



オンプレよりもセキュアに！ GCVE ができるセキュリティ強化 ～その対策方法とは

屋良 旦

ヴィエムウェア株式会社 クラウドサービス技術統括部
スタッフクラウドソリューションアーキテクト

スピーカー自己紹介



屋良 旦

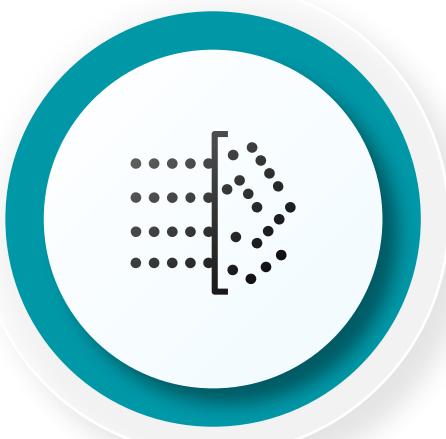
ヴイエムウェア株式会社
クラウドサービス技術統括部
スタッフクラウドソリューションアーキテクト

2013 年に VMware へ入社、プリセールス エンジニアとして、仮想化を軸にしつつ、黎明期の NSX や vSAN のお客様への導入を支援。現在はソリューション アーキテクトとして、VMware を活用頂いているクラウド プロバイダー様の新たなクラウド サービスの支援や、既存サービスのよろず相談窓口として日々活動中。

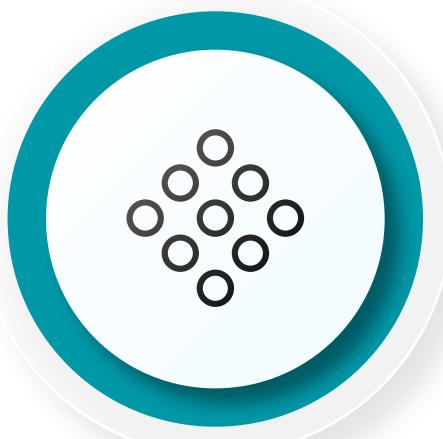
アジェンダ

- 昨今のセキュリティ課題
- Google Cloud VMware Engine ができるセキュリティ強化
 - ネットワークからのアプローチ
 - エンドポイントからのアプローチ
- まとめ

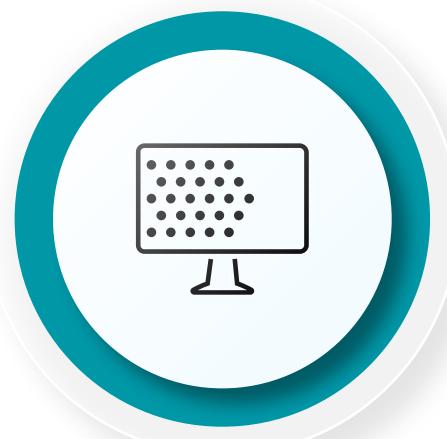
昨今のセキュリティ課題



攻撃対象範囲の
急増



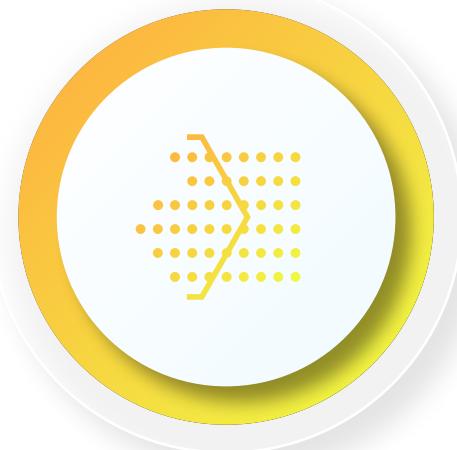
多くのツールによる
運用と組織の
サイロ化



コンテキストの
欠如

VMware Security Vision: セキュリティをシンプルに

より簡単に



セキュリティを
ビルトインの分散型
サービスとして提供

より迅速に



連携によりツールと
サイロを削減し
ゼロトラストを実現

より賢く



脅威インテリジェンス
とインフラのデータを
もとに迅速かつ正確に
対応



Google Cloud VMware Engine ができるセキュリティ強化 - ネットワークからのアプローチ -

Google Cloud VMware Engine(GCVE)の概要

既存の vSphere 環境を手軽にクラウド化

移行の障壁が低い

vSphere 基盤上のワークロードを現行のままクラウド
に移行

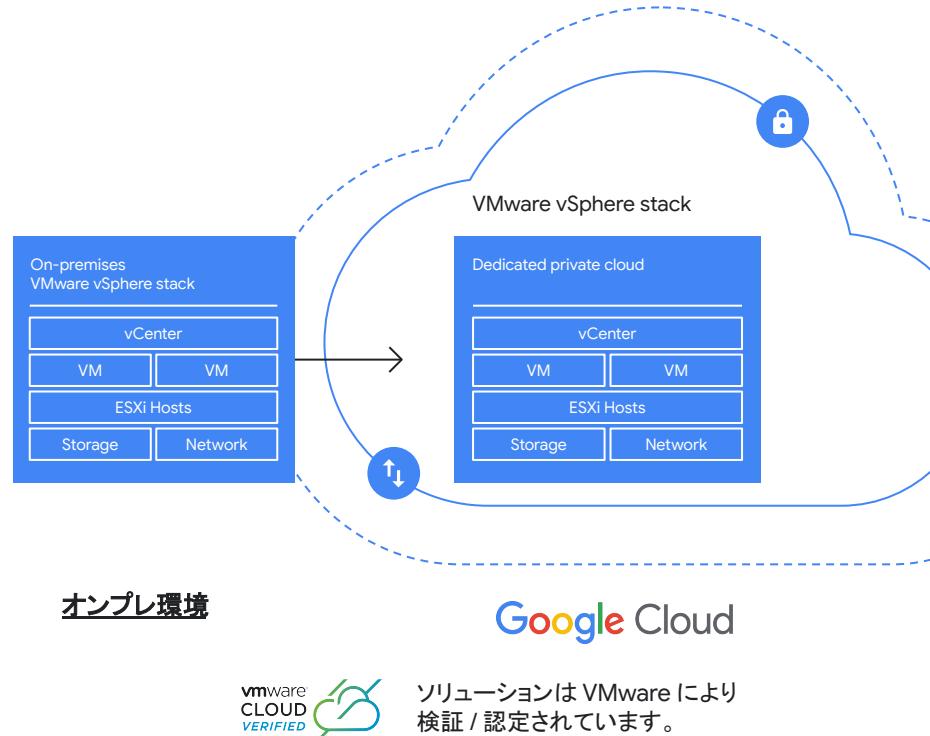
簡単にアプリの移行とオペレーションの継続が可能

TCO 削減

Google がマネージする VMware ソリューションと
ハードウェアを利用することで TCO を削減

Google Cloud の別プロダクトとの連携

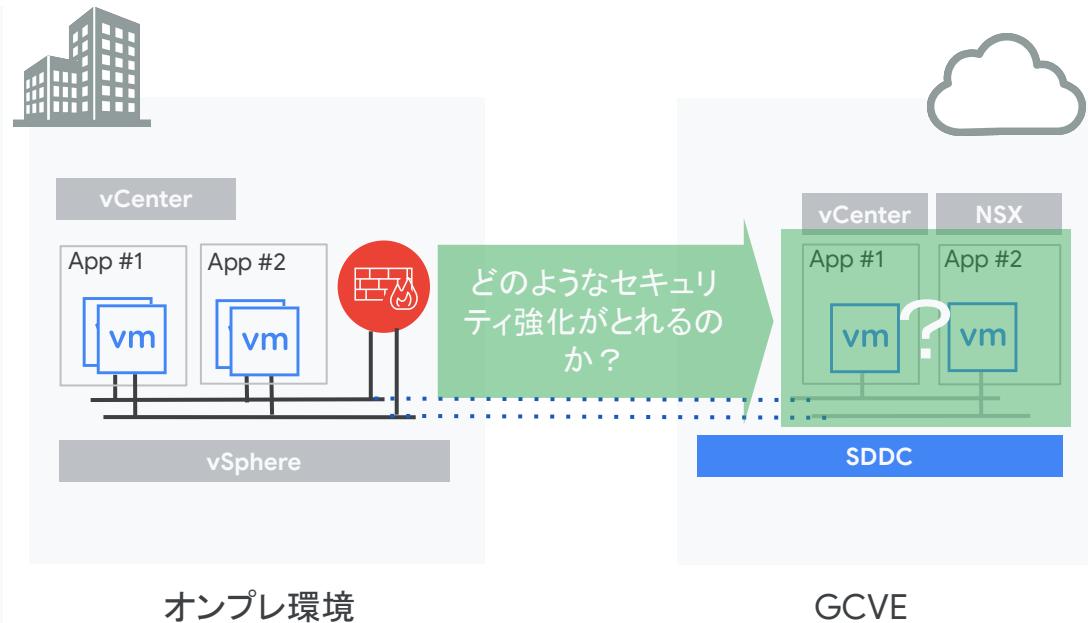
Google Cloud ネイティブ サービスとの統合や、
自動化によるベネフィットを享受



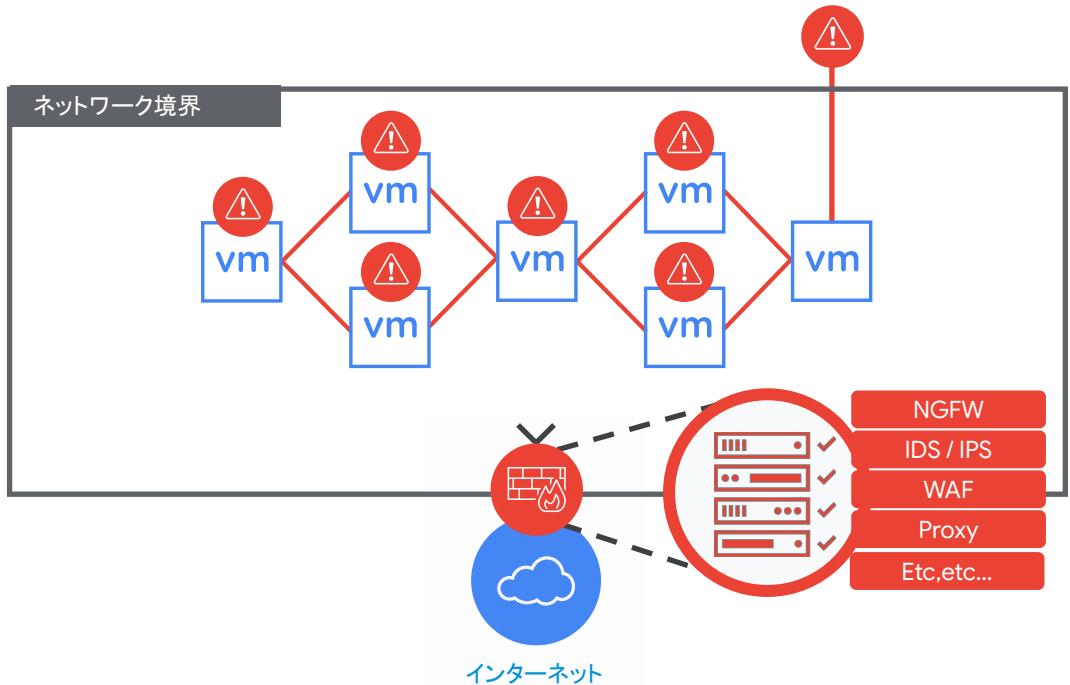
シナリオ 1: オンプレ環境のワークロードを移行するだけで実現可能なセキュリティ強化

オンプレ環境の課題例

- ・ ワークロード間のアクセス制御するには
セグメント分けが必要
- ・ ワークロード追加/変更の度にファイアウォー
ルの設定変更が発生
- ・ ワークロードが塩漬けになっており、
十分なセキュリティ対策が取れていない
オンプレ環境
- ・ ファイヤウォールには物理アプライアンスを
利用



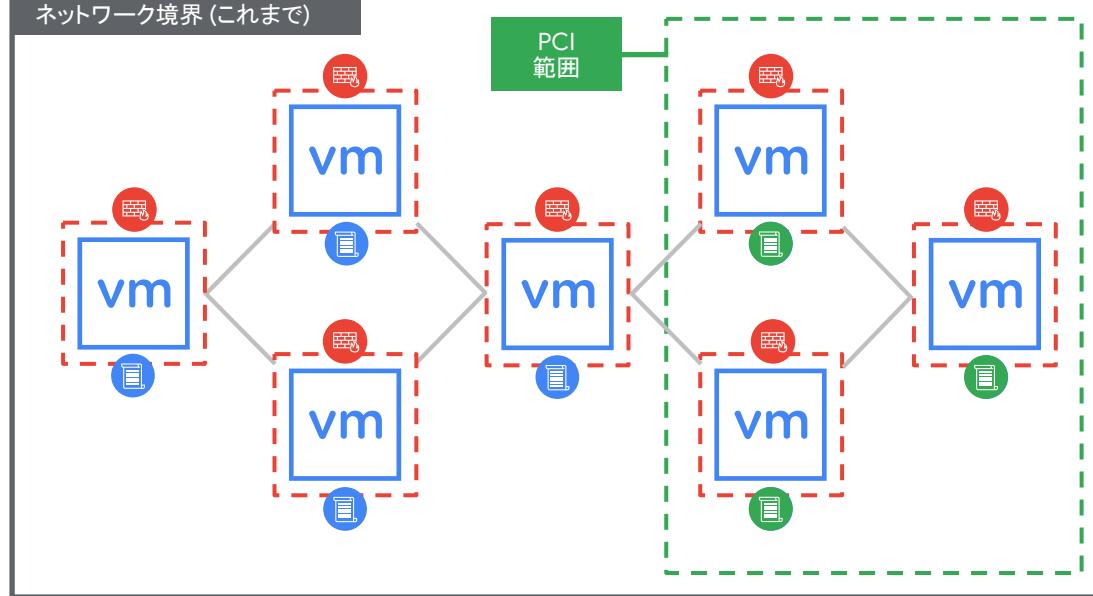
これまでの境界型セキュリティの現実



- ・ 攻撃が一旦境界防御を超えると、それ以降拡散を防止する手立てがない
- ・ 低いプライオリティのシステムが最初のターゲットに
- ・ 攻撃者は一度侵入してしまえば自由に行動を開始することが可能
- ・ 攻撃者はやがて内部情報を入手し目的を達成

GCVE に組み込み済みのネットワーク セキュリティ： 分散ファイアウォール

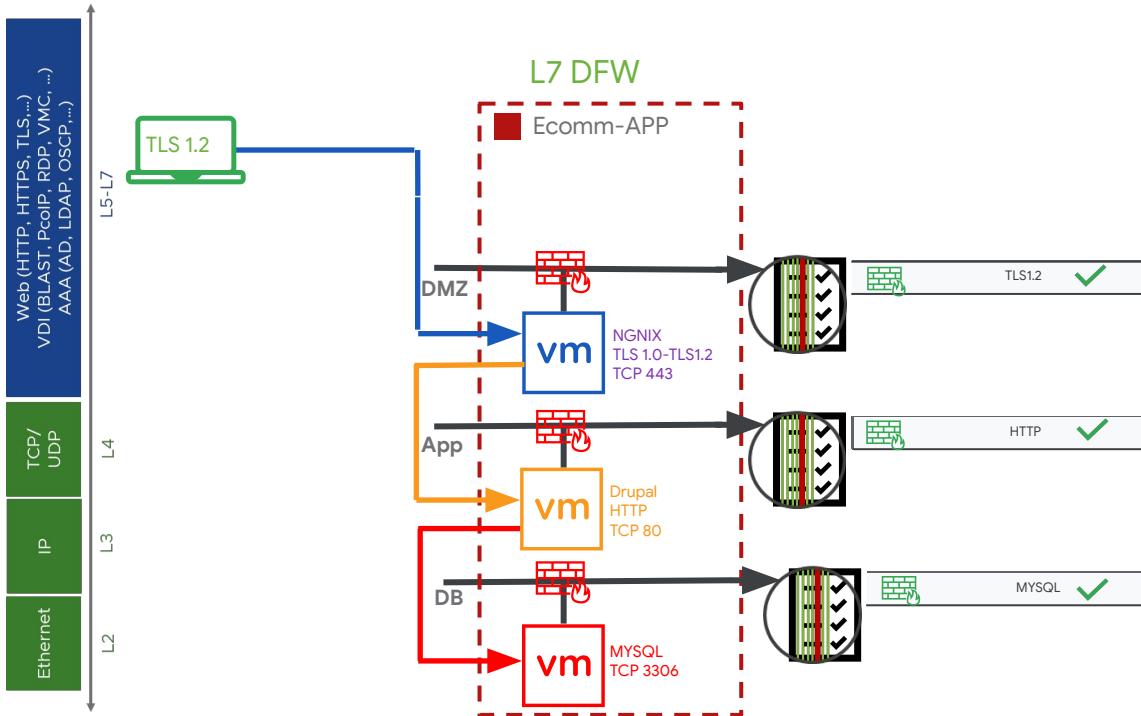
ワークロードを GCVE 上で稼働させるだけでセキュリティ強化を実現



- GCVE に組み込まれた分散ファイアウォール
 - セグメントに縛られず、仮想マシン (vNIC) 単位でのセキュリティ ポリシーを設定可能
- セキュリティポリシーはコンテキストをもとに定義することが可能
 - VM 属性・NW 属性・アプリ属性
 - ワークロードの追加時に自動的に適用することも可能

GCVE に組み込み済みのネットワークセキュリティ： 分散ファイアウォール

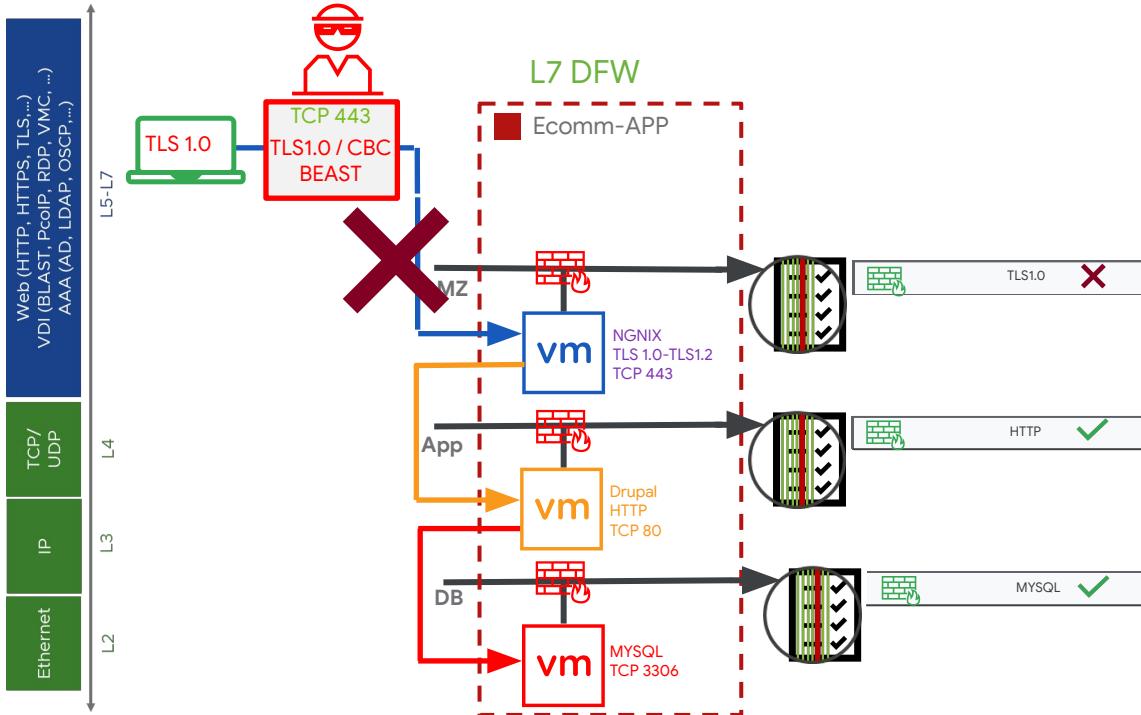
アプリケーションを意識したファイアウォール



- ・ **アプリケーション識別によるアクセス制御**
 - App-ID によるアプリケーション識別で Well-known Port であっても不適切なアクセスを排除
 - 脆弱性対応ができないないワークロードへのアクセス強化(例: TLS1.0 のブロック等)

GCVE に組み込み済みのネットワークセキュリティ： 分散ファイアウォール

アプリケーションを意識したファイアウォール

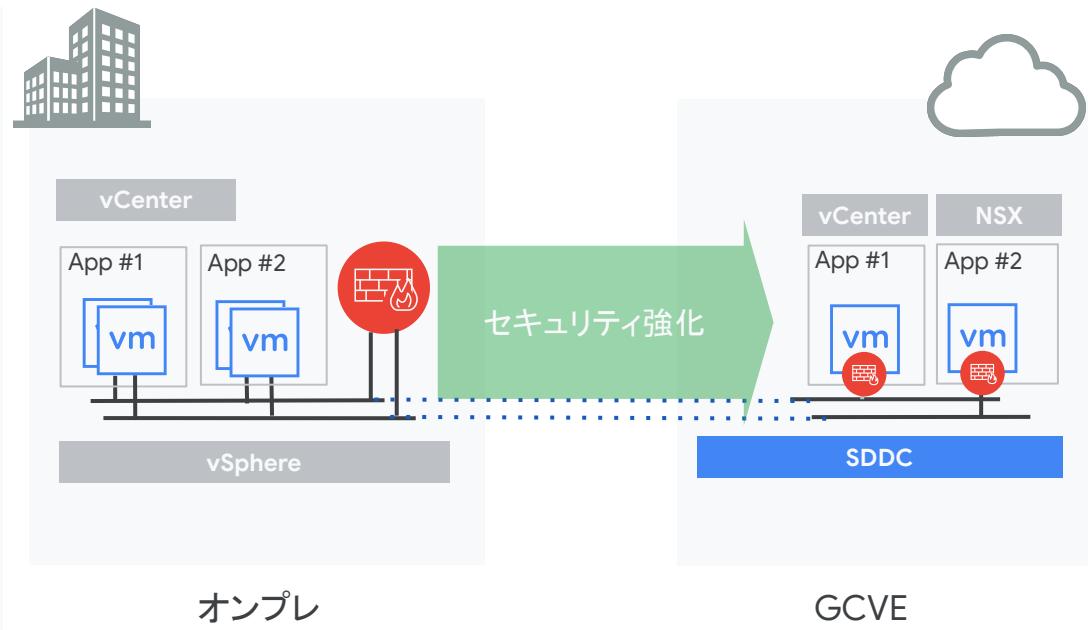


- **アプリケーション識別によるアクセス制御**
 - App-ID によるアプリケーション識別で Well-known Port であっても不適切なアクセスを排除
 - 脆弱性対応ができないないワークロードへのアクセス強化(例: TLS1.0 のブロック等)

シナリオ 1: オンプレ環境のワークロードを移行するだけで実現可能なセキュリティ強化(再掲)

オンプレ環境の課題例

- 分散ファイアウォールを活用することで、
- セグメントに縛られず、仮想マシン単位での制御が可能
- ワークロード追加時も、セキュリティポリシーを適用することで都度のルール作成が不要
- 塩漬けのワークロードに対して手を加えずにセキュリティ強化可能





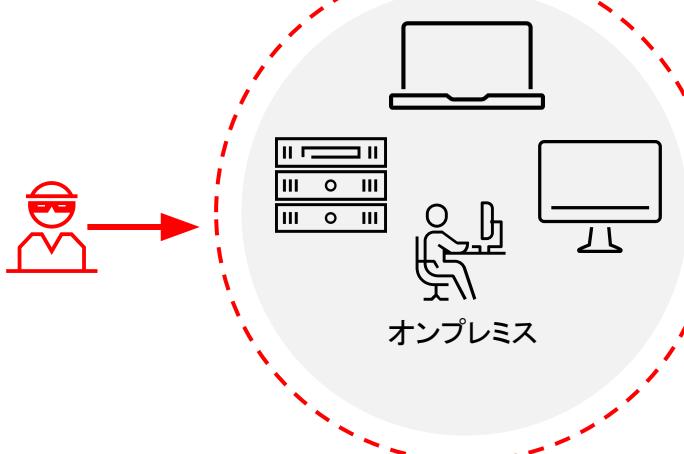
Google Cloud VMware Engine ができるセキュリティ強化 - エンドポイントからのアプローチ -

変革の進む IT 環境

エンドポイントのセキュリティはますます重要に

以前

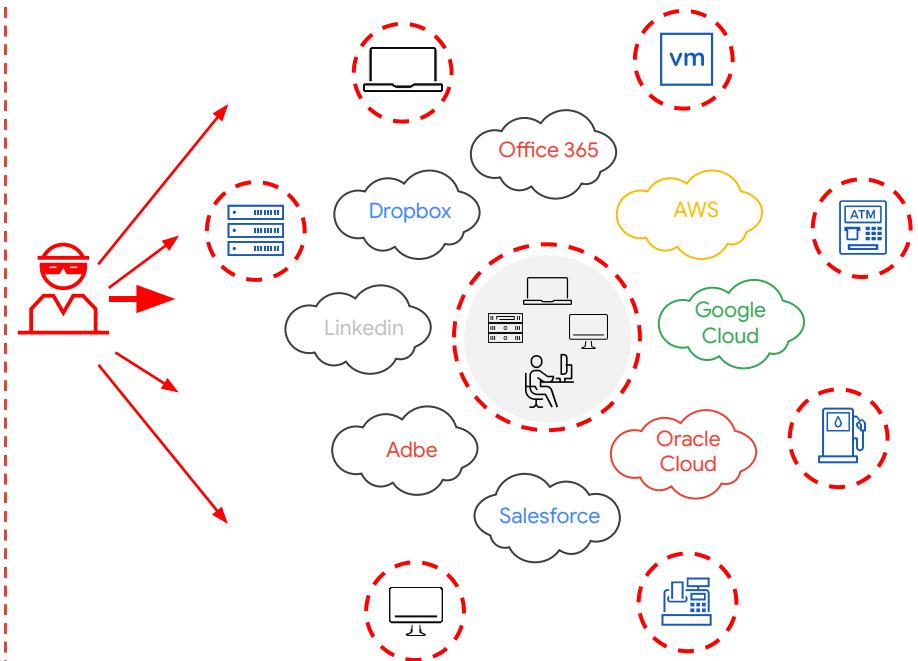
ネットワーク製品が境界



オンプレミス

今日

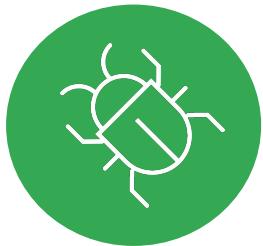
エンドポイントが境界



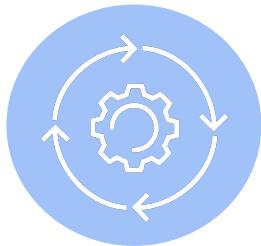
Google Cloud

こんな課題を抱えていませんか？

悩みの尽きないエンド ポイント セキュリティ対策



もはや効果的
ではない防御策
アンチウイルス製品のみ
で昨今の脅威に対抗で
きていますか



多すぎる
セキュリティ製品
複数製品の導入により
端末への負荷や管理
工数が肥大化していま
せんか



それでも
足りない情報
導入済の製品が集めた
情報で自信を持った
判断をできていますか

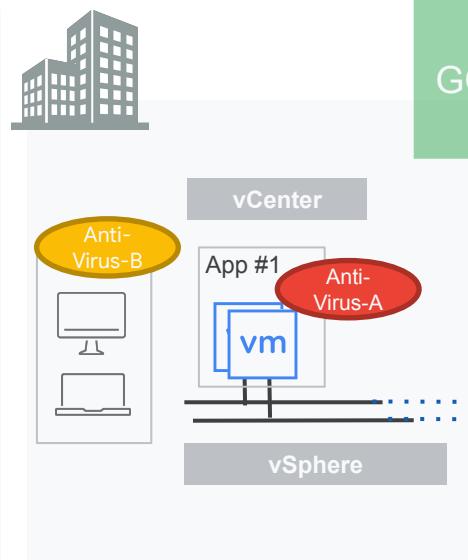


分からず
利用状況
利用形態はユーザ任せで
社内に存在するリスクを放
置していませんか

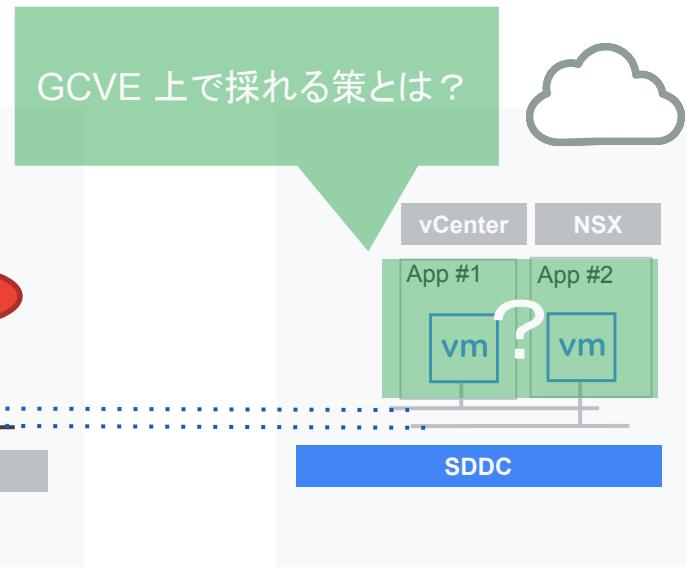
シナリオ 2: エンドポイントのセキュリティ強化

オンプレ環境の課題例

- 仮想基盤のワークロードとユーザ端末で異なるセキュリティツールを利用
- エンドポイント及びサーバセキュリティ対策はウイルス対策に限定、EDRソリューションも検討中



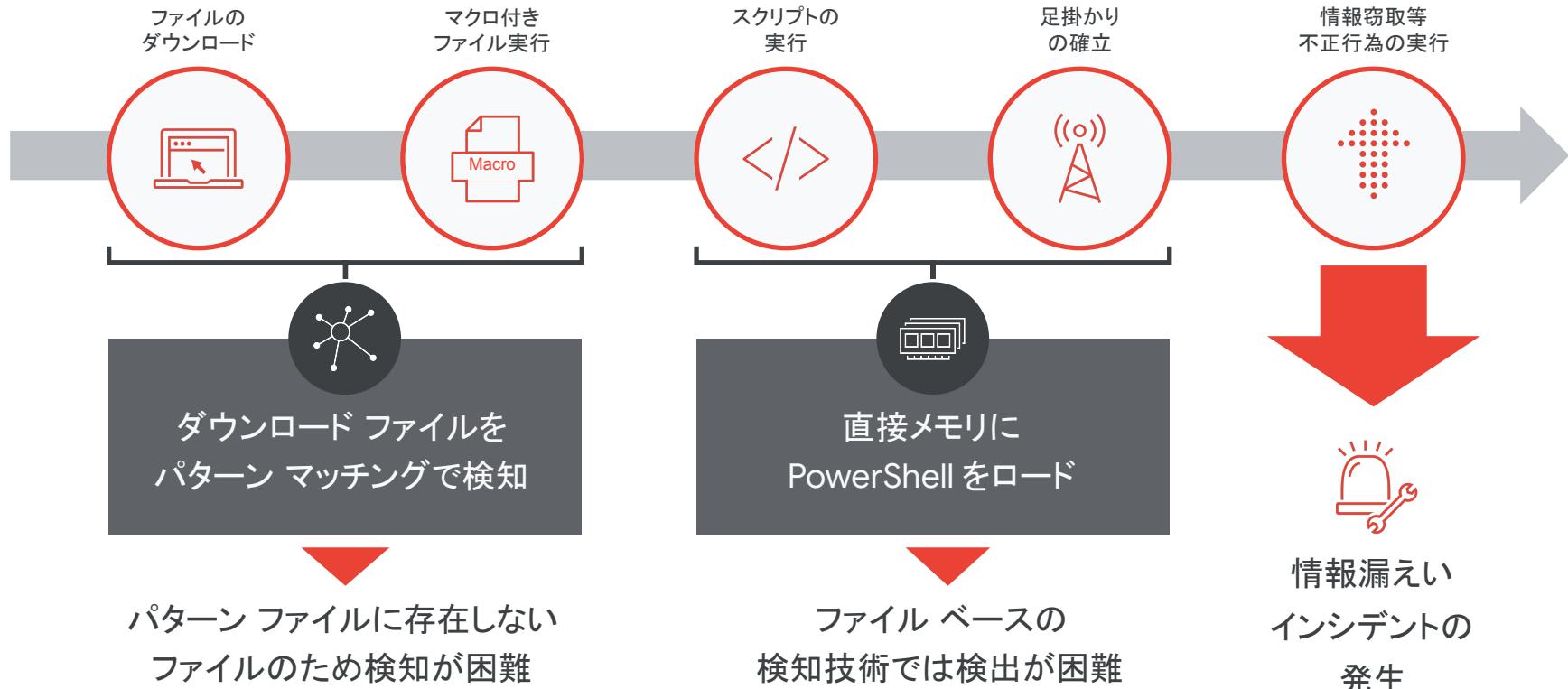
オンプレ



GCVE

従来のウイルス対策ソリューションの課題

例: ファイルレス攻撃への対応が不十分



VMware Carbon Black Cloud

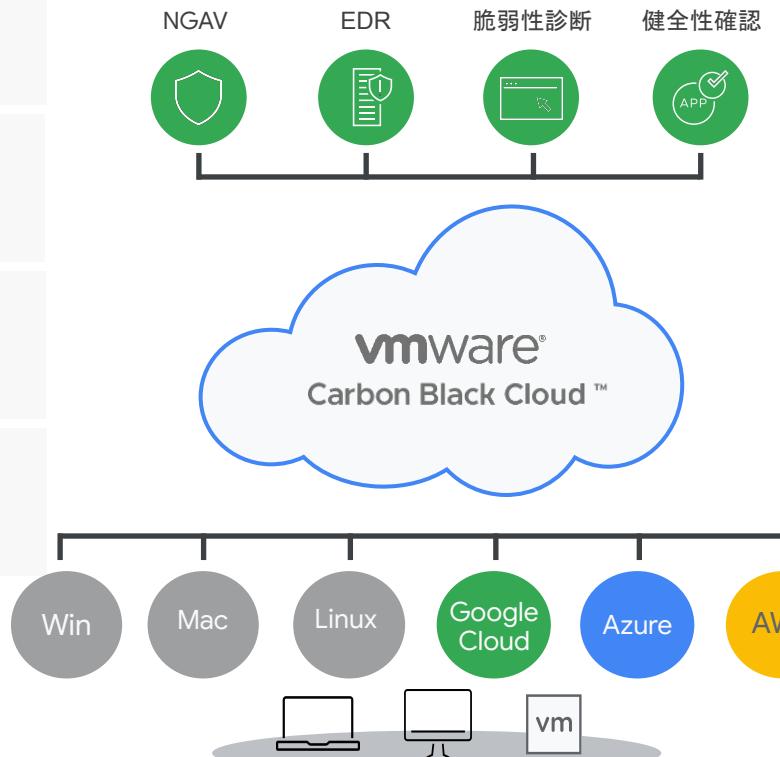
特徴・強み

シングル エージェント
シングル コンソール

オンプレ サーバー不要
完全クラウド

日本語 UI
データセンターは日本

直感的な管理コンソール



全ログ保存

全てのプロセスをクラウド保存
脅威検出に利用

センサーはカーネルモードで動作

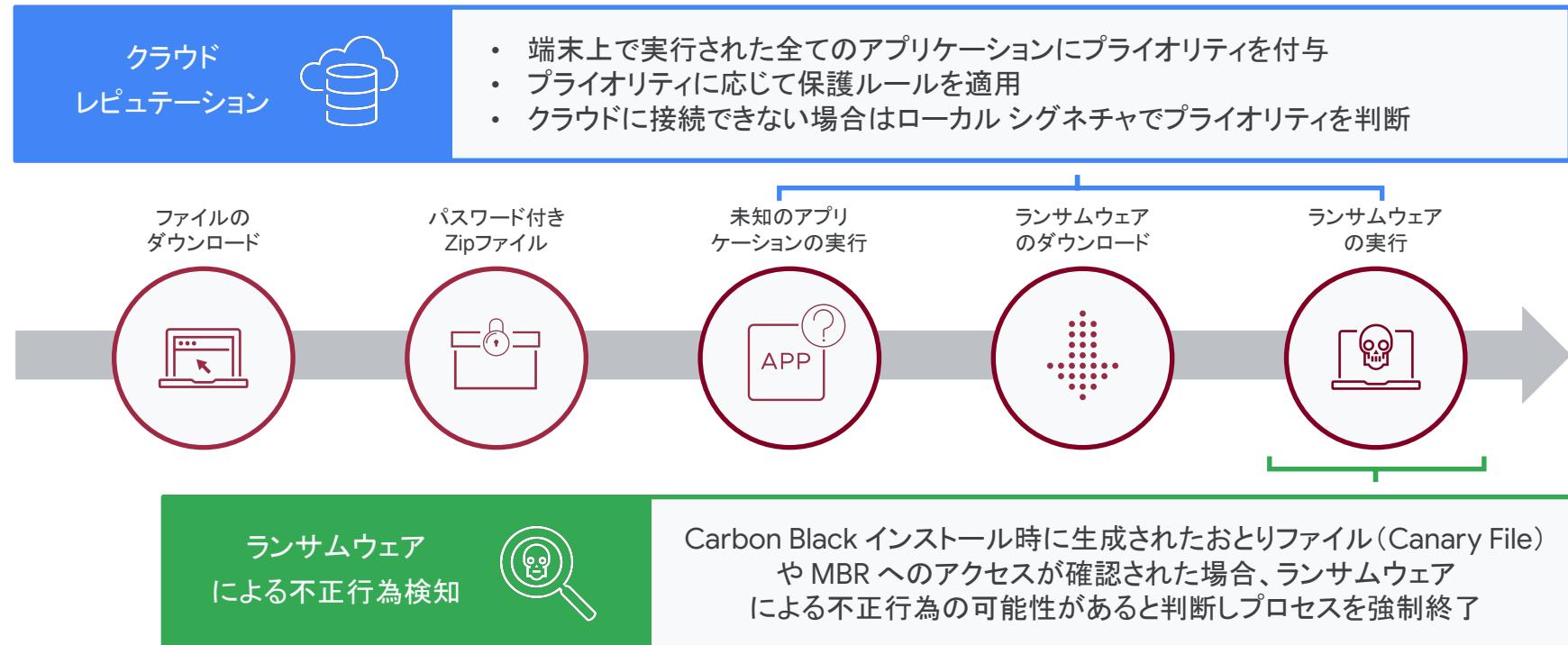
豊富な API

ログのエクスポート
他製品との連携

各種 VMware 製品との連携
Horizon サポート等

Carbon Black Cloud の活用 : NGAV 機能

パターン ファイル未対応の未知の不正プログラムにも対応



クラウド レビューションによる不明なアプリの動作制御

ランサムウェアによる不正行為検知と組み合わせた制御を実現



リモートで隔離・削除・復旧

管理コンソールから「より簡単に」操作

2 results

ステータス	最初の認... ▾ 理由	デバイス
□	10:37:01 午前 8月 14, 2021 A known virus (Malware: EICAR) was detected.	3 user01 fujitat-w10d03 >
□	適用されたポリシー実行しました	5 user01 fujitat-w10d03 >

Group alerts On

2 件中 1-2 件を表示 中 ページあたりのアイテム数 20 次のページにジャンプ # < 1 >

復旧

潜在的な次のステップ

アプリケーションを削除
ユーザーのデバイスから 275a0...1fd0f を削除する

アセットの隔離
ネットワーク上の fujitat-w10d03 を分離してリスクを低減する

Live Response
fujitat-w10d03 のリモート調査を実行

非表示 ▾

ハッシュが信頼できない場合

ファイルを調査する
VirusTotal の 275a0...1fd0f の分析を表示する

ハッシュを禁止リストに追加
275a0...1fd0f のレビューと信頼できないとして指定

アップロードをリクエスト
後で調査するために 275a0...1fd0f を保存する

ハッシュが信頼できる場合

ハッシュを承認リストに追加
275a0...1fd0f のレビューと信頼できるとして指定

ポリシーの調整
fujitat - Advanced 01 ポリシーのルールを更新して誤検出を削減する

削除

隔離

ライブ状態に移行

表示

追加

アップロード

追加

ポリシーの表示

検知された不正プログラムを削除



検知された端末をネットワークから隔離



検知された端末をリモート操作・復旧



もう一步先のエンド ポイント セキュリティ対策へ

侵入を前提とした対策 – EDR ソリューションの検討



見慣れない IP アドレスに
対して頻繁に通信が発生
しているのですが…

本当ですか？！
すぐに調べなければ！



ファイルの
ダウンロード

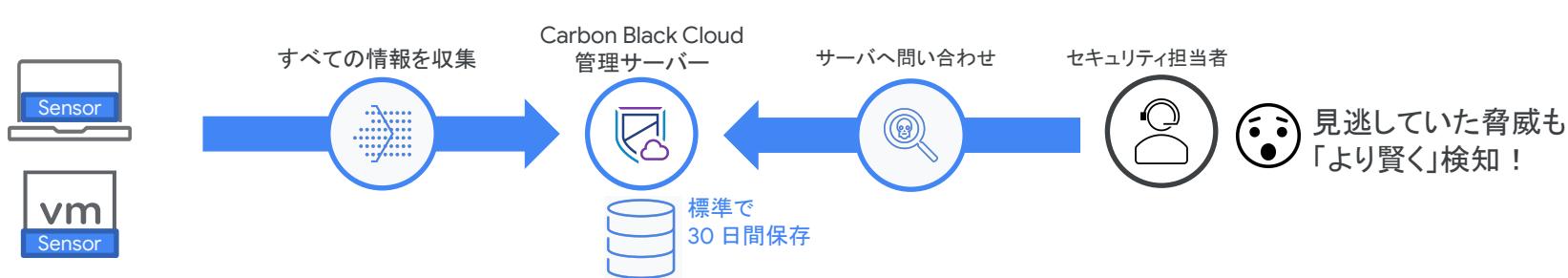
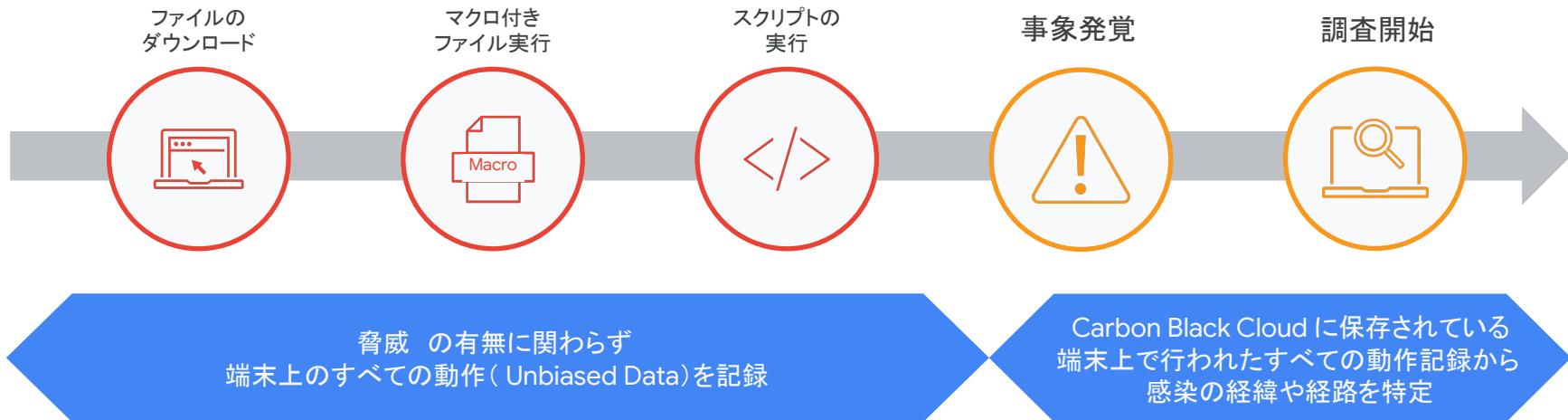
マクロ付き
ファイル実行

スクリプトの
実行

足掛かりの確立・
情報収集



動作の可視化と迅速な脅威の調査・特定を実現 : EDR 機能





脆弱性診断

OS および導入アプリケーションの脆弱性評価

脆弱性評価の結果に基づいて優先的に対応することでインシデントの再発を抑止

脆弱性
展開されたアセットで検出されたセキュリティの脆弱性を確認 [詳細を表示](#)

エンドポイント

状態	数	説明
6,134	9	全体的な脆弱性 監視対象のエンドポイント
すべて	4,117	4,117 台の製品の脆弱性 9 個のエンドポイント
クリティカル	7	7 台の製品の脆弱性 5 個のエンドポイント
重要	41	41 台の製品の脆弱性 9 個のエンドポイント
中	197	197 台の製品の脆弱性 9 個のエンドポイント
低	3,872	3,872 9 個のエンドポイント

すべて の 製品の脆弱性

オペレーティングシステム	数
Windows OS	2,060
Linux OS	1,212
Windows アプリケーション	324
Linux アプリケーション	521

影響を受けるエンドポイント

オペレーティングシステム	数
Windows	4
Linux	5

リスク評価

名前	リスク
CBSTD-WKSH	クリティカル (10)
CBSTD-WKSH2	クリティカル (10)
CBSTD-LQWIN7	クリティカル (10)

9 件中 1-9 件を表示中

リスクの評価

NIST

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

≡ NVD MENU

NVD

VULNERABILITIES

CVE-2021-21220 Detail

Current Description

Insufficient validation of untrusted input in V8 in Google Chrome prior to 89.0.4389.128 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

[View Analysis Description](#)

Severity

[CVSS Version 3.x](#)
[CVSS Version 2.0](#)

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: 8.9 HIGH

Vector:

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis.
The CNA has not provided a score within the CVE List.

出典:

<https://nvd.nist.gov/vuln/detail/CVE-2021-21220>

Google Cloud



強力な検索機能によるコンプライアンス チェックへの活用

健全性確認

- 使用履歴のある USB のリスト化

コンプライアンス

USB Devices on Linux/macOS

Schedule 実行

説明: Discover how many USB devices are attached to the operating system.

結果: Lists all USB devices that are attached to a Linux or macOS system.

Carbon Black recommends that you run this query as needed

+

Apple logo

- BitLocker の設定の確認

コンプライアンス

BitLocker Configuration Details

Schedule 実行

説明: Bitlocker is a Windows feature that encrypts your volume drive.

結果: Details on the BitLocker status for target systems, such as device ID, conversion status, and encryption method.

Carbon Black recommends that you run this query weekly

+

Windows logo

- リモートデスクトップの設定確認

コンプライアンス

Verify RDP Status

Schedule 実行

説明: Remote Desktop Protocol (RDP) can remotely access Windows systems. CB recommends auditing and limiting RDP capabilities to reduce possible malicious access. 詳細を表示: <https://attack.mitre.org/techniques/T1076/>

結果: If there are active connections, returns 0 if RDP is enabled, or 1 if disabled. Includes metadata such as process ID and open sockets.

Carbon Black recommends that you run this query as needed

+

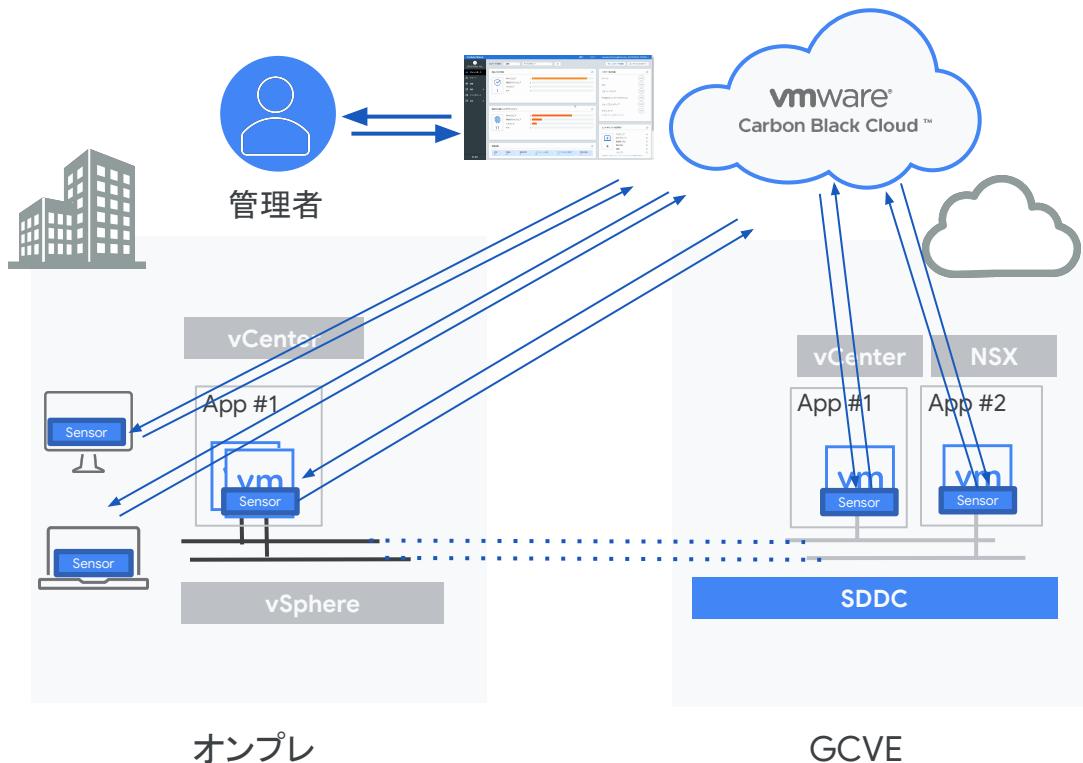
Windows logo

シナリオ 2：エンドポイントのセキュリティ強化(再掲)

オンプレ環境の課題例

Carbon Black Cloud を活用することで、

- GCVE 上のワークロードはもちろんのこと、ユーザ端末も一元的に管理可能
- 同じエージェントでウイルス対策からEDRまで幅広く対応
- 将来的に機能追加したい場合もエージェント(Sensor)の入れ替え不要



まとめ

- GCVE に組み込み済みの分散ファイア ウォールを活用したセキュリティ強化
 - GCVE 上であればすぐに利用可能なソリューション
 - セキュリティ ポリシーの自動適用により、運用の効率化
 - ワークロードに手を加えずにセキュリティ強化を実現
- GCVE 上のワークロードに対するエンド ポイント セキュリティ強化
 - GCVE 上のワークロードに加え、ユーザ端末をも含めた一元的な管理を実現
 - シングル エージェントでさまざまなセキュリティ機能をサポート
 - 将来を見据えた機能追加にも柔軟に対応

Thank you.

