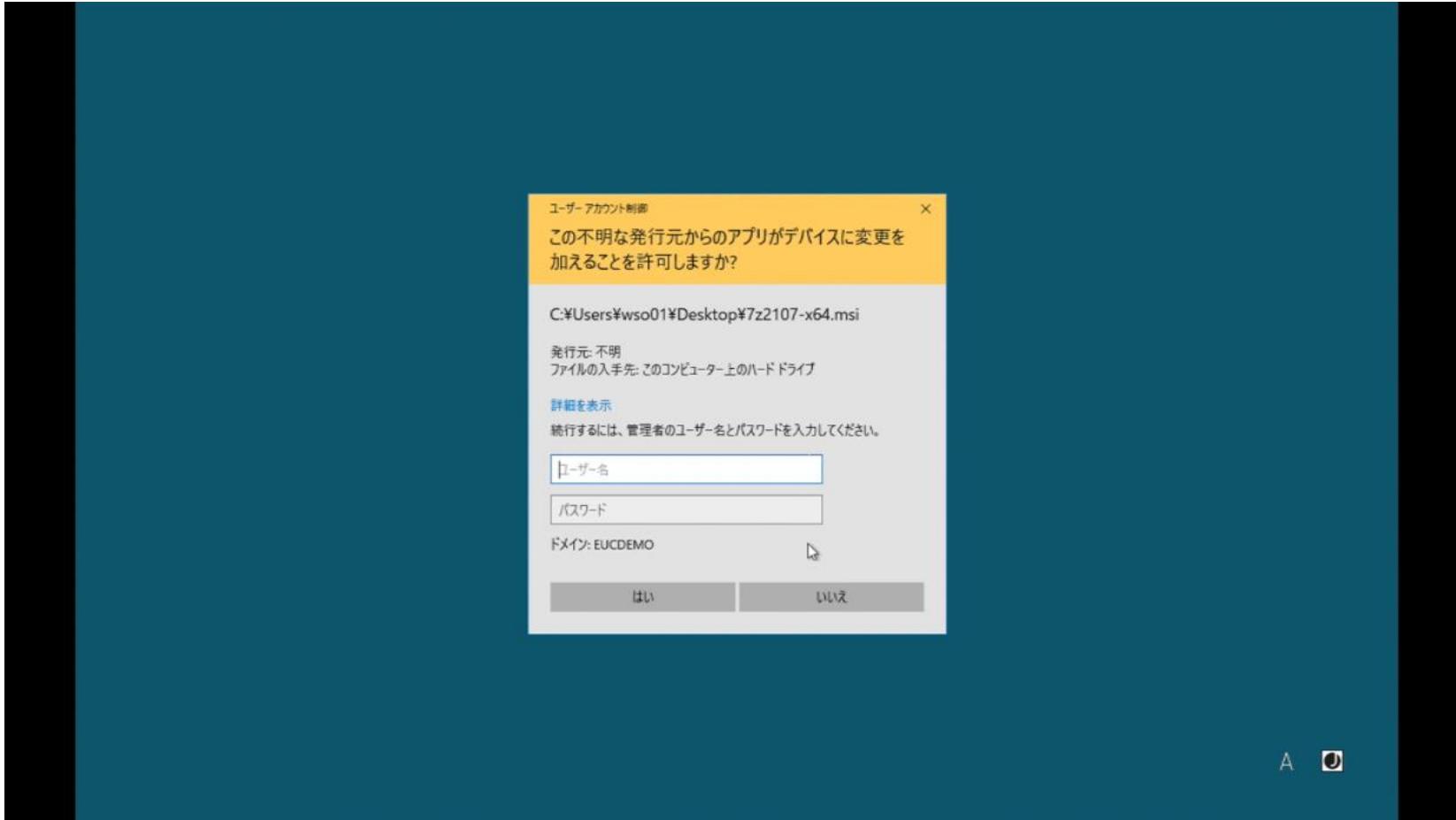
ユーザーに管理者権限不要でアプリケーションインストールを実現



- 管理者権限の剥奪によるセキュリティ向上
- ユーザ属性に基づくアプリケーションの資格付与を実現（アプリケーションカタログ）
- 自動インストール or 必要なときにユーザが自身でインストール可能

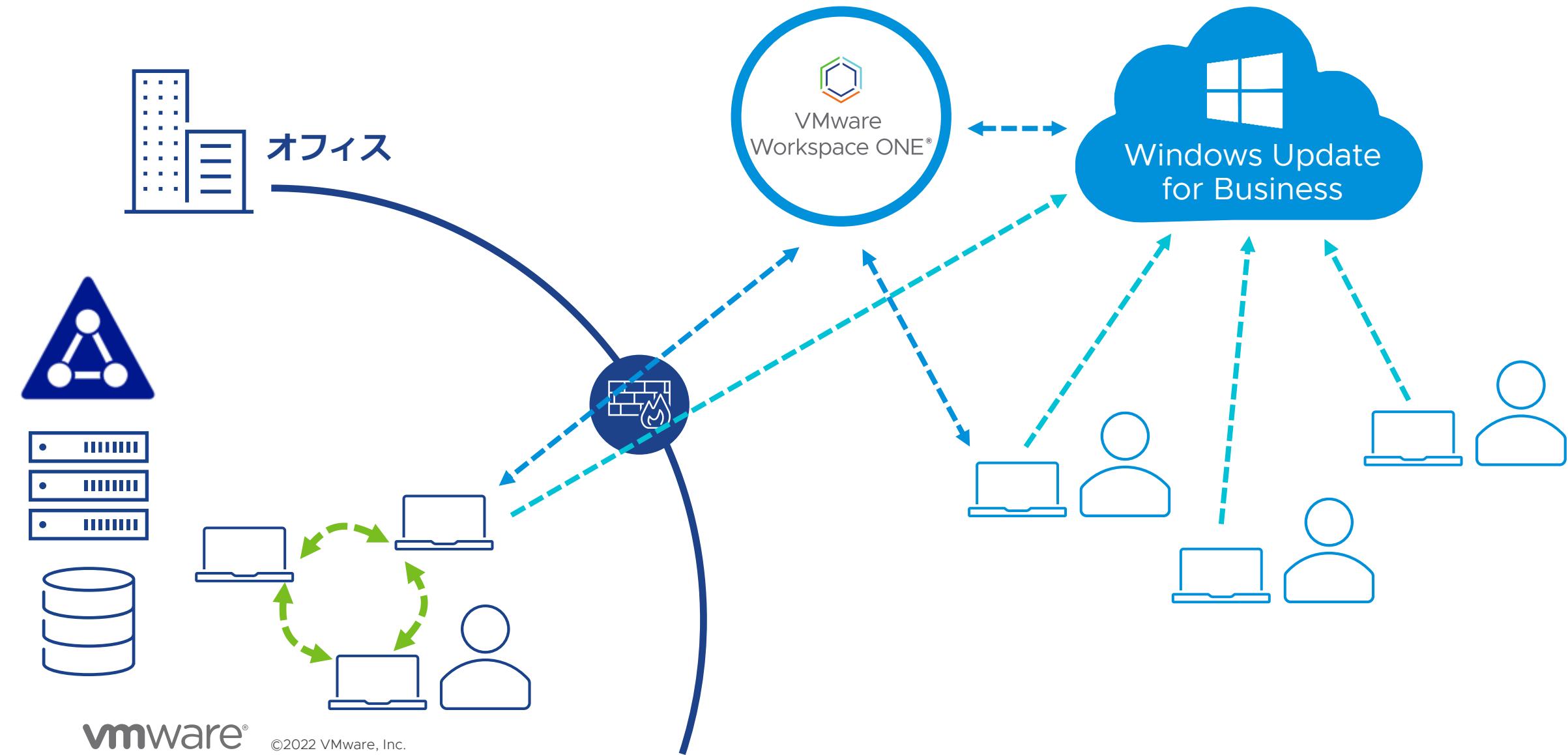
[デモ]管理者権限不要でアプリケーションのインストールを実現

業務に必要なアプリケーションをアプリカタログからインストール



インターネットを前提とした Windows Update 管理

クラウドから Windows Update を制御



インターネットを前提とした Windows Update 管理

デバイスに対する Windows Update ポリシーを定義しデバイスに配布

Windows Update - Demo

ペイロードの検索

全般

パスワード

Wi-Fi

VPN

資格情報

制限

Defender Exploit Guard

データ保護

Windows Hello

ファイアウォール（レガシー）

ファイアウォール

アンチウイルス

暗号化

Windows 更新プログラム

プロキシ

OEM 更新プログラム

Windows 更新プログラム

Windows 10

プランチを作成して延期

Windows 更新ソース

MICROSOFT アップデートサービス WSUS

プランチを更新

年 2 回チャンネル

Insider ビルド

許可済み 許可しない

機能更新プログラムを延期 (日)

180

機能更新プログラムを停止

有効化 無効化

品質更新プログラムを延期 (日)

21

品質更新プログラムを停止

有効化 無効化

コンソール画面

Workspace ONE UEM

← 設定

構成されている更新ポリシーを表示

[一部の設定は組織によって管理されています] と表示される理由は次のとおりです。

このテキストは通常、インストールと配信のポリシーが構成された後の Windows Update で表示されます。

次のような例があります。

- 組織により、更新プログラムを管理するためのポリシーが設定されている場合
- Windows Insider Program にオプトインしている場合

デバイスに設定されているポリシー

更新プログラムを自動的にダウンロードし、指定されたスケジュールでインストールする
ソース: 管理者
種類: グループ ポリシー

自動でインストールし、再起動をするよう通知する
ソース: 管理者
種類: モバイル デバイス管理

アクティブ時間の開始時刻を設定する
ソース: 管理者
種類: モバイル デバイス管理

アクティブ時間の終了時刻を設定する
ソース: 管理者
種類: モバイル デバイス管理

アクティブ時間の最大範囲
ソース: 管理者
種類: モバイル デバイス管理

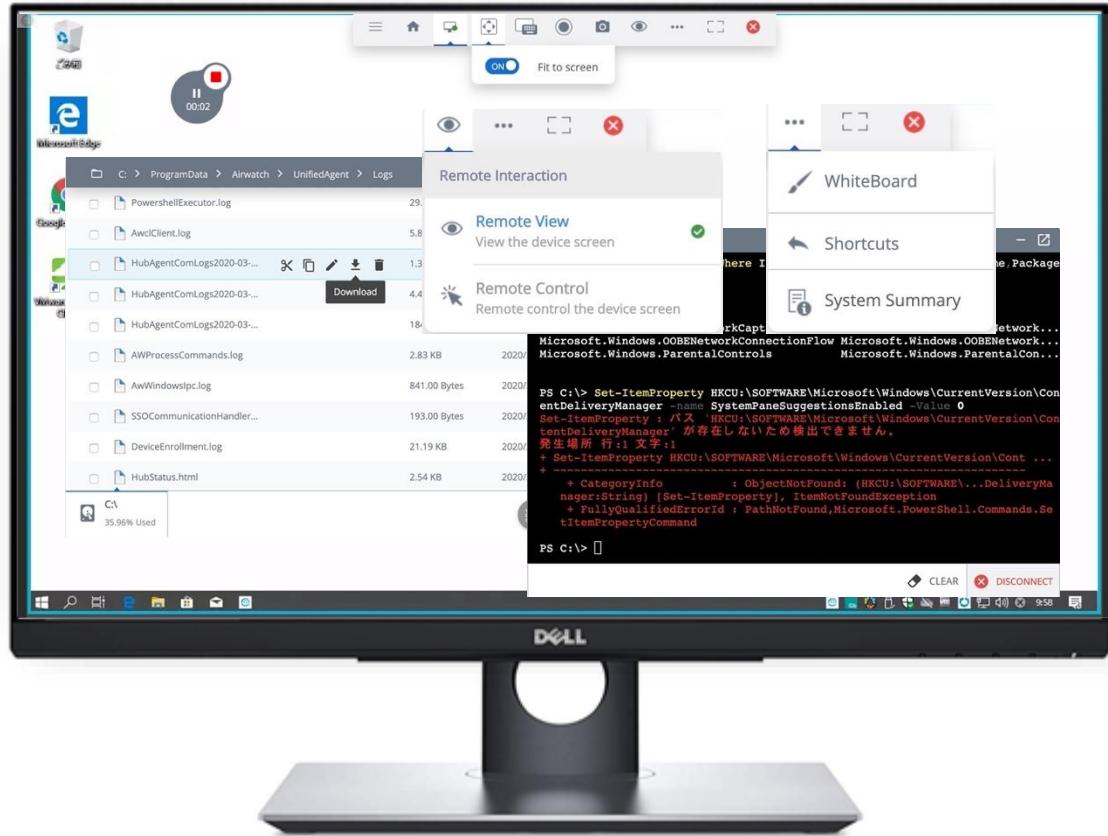
他の Microsoft 製品の更新プログラムの入手
ソース: 管理者
種類: モバイル デバイス管理

デバイスのポリシー

Workspace ONE UEM

テレワークに必須な遠隔サポート機能

VMware Workspace ONE Assist



- リアルタイムで社員のデバイスを表示およびリモートコントロール
- デバイス情報を取得することで、迅速な問題点の特定および修正を実現
- 画面を共有していることをユーザーに通知し、リモートセッションを切断する権限を与えることでプライバシーを保護
- セッションレコーディング機能

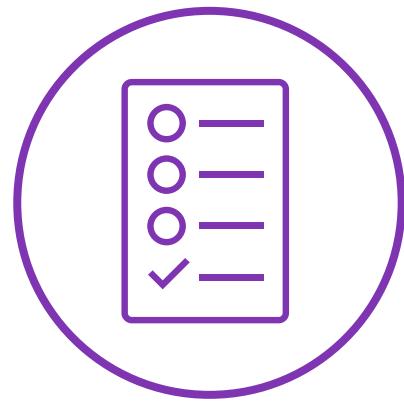
社員のプライバシーを保護しながら遠隔サポートを実現

高度化するセキュリティ攻撃

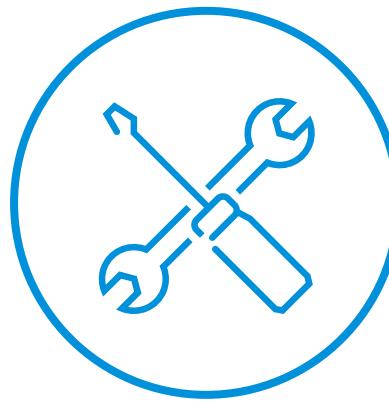
昨今の高度化した脅威への対応は
これで大丈夫なのでしょうか？



サイバー攻撃の防御に大切なこと



攻撃可能な対象を
最小化

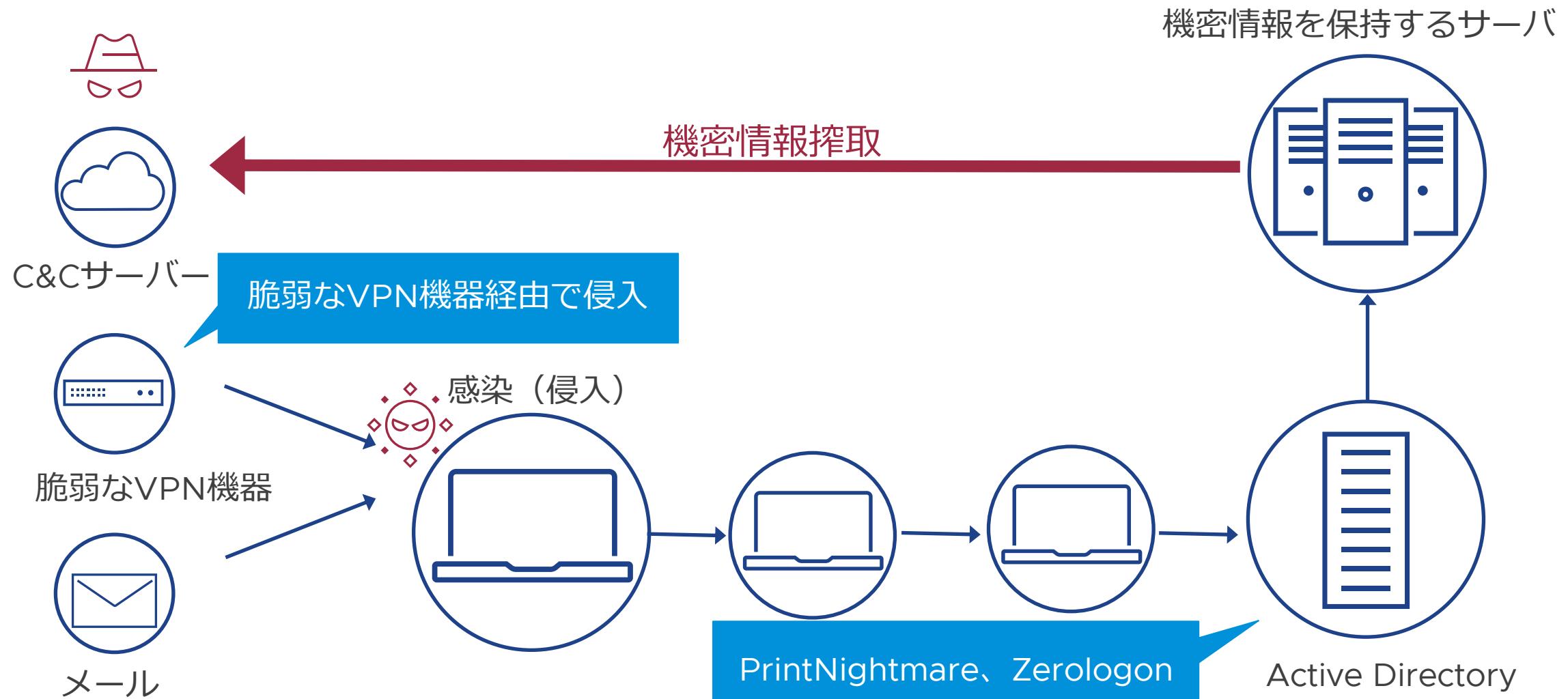


被害の拡大を
最小化



ユーザ利便性と
セキュリティの両立

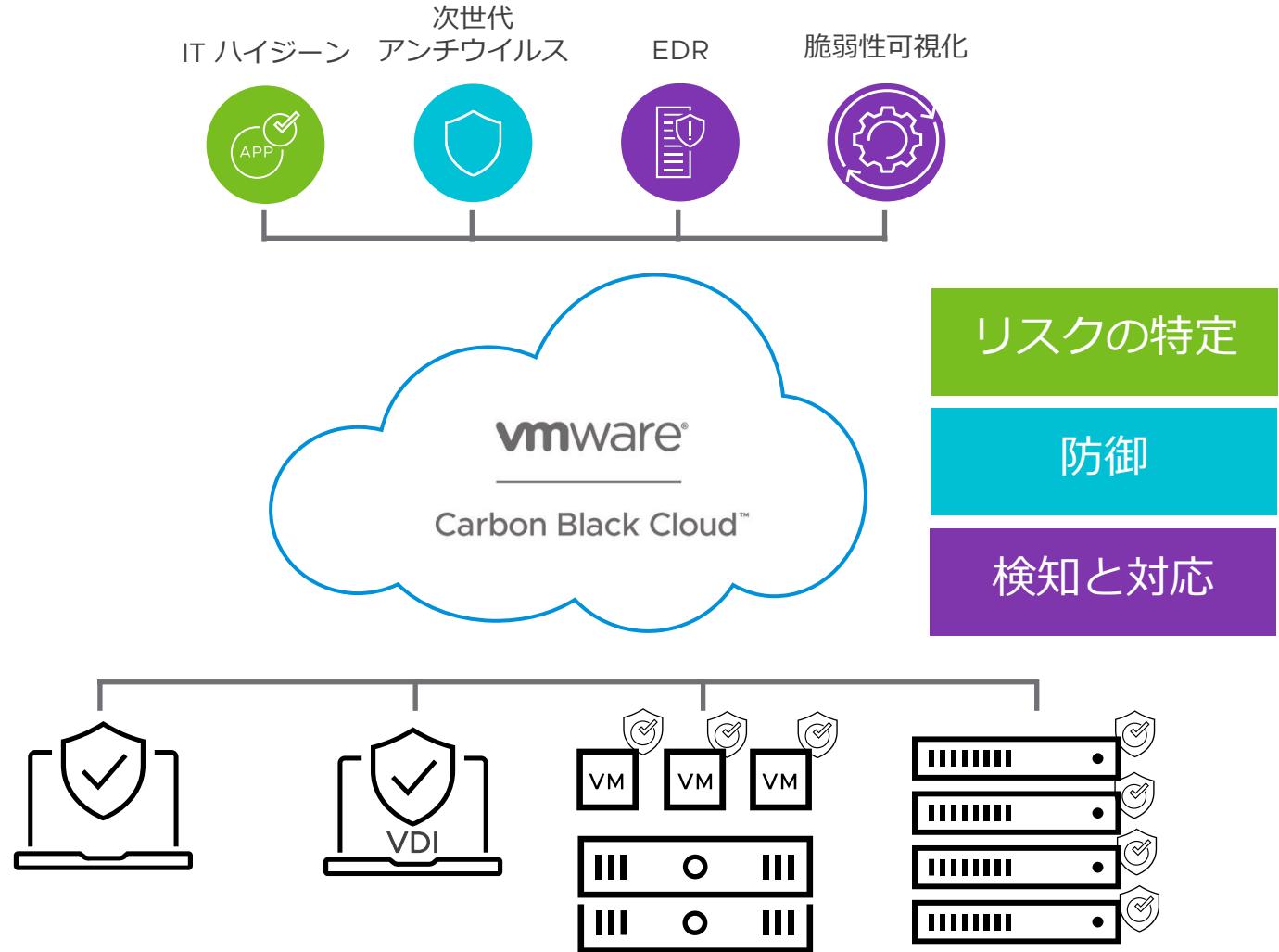
その他の脅威



Carbon Black Cloudとは



Carbon Black Cloud



シングルエージェント
シングルコンソール
端末のすべての挙動をクラウドに保存
カーネルモードで動作
日本語 UI
日本にデータセンター
NGAV
EDR
IT ハイジーン
脆弱性可視化

攻撃者は巧妙に攻撃を仕掛ける

ターゲットの情報を収集

- フィッシングメールでペイロードを配信
- 脆弱性を悪用

ターゲットとのネットワーク接続を維持

- 認証情報の取得
- 搾取するデータの探索

ランサムウェア実行

ファイルを暗号化

ファイルを外部へ送信

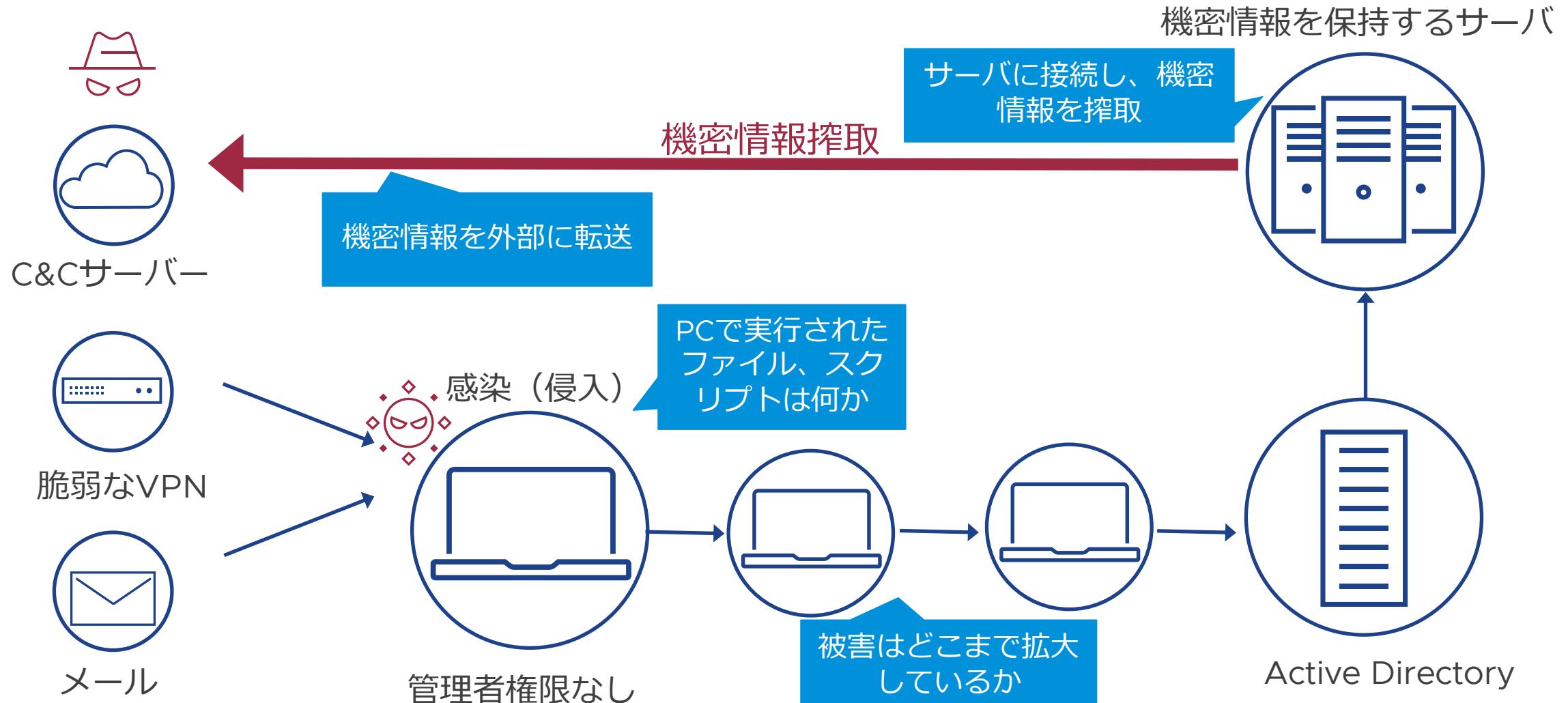


EDR とは

- 01 侵入経路の特定
- 02 侵害端末の特定
- 03 漏洩した情報と経路の特定
- 04 被害の封じ込め
- 05 復旧、再発防止

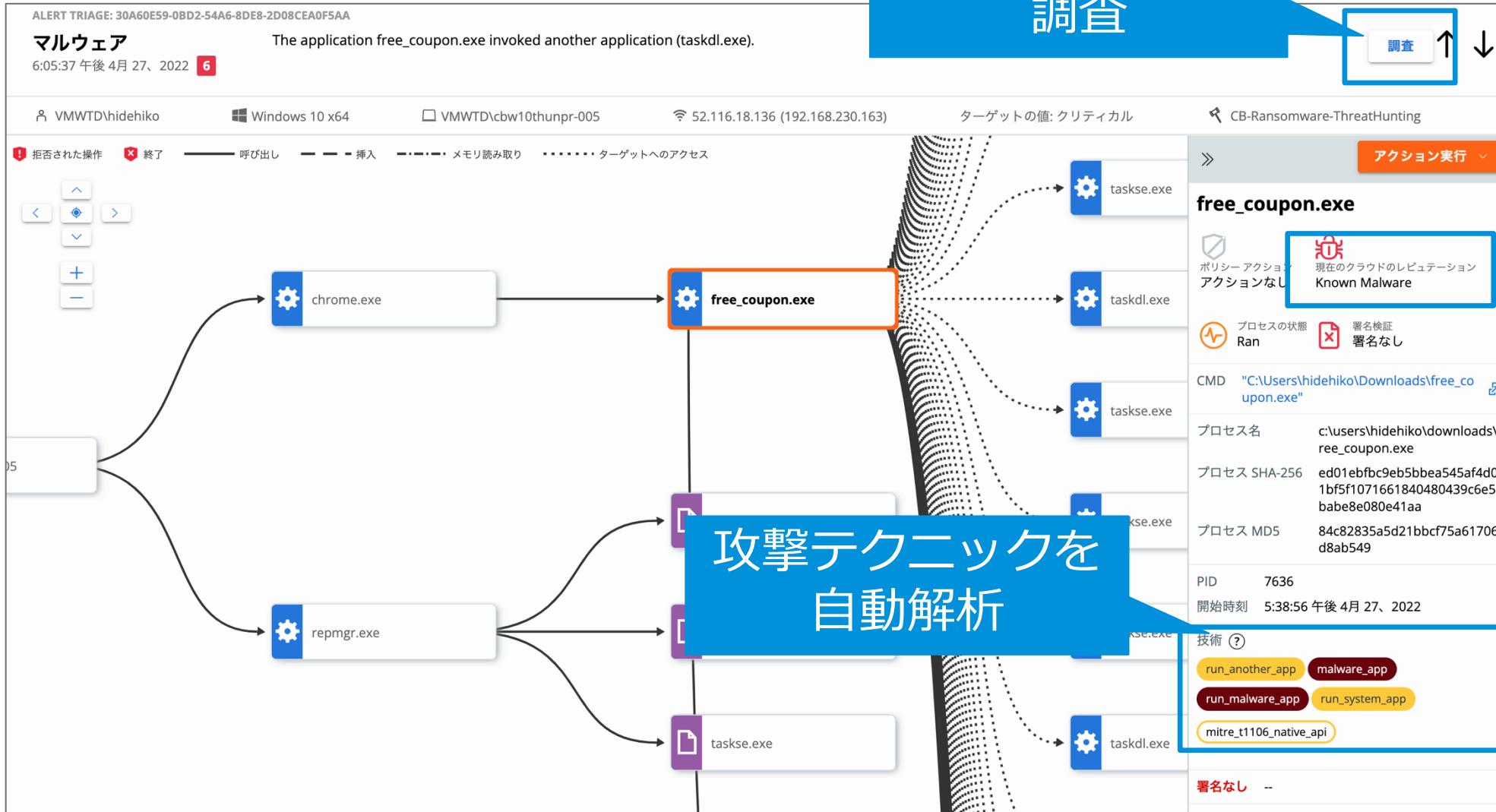


EDRはすべての挙動を記録

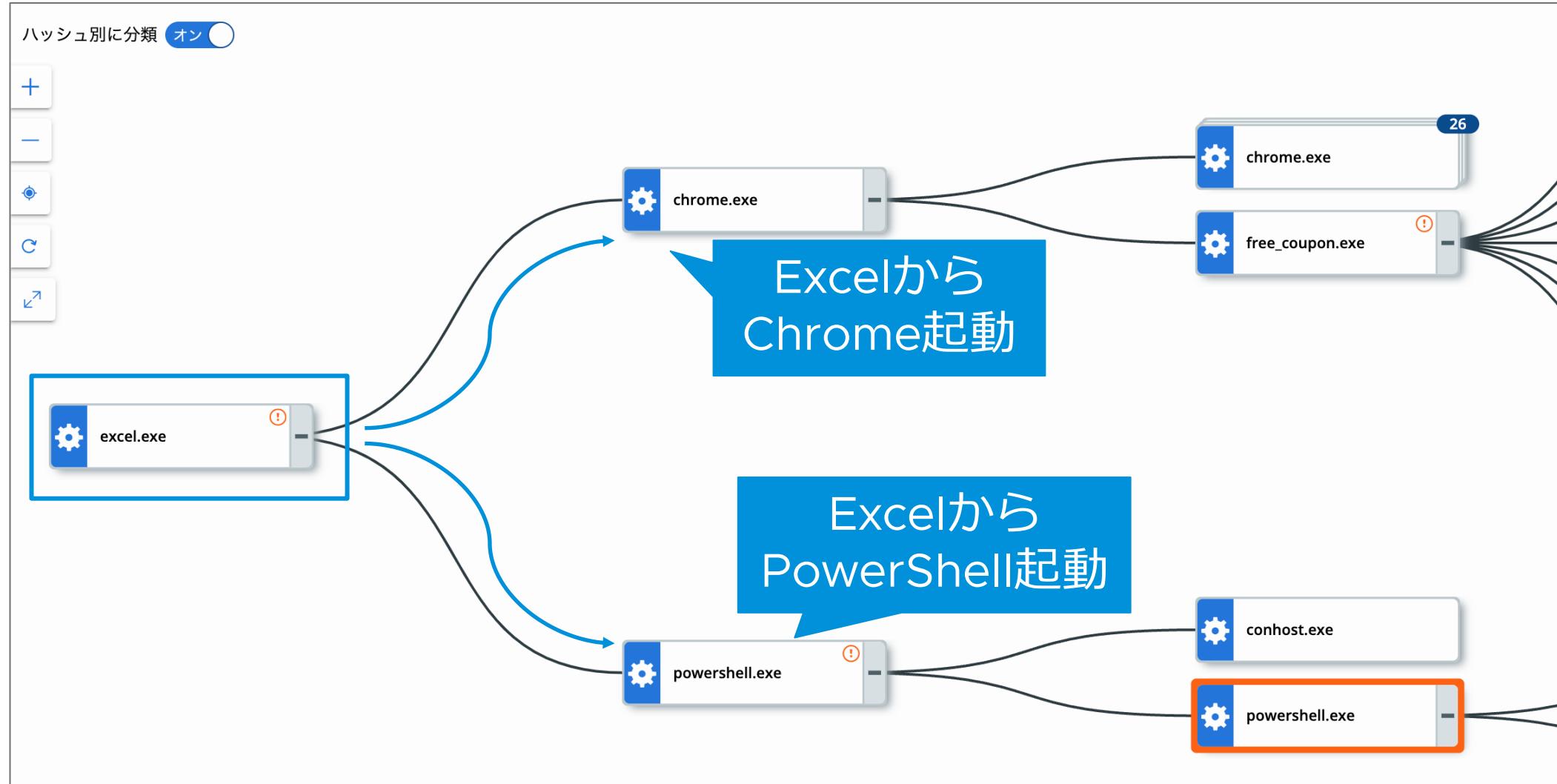


NGAVによる検知、ブロック

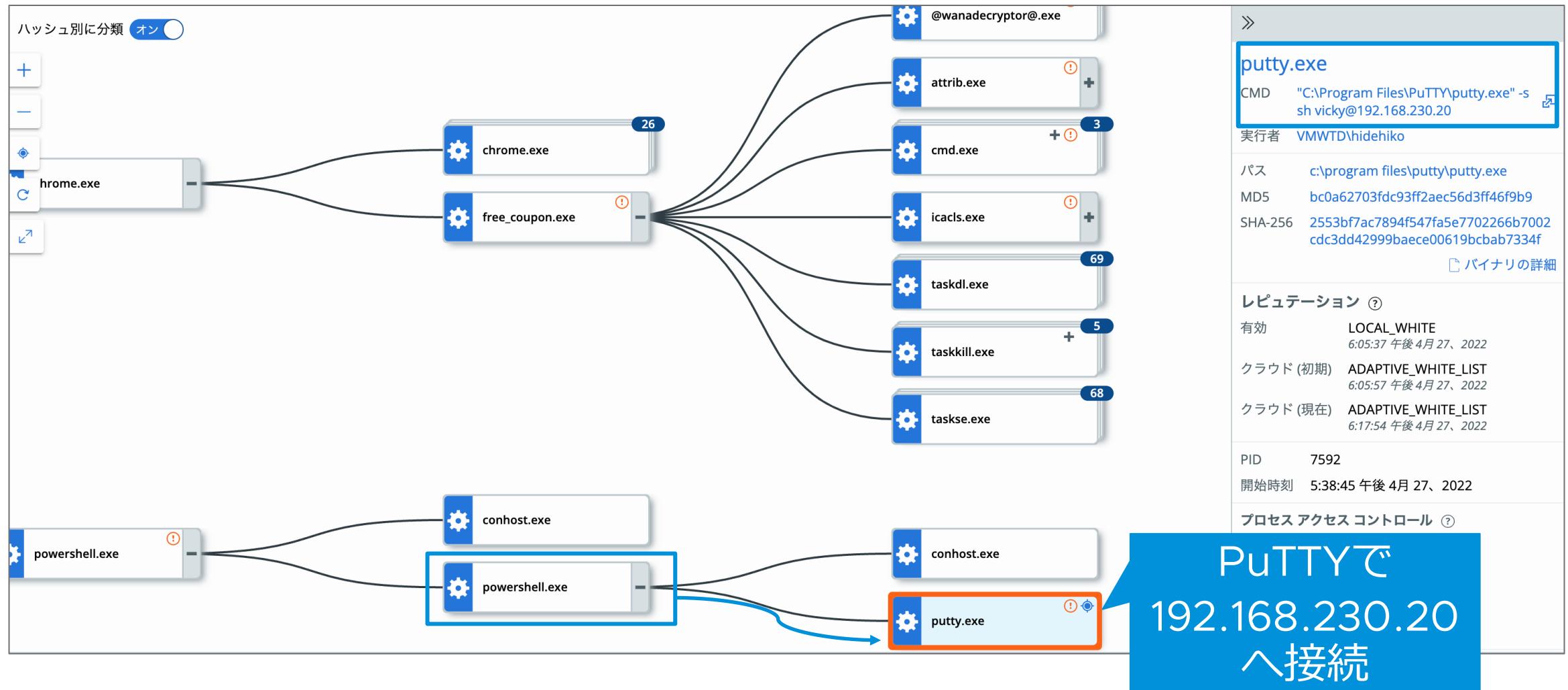
さらなる深堀り
調査



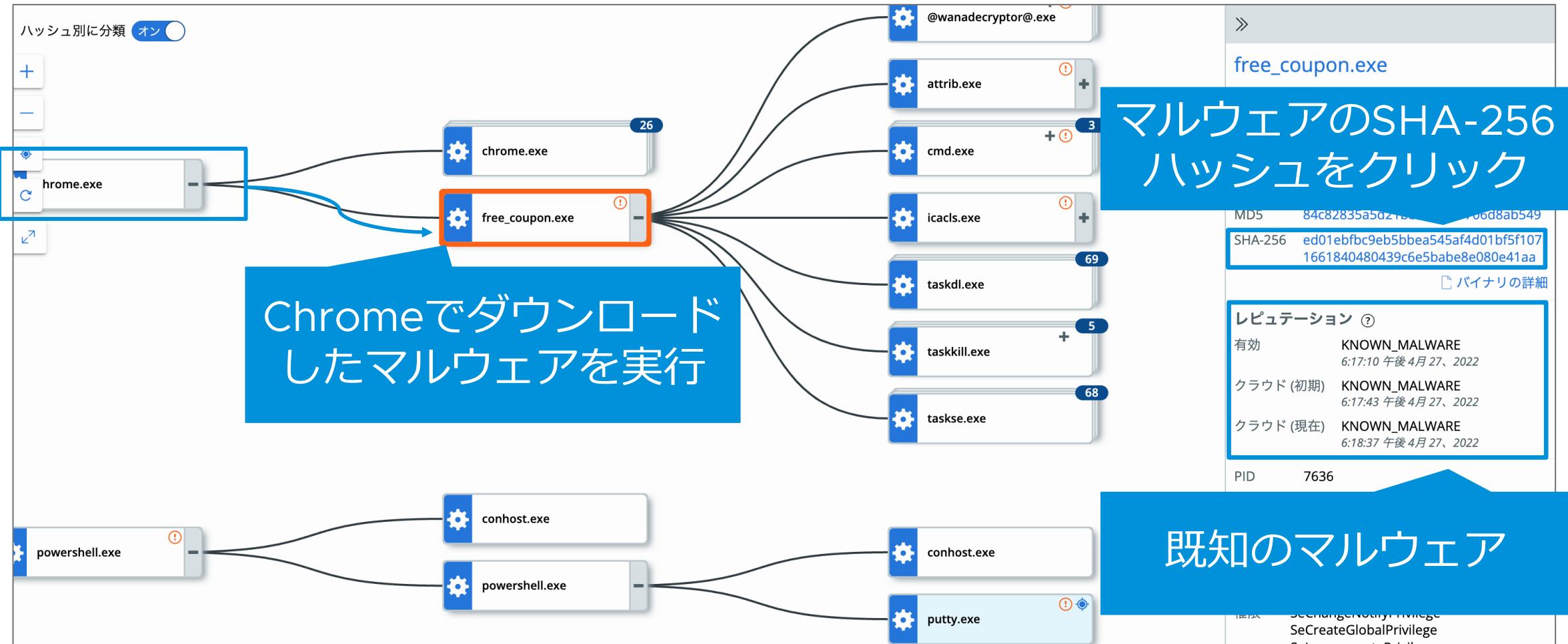
EDRによる可視化、調査



EDRによる可視化



EDRはすべての挙動を記録



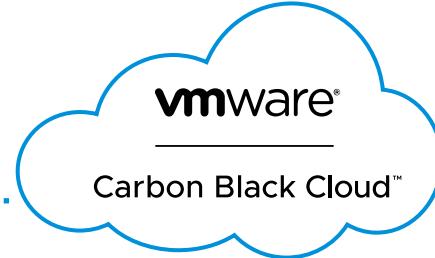
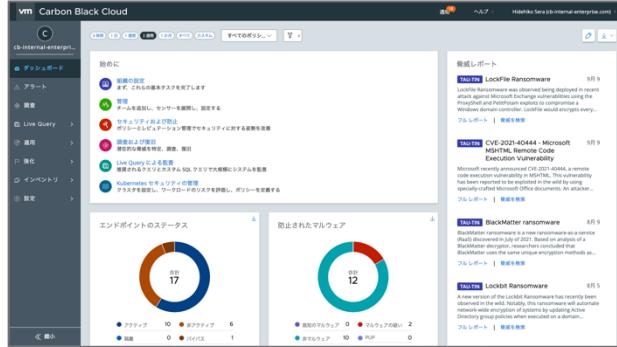
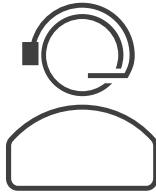
EDRはすべての挙動を記録

過去30分、1時間、6時間、1日、3日、30日、カスタムでの指定が可能

The screenshot shows a network monitoring interface with a search bar at the top containing the query "(process_hash:ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa)". Below the search bar are tabs for "イベント詳細" and "プロセス". A blue callout box points to the search bar with the text "過去30分、1時間、6時間、1日、3日、30日、カスタムでの指定が可能". Another blue callout box points to the list of results with the text "過去3日間にマルウェアを実行した端末を一覧で表示". The results table has columns: デバイス, ユーザー, ポリシー, グループ, OS, イベント, and アクション. The results show multiple entries for devices like "vmwtd\cbw10thunpr-005" through "vmwtd\cbw10thunpr-002", all under the "cb-ransomware-threathunting" policy and group, running on WINDOWS operating systems with event counts of 62, 33, 36, 34, 33, and 34 respectively. The left sidebar includes sections for "フィルタ", "タイプ (3)", "プロセス (4)", "有効なレピュテーション (1)", and "プロセス ハッシュ (2)".

デバイス	ユーザー	ポリシー	グループ	OS	イベント	アクション
vmwtd\cbw10thunpr-005		cb-ransomware-threathunting	cb-ransomware-threathunting	WINDOWS	62	
vmwtd\cbw10thunpr-003		cb-ransomware-threathunting	cb-ransomware-threathunting	WINDOWS	33	
vmwtd\cbw10thunpr-003		cb-ransomware-threathunting	cb-ransomware-threathunting	WINDOWS	36	
vmwtd\cbw10thunpr-001		cb-ransomware-threathunting	cb-ransomware-threathunting	WINDOWS	34	
vmwtd\cbw10thunpr-004		cb-ransomware-threathunting	cb-ransomware-threathunting	WINDOWS	33	
vmwtd\cbw10thunpr-002		cb-ransomware-threathunting	cb-ransomware-threathunting	WINDOWS	34	

EDR の重要性



EDR ログを元に
インシデントの深刻化を
防ぐことが重要

端末上のすべての挙動を記録することが重要

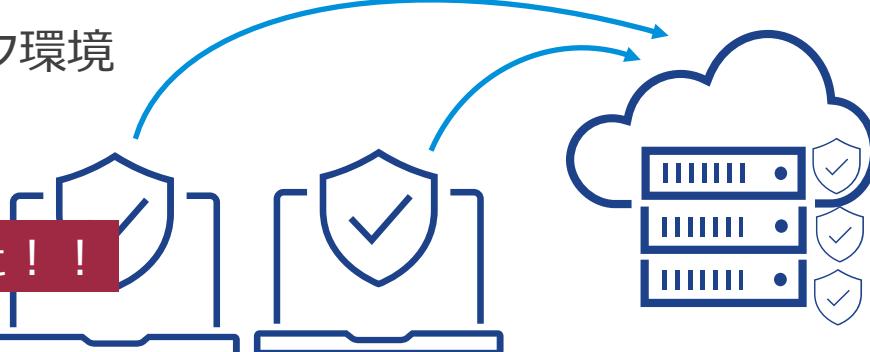
PCを再インストールし直しても

解決とはならない

テレワーク環境



侵入された！！



オフィス環境

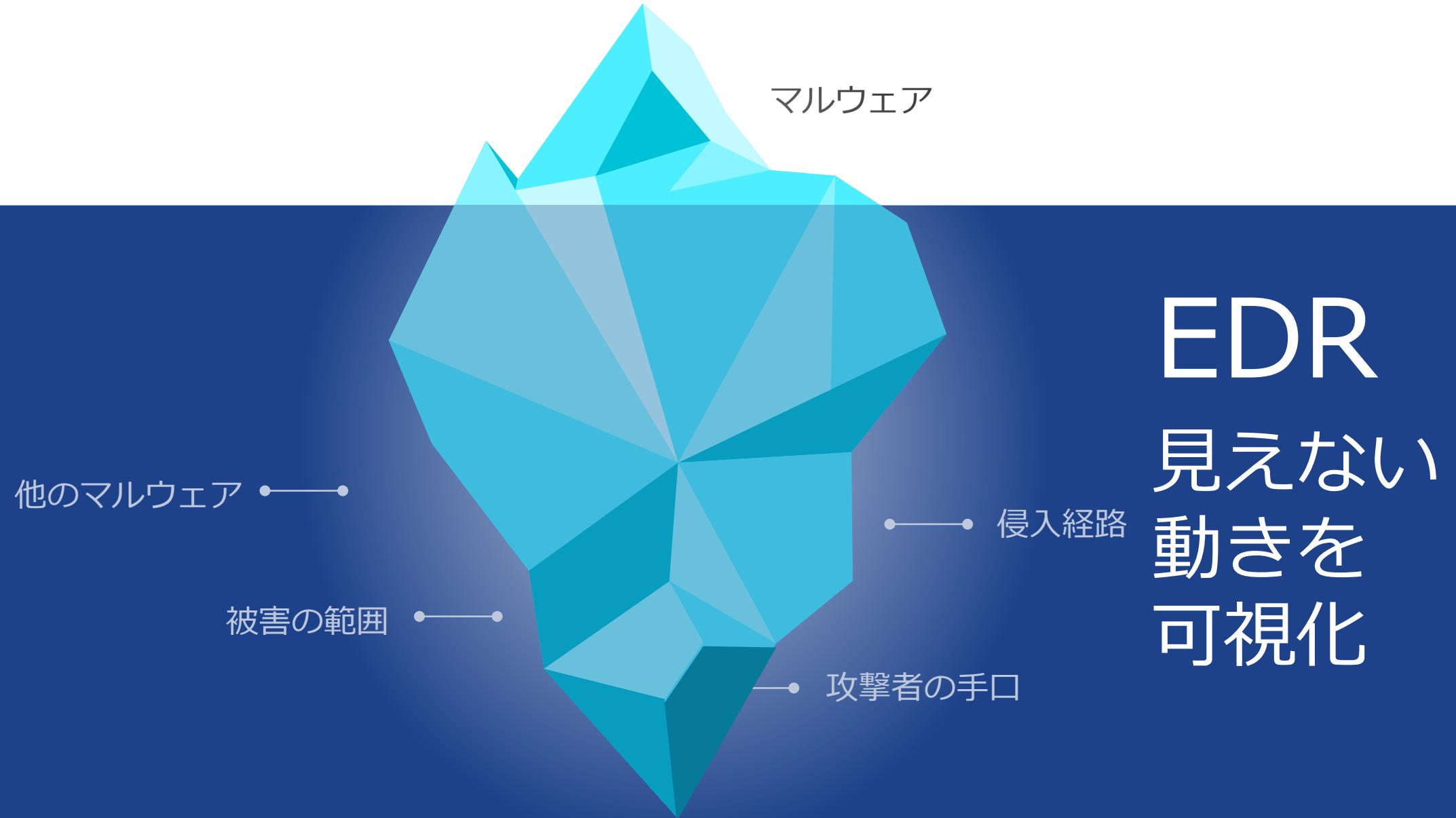


侵入された！！



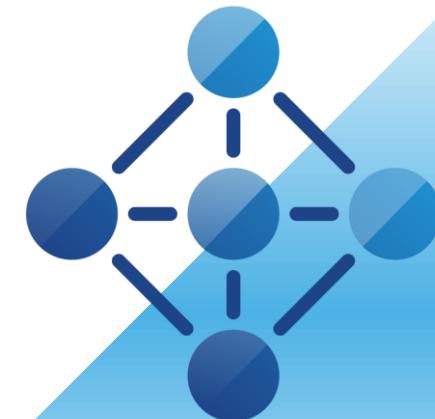
攻撃者は組織内の標的に到達し目的を実行

EDR とは



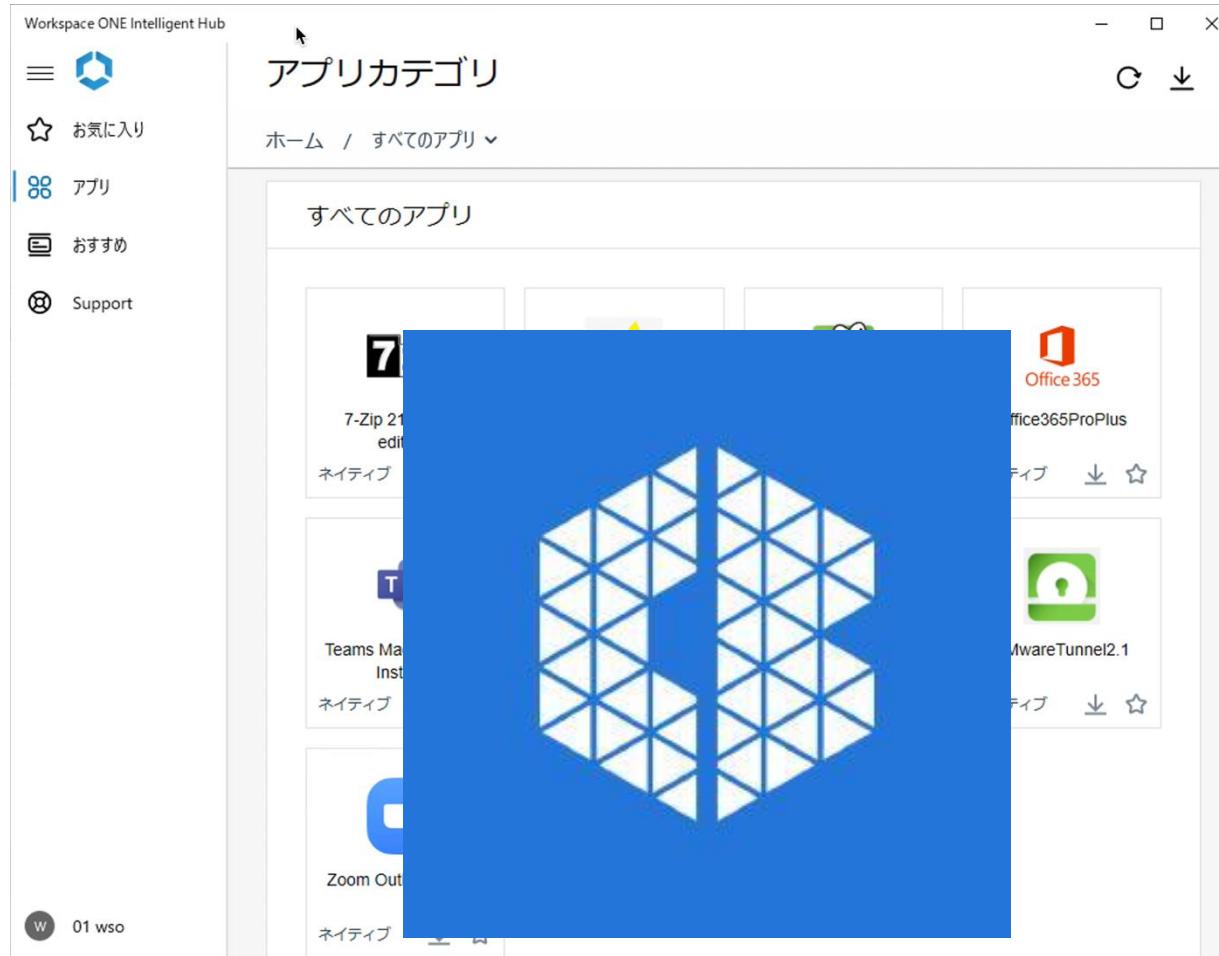
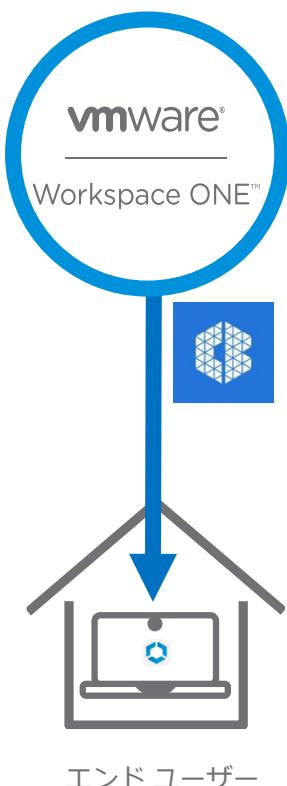


Workspace ONE x Carbon Black 連携



1. CB エージェントの配信

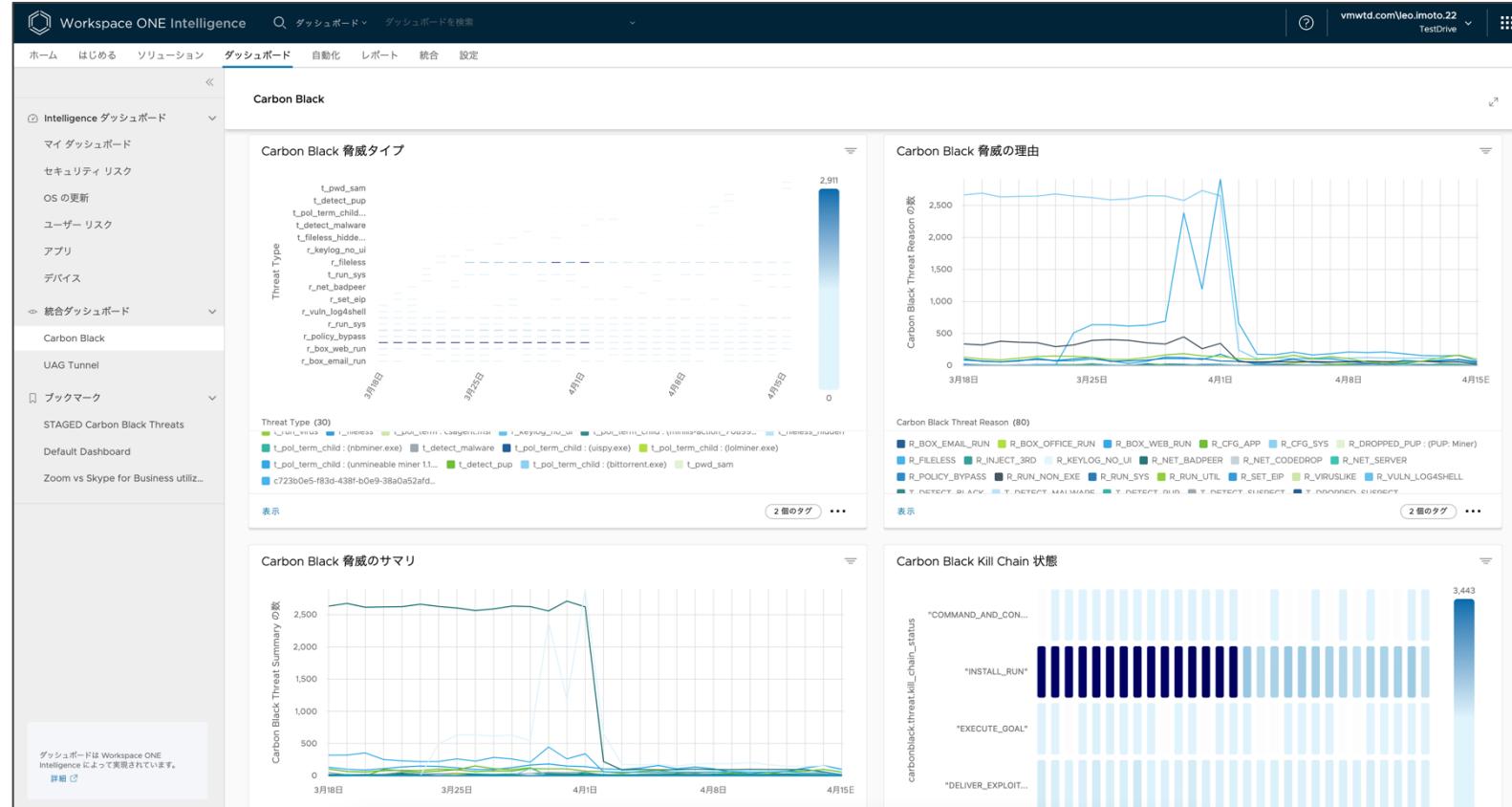
セキュリティソフトウェアのサイレントインストール実現



- 管理者権限の剥奪によるセキュリティ向上
- WS1 加入と同時にCB エージェントのサイレントインストールを実現
- CB エージェントのインストール状況を可視化

2. 脅威の可視化・インサイト

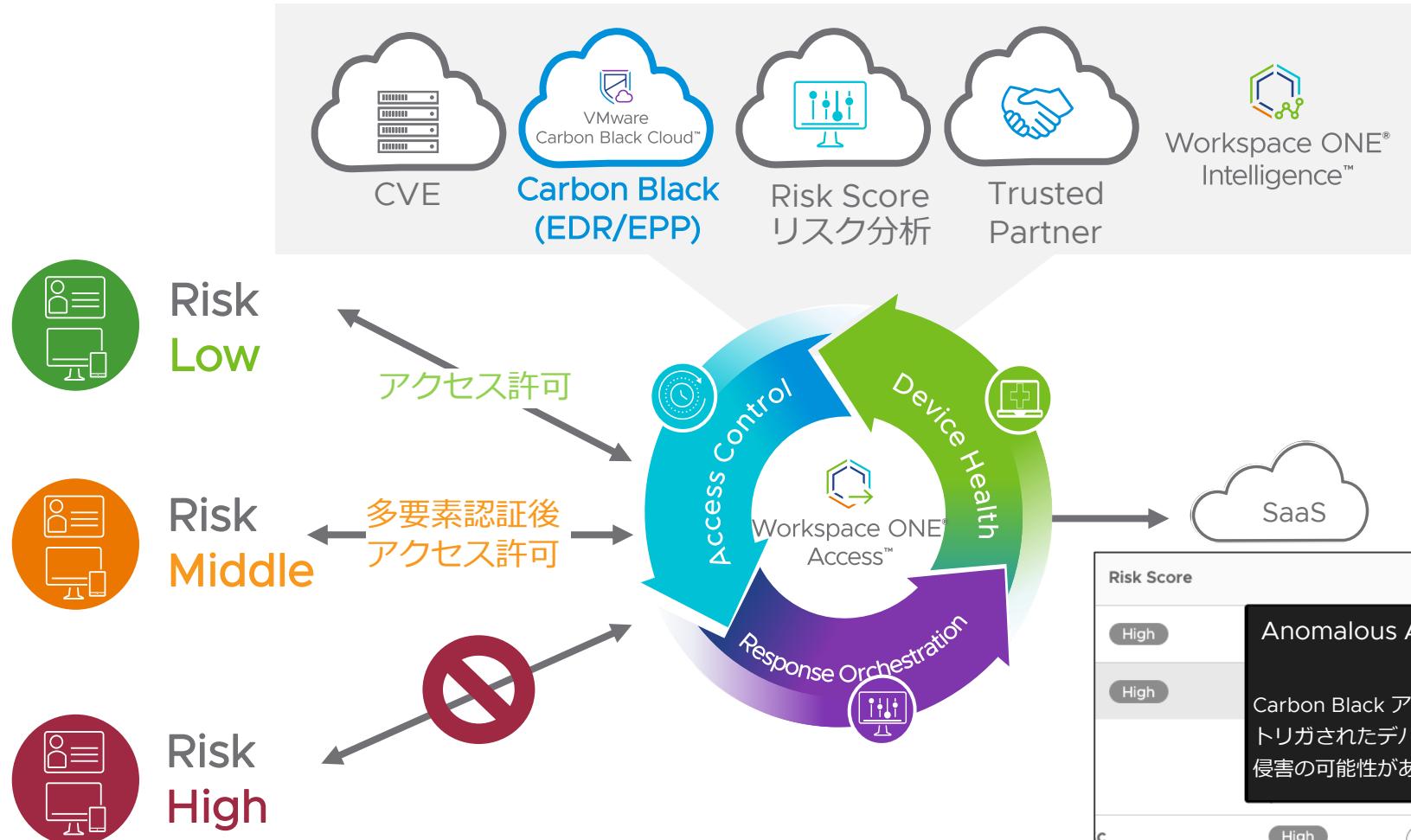
CB から連携される脅威イベントをダッシュボード・レポートで可視化しインサイトを提供



- デバイス管理者とセキュリティ管理者が共通のダッシュボードを利用するによる連携強化・コミュニケーションの効率化を実現
 - ある脅威への対策の進捗状況を履歴グラフにより簡単に可視化

3. リスクスコアによるアクセス制御

Carbon Black の脅威レポートを基にした SaaS へのアクセス制御



- Carbon Black の脅威レポートを基にしたアクセス制御の実現
 - リスクスコアに基づくアクセス許可 / 追加認証の要求 / アクセス拒否の実現

Risk Score

High	Anomalous Alert Activity
High	Carbon Black アラート数、タイプ、重要度の異常によってトリガされたデバイス。異常なアラートアクティビティは、侵害の可能性があるデバイスがあることを意味します。

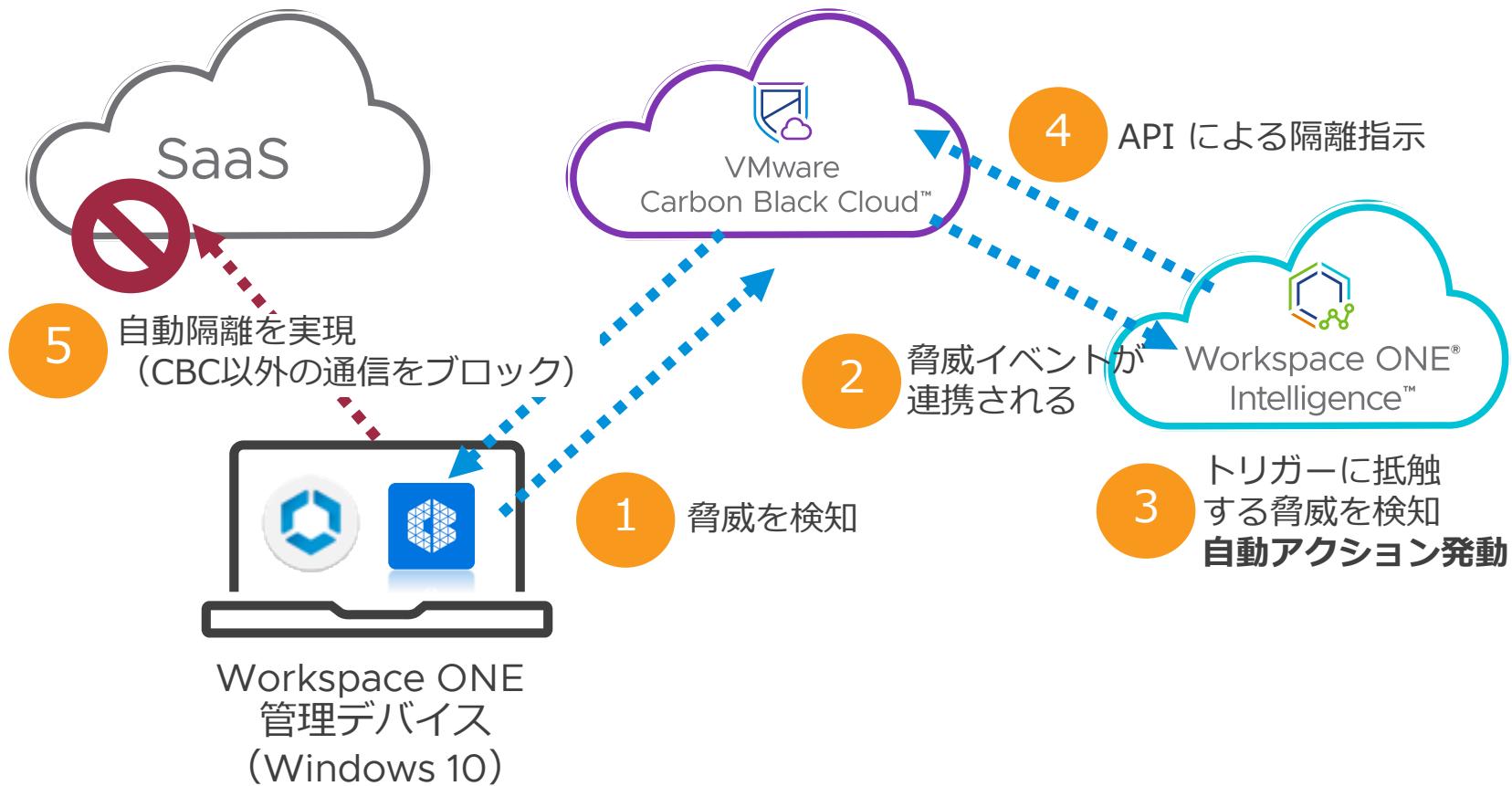
プラットフォーム

c High Anomalous Alert Activity Laggard Update Windows Desktop +1

Workspace ONE Intelligence レポート画面の抜粋

4. 脅威検出時の自動隔離

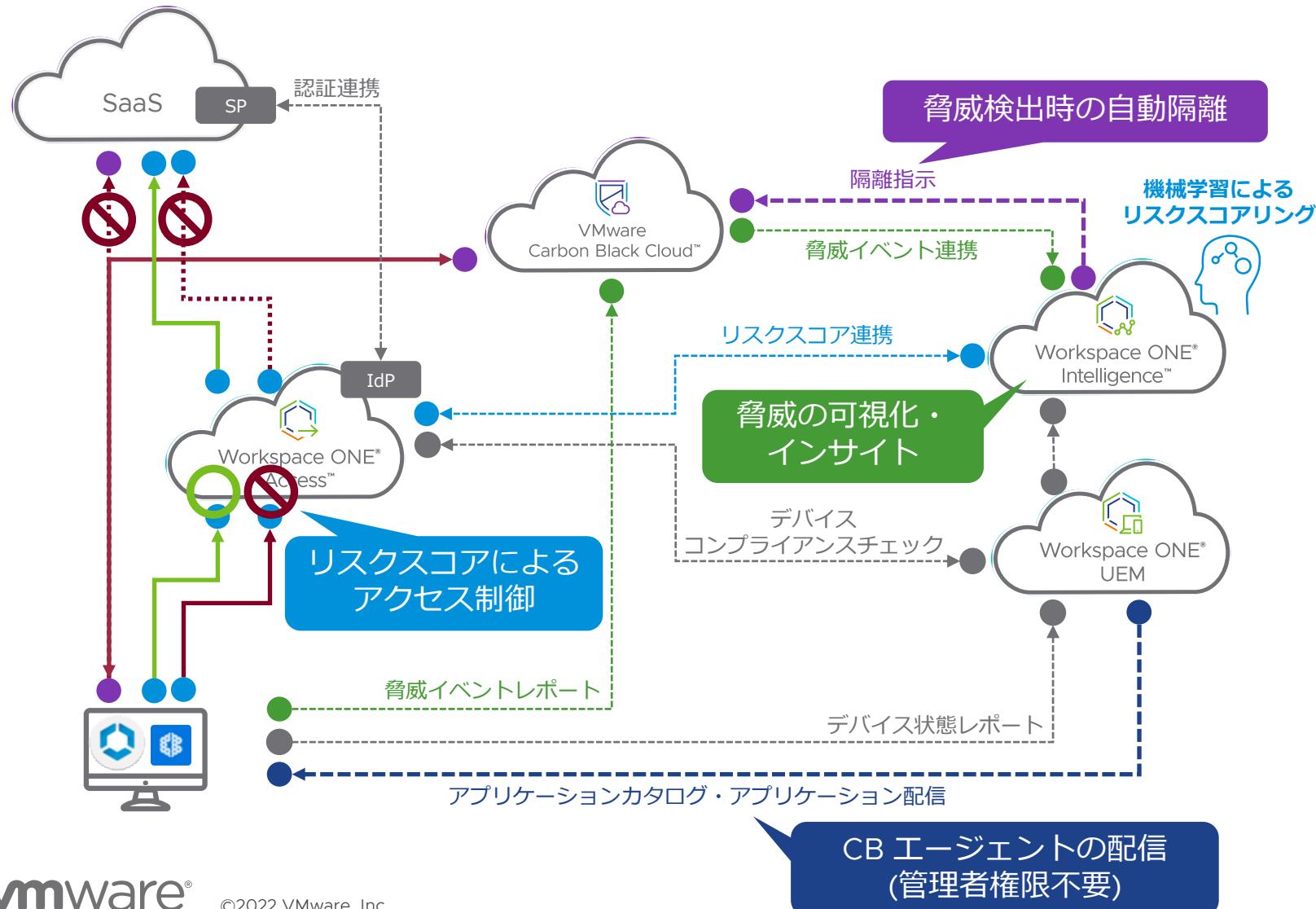
セキュリティインシデントへの自動対応



- 自動化でセキュリティ インシデントへの迅速な 対応を実現
- 自動化によるセキュリ ティチームの運用負荷 軽減
- 調査/事後対応のため 端末と CBC 通信のみを 実現

Workspace ONE x Carbon Black 連携シナジー

最新の脅威に対するセキュリティを強化



1. CB エージェントの配信

PC の管理者権限の剥奪を実現しながら、業務に必要なアプリケーションのインストールを実現

2. 脅威の可視化・インサイト

CB から連携される脅威イベントをダッシュボード・レポートで可視化しインサイトを提供

3. リスクスコアによるアクセス制御

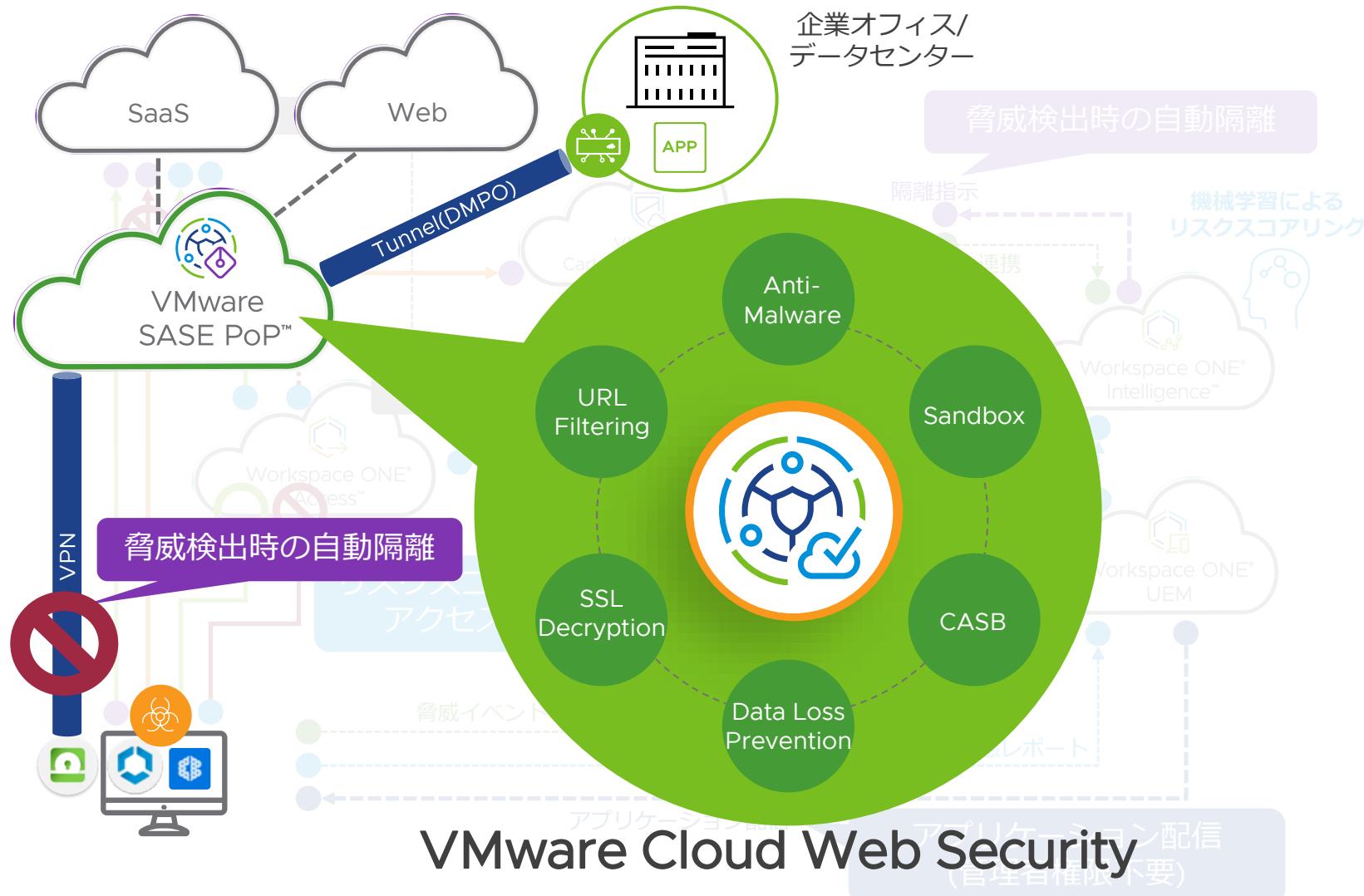
WS1 Intelligence で CB の脅威イベントやデバイスのセキュリティ状態を基にリスクスコアを算出し、WS1 Access がリスクスコアに基づくアクセス制御を実現

4. 脅威検出時の自動隔離

脅威を検出した際に端末の自動隔離を実現し、SOC チームの安全性を確認後に隔離を解除（調査のための端末と CBC のみ接続実現）

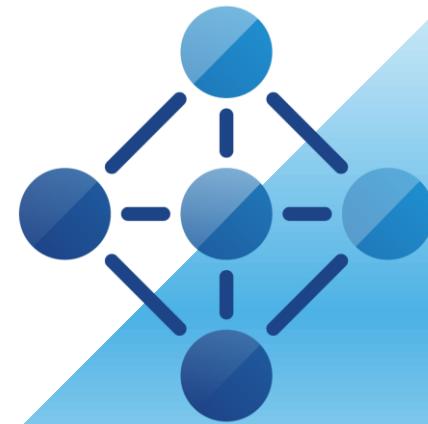
VMware SASE x Workspace ONE x Carbon Black

SaaS/Webトラフィックに対するセキュリティ対策も提供



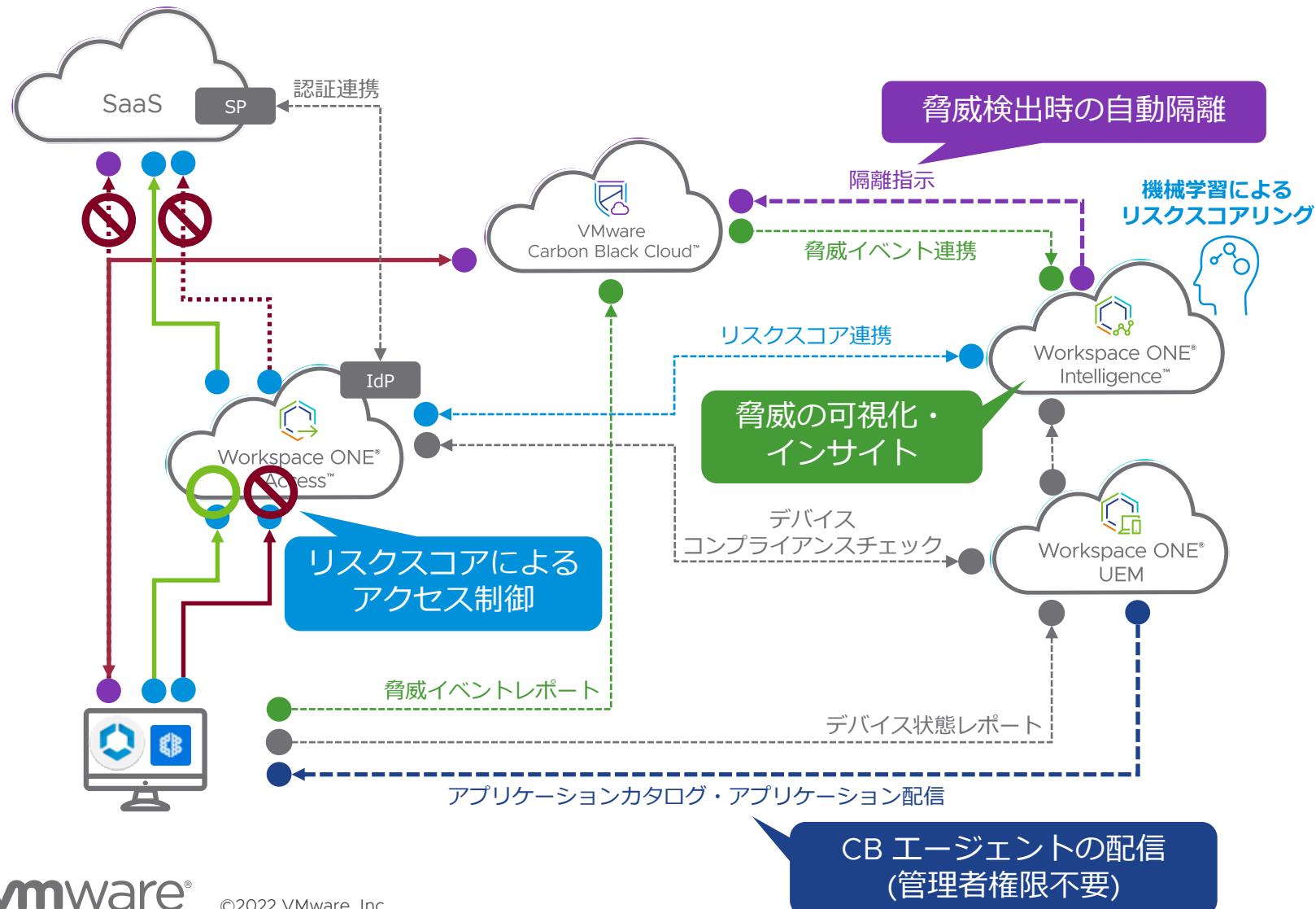
- 既知の脅威からの保護
- ゼロデイ脅威からの保護
- SaaS でのユーザーアクションの可視性と制御
- 意図しない情報漏洩による企業損失を保護
- SSL / TLS トラフィックを復号化し検査
- マルウェア、情報剽窃など Web 脅威からの保護

まとめ



Workspace ONE x Carbon Black 連携シナジー

最新の脅威に対するセキュリティを強化



1. CB エージェントの配信

PC の管理者権限の剥奪を実現しながら、業務に必要なアプリケーションのインストールを実現

2. 脅威の可視化・インサイト

CB から連携される脅威イベントをダッシュボード・レポートで可視化しインサイトを提供

3. リスクスコアによるアクセス制御

WS1 Intelligence で CB の脅威イベントやデバイスのセキュリティ状態を基にリスクスコアを算出し、WS1 Access がリスクスコアに基づくアクセス制御を実現

4. 脅威検出時の自動隔離

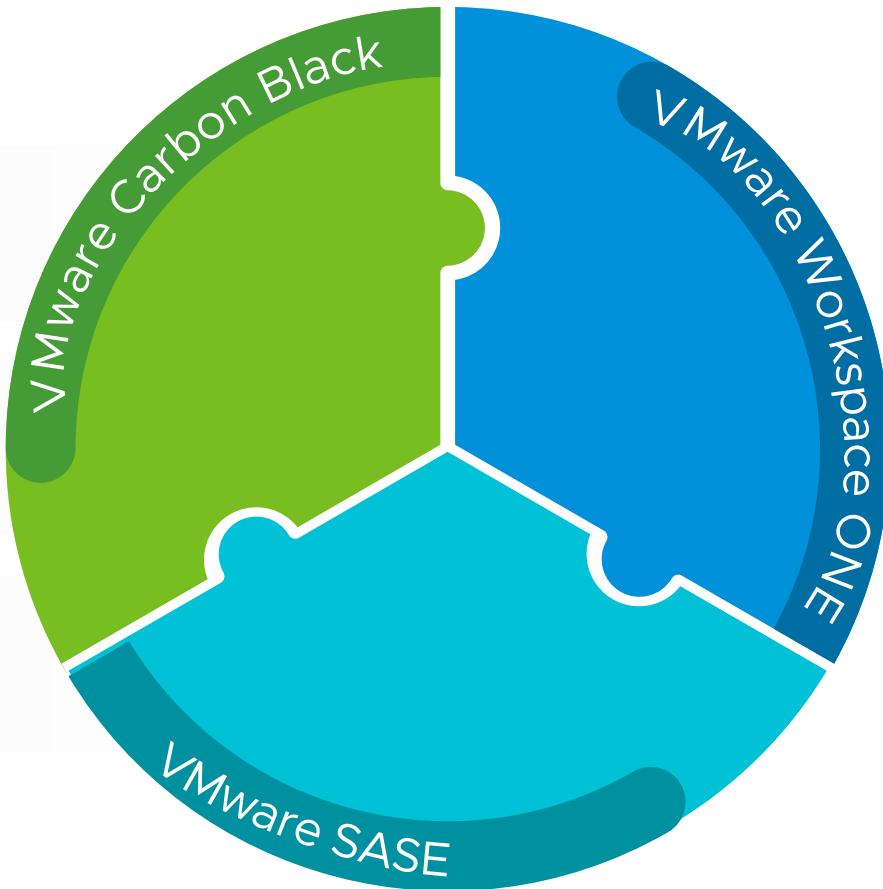
脅威を検出した際に端末の自動隔離を実現し、SOC チームの安全性を確認後に隔離を解除（調査のための端末と CBC のみ接続実現）

Anywhere Workspace が備える優れたテクノロジー

多様な
従業員体験の管理

分散化された
エッジの保護

ワークスペースの
自動化



VMware Carbon Black®

クラウドネイティブな
エンドポイントの保護

VMware Workspace ONE®

統合エンドポイント管理および
仮想アプリ/デスクトップの提供

VMware SASE™

ゼロトラストセキュリティと
ネットワークパフォーマンスの管理

IT、ネットワーク、セキュリティを網羅する統合テクノロジー



Thank You