デジタルテクノロジー株式会社

VMware Workspace ONE® & VMware Carbon Black®

まずはエンドポイントセキュリティの強化を! そのための基盤としておすすめしたい

ランサムウェアの脅威が増大するなど、
高まり続けているサイバー攻撃の被害リスク。
近年はテレワークに使用する端末が侵入の標的になることも増えており、
そこを踏み台にして企業ネットワーク全体に
脅威が拡大する危険性も高まっています。
また従業員が使用する端末が社外に持ち出された結果、
管理が行き届かないケースも。

例えば貴社のIT部門は、次のような不安を抱えていませんか?

テレワーク端末が実際にどう使われているのかわからない…

社外に持ち出された端末は、管理者の目から離れた場所で使われることになるため、その利用状況を把握することは簡単ではありません。そのため管理者の見えないところで、不適切な利用が行われる可能性も考えられます。例えばリテラシーが十分でない従業員が不正サイトにアクセスすれば、そこからマルウェアが感染する危険性も。また端末が紛失・盗難された場合には、悪意のある第三者によって端末の情報が漏洩することも考えられます。

アプリやSaaSの不適切な利用で情報漏洩しているかも…

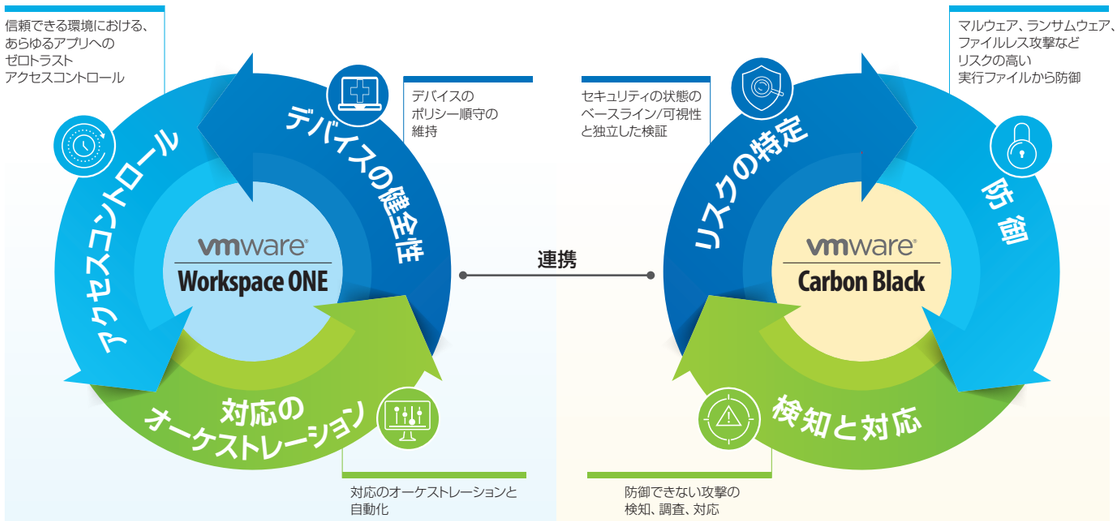
ユーザーが自由にアプリケーションをインストールできる場合や、クラウドストレージなどのSaaSの利用が制限されていない場合には、ここから社内の情報が外部に漏洩する危険性があります。例えばモバイル端末で個人使用しているSNSに業務データがコピー&ペーストされたら? あるいは社内の機密ファイルが勝手にクラウドストレージに書き込まれてしまっていたら? このような不安は、BYODの場合には特に大きくなるはずです。

端末がマルウェア感染した際に適切な対処が行えるか不安…

最近のマルウェアは、関係者のメールを装って添付ファイルを開かせるなど、侵入方法が高度化しています。またターゲットに感染した後も、アンチウイルスソフトの目をかいくぐって感染したことを検知させないよう、様々な工夫が凝らされています。そのため感染したことが発覚するまでに時間がかかり、その間に社内ネットワークに接続され、知らないうちに感染が拡大していることも… 発見されたときにはすでに手遅れ、というケースも珍しくありません。

問題解決に必要なのはエンドポイントセキュリティの強化。しかもそれを、シンプルな形で実現しなければなりません。

Workspace ONE & Carbon Blackなら エンドポイントセキュリティをシンプルな形で実現できます。



エンドポイントの徹底管理を可能にする

Workspace ONE

あらゆるエンドポイントを統合的に管理

デスクトップからモバイルデバイスまで、あらゆるエンドポイントを統合的に管理することで、管理のサイロ化を解消。最新状態をリアルタイムで把握できるため、手間を掛けずにセキュリティを強化できます。

企業アプリケーションの配信と管理

モバイル端末を管理する一般的なモバイルデバイス管理(MDM)とは異なり、企業が許可するアプリケーションを配信・管理するモバイルアプリケーション管理(MAM)機能も装備。SaaSアプリや内製アプリをカタログ化し、社員の属性に応じてプッシュ型で配信できます。

端末紛失時の対策とGPSトラッキング

ユーザーが使用する端末が紛失した際には、端末のロックやメッセージ表示、データ消去などを組み合わせて実行可能。また「特定エリア内でのみ端末の利用を許可する」といった、GPSと連動したポリシーの設定も可能です。

不適切な端末からのアクセスを遮断

OSバージョンやパッチ適用状況、稼働しているソフトウェアなど、エンドポイントの状態をチェックした上で、アプリケーションへのアクセスをコントロール。「不適切な状態」だと判断された端末からのアクセスを遮断することで、脅威の拡大を防ぎます。

マルウェアからの防御を強化する

Carbon Black

次世代アンチウイルス

既知のマルウェアを識別するシグネチャだけに依存するのではなく、AIを活用した振る舞い検知も行うことで、未知のマルウェアにも対応可能。エンドポイントで発生したすべてのアクティビティは、リアルタイムに監視・記録・収集・解析され、インシデントの検知・防御が行われます。そのためこれまでは検知が難しかったファイルレス攻撃からの防御も可能です。

EDR機能を統合

攻撃を検知・防御するアンチマルウェアだけではなく、Endpoint Detection and Response (EDR:エンドポイントでの検知と対処)機能も装備。攻撃の迅速な封じ込め、調査・復旧、その後の対応策立案も、強力に支援します。

リアルタイムでのデバイス評価

パッチレベルやユーザー権限、ディスクの暗号化など、デバイスの状況を簡単な手順で可視化。保護対象となるすべてのデバイスのセキュリティ状態を追跡・強化できます。

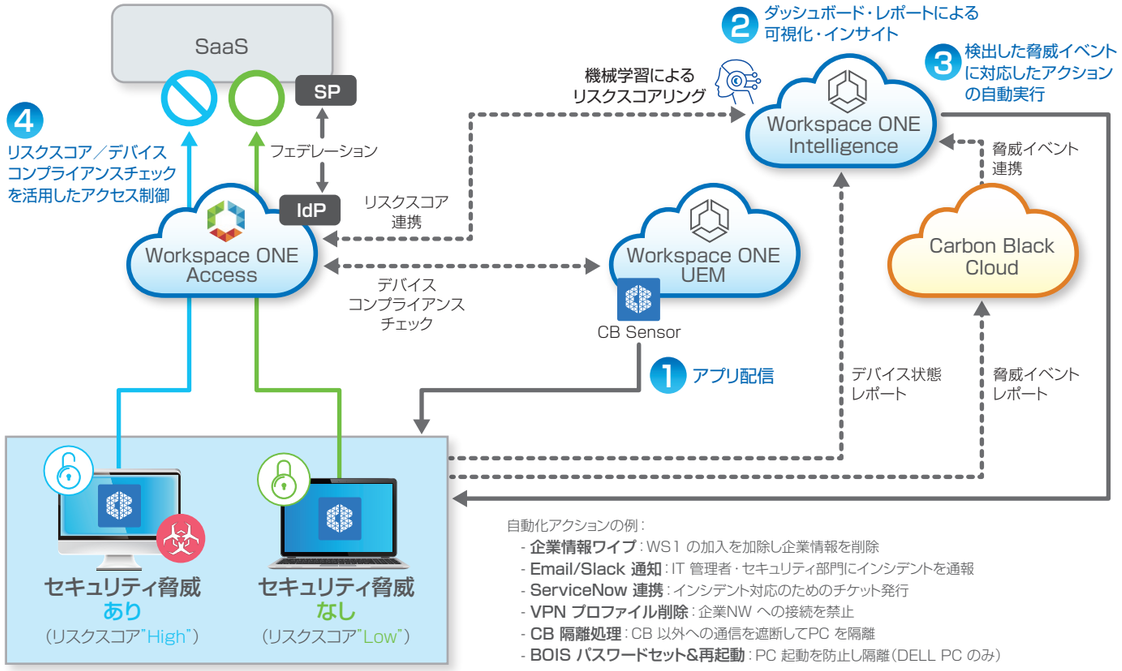
国内データセンターからクラウドサービスとして提供

Workspace ONE と Carbon Blackの主要な機能は、クラウドサービスとして提供されています。しかもそれらが稼働する場所は国内データセンター。安心してご利用いただけます。

※提供される機能の内容は、エディションによって異なります。

VMware Workspace ONE® & VMware Carbon Black®

Workspace ONE & Carbon Blackの具体的な利用イメージ



自動化アクションの例:
- **企業情報ワイプ**:WS1 の加入を加除し企業情報を削除
- **Email/Slack 通知**:IT 管理者・セキュリティ部門にインシデントを通報
- **ServiceNow 連携**:インシデント対応のためのチケット発行
- **VPN プロファイル削除**:企業NW への接続を禁止
- **CB 隔離処理**:CB 以外への通信を遮断してPC を隔離
- **BOIS パスワードセット&再起動**:PC 起動を防止し隔離(DELL PC のみ)

Step 1 アプリ配信

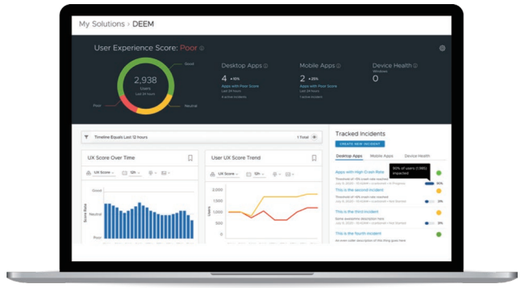
まず管理対象となるデバイスをWorkspace ONEに加入させます。これによってデバイスにはCarbon Blackのセンサーモジュール(CB Sensor)が自動的にインストールされます。必要であればユーザーによるオンデマンドインストールも可能です。

Step 2 脅威の可視化とインサイト

Carbon Black Sensorが収集した情報は、自動的にクラウド上のCarbon Blackへと蓄積。そこで発見される脅威イベントは、Workspace ONEのダッシュボードで可視化されます。

Step 3 自動化アクション

Carbon Blackが脅威イベントを検知した場合には、事前に定義したアクションを自動的に実行。脅威の封じ込めと初期対応の時間を大幅に短縮できます。これによって他のエンドポイントへの脅威の波及も防止できます。



Step 4 アクセス制御

Carbon Blackで検知した脅威イベントやデバイスのセキュリティ状態から、Workspace ONEがリスクスコアを算出。このリスクスコアとデバイスコンプライアンスを使用することで、より高度なアクセス制御を実施できます。

マルウェア対策になぜEDRが必要なのでしょうか?

従来の一般的なマルウェア対策は、アンチウイルスソフトなどでマルウェアの侵入を検知し、水際で感染を防止するというものでした。しかし最近のマルウェアは侵入方法が高度化しており、侵入を100%検知することが難しくなっています。また一般には知られていない脆弱性を悪用した「ゼロデイ攻撃」の場合には、そもそも検知に必要な情報が存在しないというケースもあります。

このような「検知をすり抜けた攻撃」や「未知の脅威」に対応するには、侵入されることを前提に、その後の対策を考えなければなりません。これを実現するのがEDRです。EDRは侵入後の検出・調査・対応・回復を担うものであり、その目的は侵入後の影響を最小化すること。もちろんその効果を引き出すには、EDRが発するアラートを常時チェックし、問題発生時に迅速に対応できる「セキュリティ・オペレーション・センター(SOC)」の設置も欠かせません。

デジタルテクノロジーはEDRを提供するのみならず、24時間365日対応のセキュリティ監視サービスのご提供も可能です。

Workspace ONE & Carbon Blackの導入・運用はデジタルテクノロジーにお任せください。

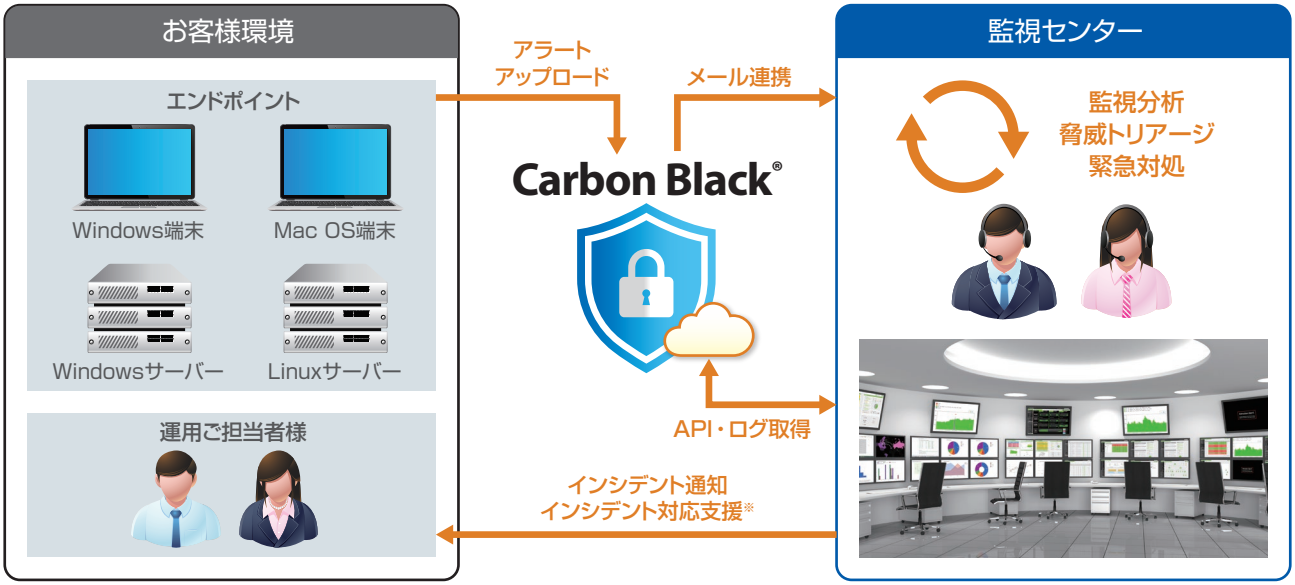
デジタルテクノロジーはVMwareのパートナーとして、Workspace ONE & Carbon Blackの導入・運用をご支援しています。そのために以下のVMware関連のサポートサービスを提供しています。

お客様の状況に合わせた導入方法をご提案

経験豊富なエンジニアがヒアリングを行い、お客様の課題を整理した上で、ご希望の予算に合わせた最適な提案を行います。その後、Workspace ONE & Carbon Blackの導入に関する設計や、導入に必要な既存システムの構成変更、既存ベンダーとの連携・調整なども実施。さらに設計内容にもとづいた導入作業や機能チェック、通信・動作確認試験を行った上で、お客様に引き渡します。

セキュリティのプロがEDR運用をサポート

EDRの効果は、単に導入しただけでは得ることができません。その真価を発揮する上で欠かせないのが、セキュリティに関する高度な知見を持つ専門家が参画した上で、適切な運用を続けることです。デジタルテクノロジーは、セキュリティのプロがセキュアかつシンプルなEDR運用をサポートする体制を確立。お客様側にセキュリティの専門家がいない場合でも、適切な運用を支援し続けます。



※ 一部サービスはオプションです。

さらなる導入効果を引き出す D-Cloud Operation

Workspace ONEやCarbon Blackのようなクラウドサービスは、適切な運用を行うことで、さらなる効率化やコスト削減を図ることができます。そのために提供しているのが「D-Cloud Operation」。監視ソフトウェアを用いた稼働状態の自動監視や、運用担当者様への通知、DR用途利用時の切替試験など、日々の操作代行を含めたクラウド運用をご支援いたします。

デジタルテクノロジー株式会社

［ 本 社 ］〒116-0014 東京都荒川区東日暮里5丁目7-18 コスモパークビル
TEL：03-5604-7565　FAX：03-3802-3400
［大阪支店］〒532-0004 大阪市淀川区西宮原2-7-53 Marutaビル
TEL：06-6393-1301　FAX：06-6393-1300
https://www.dtc.co.jp/

2022.7