SB C&S

次世代アンチウイルスソフト

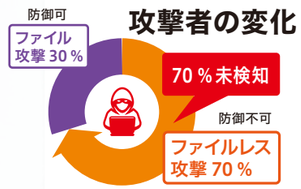
Carbon Black Cloud Prevention

従来型のアンチウイルスソフトは、約 70 %の脅威を素通りさせています

今、従来型エンドポイント対策の見直しが求められています

理由 1 エンドポイントまで到着する威力を増した脅威

これまでのエンドポイント対策は、シグネチャーでパターンマッチングを行うアンチウイルス製品が主流でした。しかし、パターンマッチング方式をすり抜けるファイルレス、ランサムウェア、環境寄生型の脅威が爆発的に増加したことで、従来のエンドポイント対策では不十分になってきています。



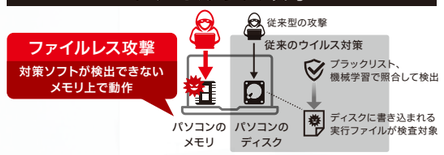
攻撃者の変化：情報セキュリティ 10大脅威 2021

1位 ランサムウェアによる被害 （昨年 5 位）
2位 標的型攻撃による情報窃取 （昨年 1 位）
3位 テレワークなどの働き方を狙った攻撃（NEW）
4位サプライチェーンの弱点を悪用した攻撃 （昨年 4 位）
5位ビジネスメール詐欺による金銭被害 （昨年 3 位）

出典：独立行政法人情報処理推進機構「情報セキュリティ 10 大脅威 2021」

従来型アンチウイルスソフトでは、防ぐことが困難な攻撃が増加

ファイルレス攻撃



凶悪な新種のマルウェア

侵入時に回避行動を取るランサムウェアの増加

Emotet などの凶悪な未知のマルウェアが横行

機械学習を搭載した既存のセキュリティーを回避するマルウェアが増加

理由 2 ネットワーク環境の多様化で顕在化する脆弱性

これまでエンドポイントは、社内のネットワークに接続されていました。しかし、テレワークなどにより社外に持ち出され、インターネット経由でアクセスすることで、サイバー攻撃の被害に遭いやすくなっています。こうした環境の変化により、エンドポイントを保護する必要に迫られています。

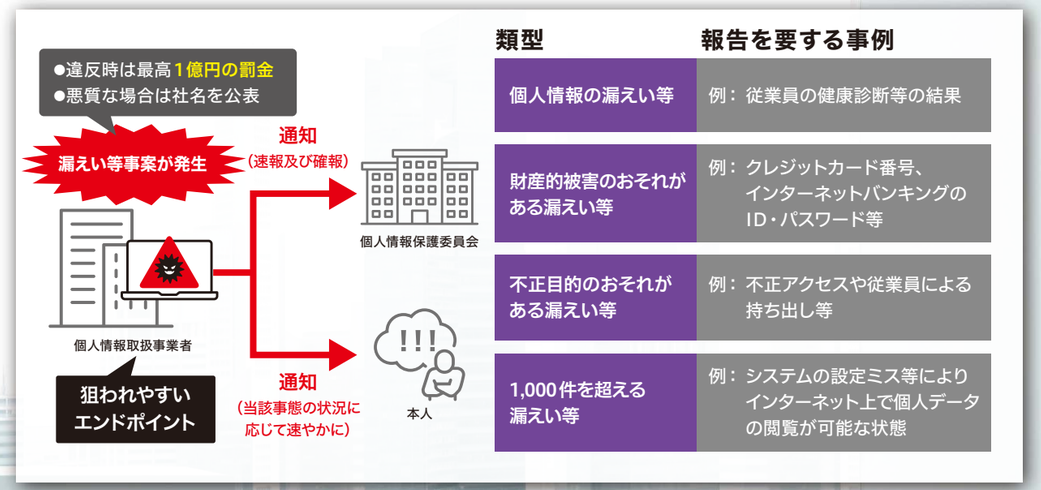
環境の変化		変化に伴う課題
① テレワークの定着による持ち出し PC の増加	>	① 社内ネットワークを通らないためゲートウェイ対策が困難
② 国内・海外拠点、国内サテライトオフィスの増加	>	② 拠点ごとにゲートウェイセキュリティー対策が必要となる
③ クラウドの進展により暗号化通信（HTTPS）が普及	>	③ 内容が見えないためゲートウェイセキュリティー対策が困難

理由 3 <個人情報保護法改正> 情報漏えいの報告・本人通知が「努力義務」から「義務化」へ

個人情報保護法は、3 年ごとに検討を行い、社会情勢の変化に応じて改正されることになっています。令和 2 年の見直しで一部が改正され、情報漏えい等が発生して個人の権利や利益を害するおそれが大きい場合、現行法では、「努力義務」であるのに対して、改正法では「義務化」されます。
これら事業者へのさらなる対応強化が求められており、**令和 4 年 4 月より施行される予定です。**

罰則が厳格化され、罰金は最大1億円に

増加する組織内部の不正行為を防止するため、個人情報保護法の罰則が厳格化され、**罰金上限が 1 億円**に引き上げられました。また、前回（2017 年）の改正時、保護法の規制対象外だった「取り扱う個人情報の数が 5,000 以下の事業者」が対象となり、ほぼすべての事業者が対象になりました。



セキュリティ対策の強化が必要です

従来型からの乗り換えをお勧めします！

NGAV
Next Generation Anti-Virus

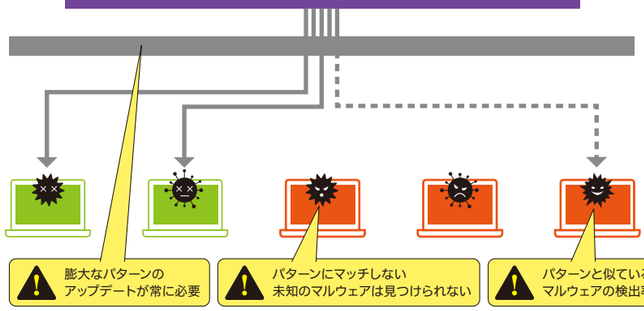
次世代アンチウイルスに特化したソリューション
VMware Carbon Black Cloud Prevention

Carbon Black Cloud Prevention は、次世代型のウイルス対策（NGAV : Next Generation Anti-Virus）に特化した ソリューションです。進化したサイバー攻撃からエンドポイントを保護するために、プログラムなどの振る舞いから検知できる NGAV への切り替えが急務となってきています。

従来型アンチウイルスソフトでは防御できない攻撃もしっかりガード

従来型アンチウイルスソフト

ファイルの特徴的なパターンを定義し、それを検知する「パターンマッチング方式」

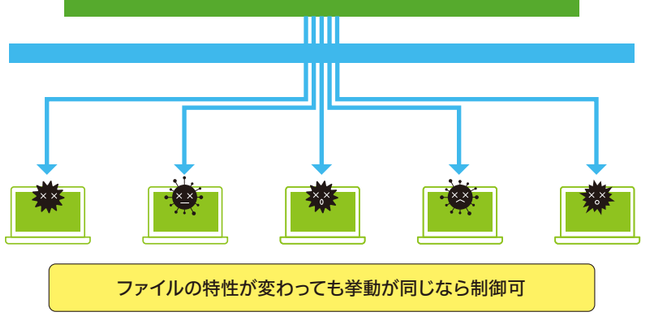


課 題

- ✓ 継続的な更新とメンテナンスが必要。
- ✓ エンドポイントの占有領域が大きい。
- ✓ ゼロディ攻撃や未知のマルウェアには効果がない。
- ✓ 最新のシグネチャデータの範囲内でしか保護できない。
- ✓ マルウェアを使わない攻撃は防御できない。

次世代アンチウイルスソフト

攻撃者の「行動パターン」を分析し悪意のある挙動を検知・防御



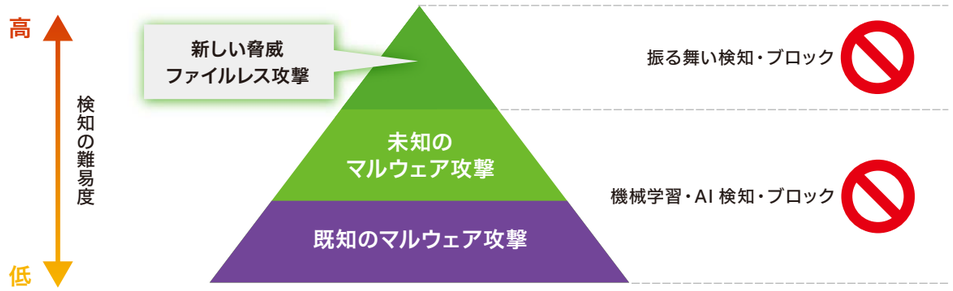
ファイルの特性が変わっても挙動が同じなら制御可

メリット

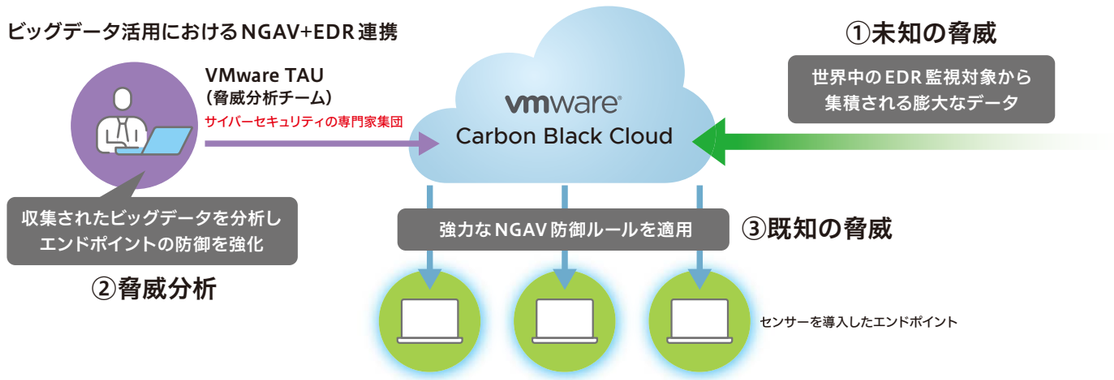
- ✓ 多様な検出方法による優れた検知・ブロック能力。
- ✓ マルウェア、ファイルレス、ランサムウエア、Living off the land 攻撃を阻止。
- ✓ 脅威検知のアラートとプロセスツリーによる侵入経路の可視化。
- ✓ 軽量なエージェントとメンテナンス不要のクラウド環境。

クラウドのインテリジェンスで最新 / 未知の脅威に対応

従来型のパターンマッチングでは、未知の脅威の検知は困難でした。Carbon Black Cloud Prevention は、機械学習・AI・振る舞いを活用するため、既知や未知のマルウェアはもちろん、主流となったファイルレス攻撃の検出も可能です。



ビッグデータ活用における NGAV+EDR 連携



Carbon Black Cloud Prevention をお勧めする４つの理由

次世代対策を簡単に導入

高機能でありながら、通常のアンチウイルスソリューションと同じ感覚で簡単に導入することができます。

始めやすく運用が容易

クラウドサービスで提供されるため、従来型のような管理サーバーや中継サーバーの準備は不要です。

EDR へ手軽にアップグレード

クラウドの管理画面や配布したエージェントを入れ替えることなく、EDR へ簡単にステップアップが可能です。

従来型と同じお手軽価格

従来型アンチウイルスソフトが値上がり傾向の一方、Prevention は高機能ながら同等の価格感で経済的です。

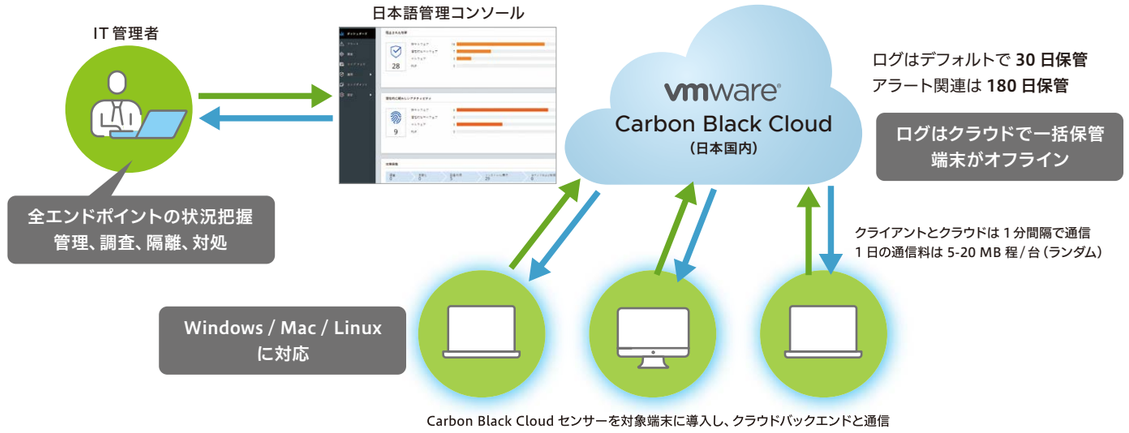
NGAV
Next Generation Anti-Virus

すばやい導入・展開、超低負荷による安定した運用を実現します

EDR
Endpoint Detection and Response

侵入後の対策を可能にする EDR 機能の追加も容易です

Carbon Black Cloud Prevention はクラウドサービスで提供されるため、オンプレミスでの管理サーバーなどの設置は一切不要で、各エンドポイントにエージェントをインストールするだけでサービスを開始することができます。



Carbon Black Cloud センサーを対象端末に導入し、クラウドバックエンドと通信

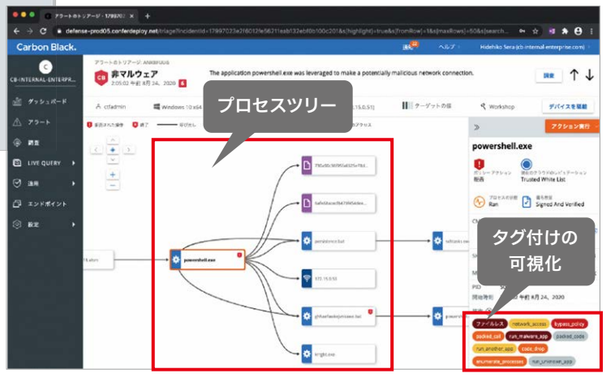
- まず NGAV 機能だけを導入し、運用に慣れてから EDR を導入することができます。
- PC、Mac、Linux に導入するエージェントのインストールも数分で完了します。
- エージェントの CPU ならびにメモリの利用率は 1 % 以下で業務に影響を与えません。

直感的に操作できるので、専任のセキュリティー担当を置く必要はありません

現在のセキュリティー状況と対処すべき課題を可視化

運用ポリシーの設定や変更についても、
管理コンソールから一括して処理することが可能。

攻撃の経路を可視化し、感染ポイントを特定



今後もサイバー攻撃が減ることはなく、複雑さや巧妙さが増すと予測されます。
この点を踏まえ、次世代アンチウイルスによる「防御策の強化」に加え、「検知」「分析」「運用性」の機能を有する、EDR（Endpoint Detection and Response）の追加をお勧めします。

サイバー攻撃の基本プロセスのすべてに対応

検　知
各エンドポイントの振る舞いを監視することで侵入した脅威の検出が可能。
侵入を迅速に検知することで即座に対応でき、被害を最小限に抑えます。

分　析
平常時から各種ログを収集・分析しているため、調査に必要なログだけを迅速に抽出・調査。
脅威の侵入検知がそのまま影響範囲や被害情報の調査へと直結しているため、
攻撃を受けた際は事態の収束に向けてすぐにアクションできます。

運用性
日本語化された UI や日本国内サーバーでの運用、コンソールやエージェントの統一により、
セキュリティーの一元管理を実現します。

Prevention のライセンスをアップデートするだけで、EDR 機能を追加できます

VMware Carbon Black Cloud には、Prevention で提供される NGAV に加えて、デバイスの振る舞いを検知・分析・調査を行う EDR 機能を提供する「Standard」「Advanced」「Enterprise」の 3 エディションがあります。

VMware Carbon Black Cloud はすべて提供

NGAV
Next Generation Anti-Virus

EDR
Endpoint Detection and Response

再インストール不要でアップグレードが可能

Prevention	Endpoint Standard	Endpoint Advanced	Endpoint Enterprise
● 次世代アンチウイルス	● 次世代アンチウイルス ● 不審な振る舞い検知 ● リモート復旧・遠隔対策	● 次世代アンチウイルス ● 不審な振る舞い検知 ● リモート復旧・遠隔対策 ● IT ハイジーン機能	● 次世代アンチウイルス ● 不審な振る舞い検知 ● リモート復旧・遠隔対策 ● IT ハイジーン機能 ● 脅威ハンティング

VMware セキュリティーソリューションの Web サイト集をご紹介します。

Prevention（NGAV）製品概要

Carbon Black Cloud Prevention のすべてがわかります。次世代アンチウィルスの導入や乗り換えをお考えのお客さまは必見。

https://licensecounter.jp/vmware/lp/carbon-black-cloud-prevention.html

EDR

変革の進む IT 環境と進化するサイバー脅威に対応する、クラウドベース EDR ソリューションをご紹介。

https://licensecounter.jp/vmware/solution/carbon-black-cloud.html

EDR

万が一の場合にも迅速な対策と早期の復旧により被害を最小化する、Carbon Black Cloud の EDR ソリューションをご紹介。

https://licensecounter.jp/vmware/lp/cbc-need-for-edr.html

EDR

従来型のアンチウイルスソフトでは防御できない理由、Carbon Black Cloud がこれまでの対策とこれからの対策どちらにも対応できる理由をご紹介。

https://licensecounter.jp/vmware/lp/cbc-role-of-edr.html

VMware Anywhere Workspace

場所を問わず業務が行える分散型のビジネス環境を実現し、より快適かつセキュアなテレワークを支援する VMware Anywhere Workspace をご紹介。

https://licensecounter.jp/vmware/solution/anywhere-workspace.html

サイバーセキュリティー

SB C&S や VMware がセキュリティーイベントで登壇した際の内容を中心に、デジタル改革を推進する VMware が目指す次世代のセキュリティーの姿をご紹介。

https://licensecounter.jp/vmware/special/security-2021sp.html

Carbon Black セキュリティ監視サービス

監視センターとセキュリティのプロが高度な EDR ツールをフル活用して、セキュアでシンプルな EDR 運用をサポートします。

https://licensecounter.jp/vmware/lp/edr-soc.html

無料 Web セミナー

EDR 検証結果や、実案件からの経験値を通して、VMware の EDR「Carbon Black」を知っていただく機会をご用意。

https://licensecounter.jp/vmware/lp/webinar-edr2021.html

SB C&S

SB C&S株式会社

〒105-7529 東京都港区海岸一丁目7番1号 東京ポートシティ竹芝オフィスタワー
https://cas.softbank.jp/

お問い合わせ先

2022/06