


今求められるアンチウイルスソフトとは

よくわかる！

ウイルス対策ソフトの選び方

A man in a dark suit and white shirt is walking across a grassy field under a blue sky with scattered clouds. He is holding a large, metallic, shield-shaped object in front of him. The shield is silver with a dark border. The background is a vast, open landscape with some rocks in the foreground. The bottom right corner of the image has a diagonal split into two shades of blue.

防御と封じ込め、異なる役割を理解して
しっかり選び攻撃に備える

脅威防御

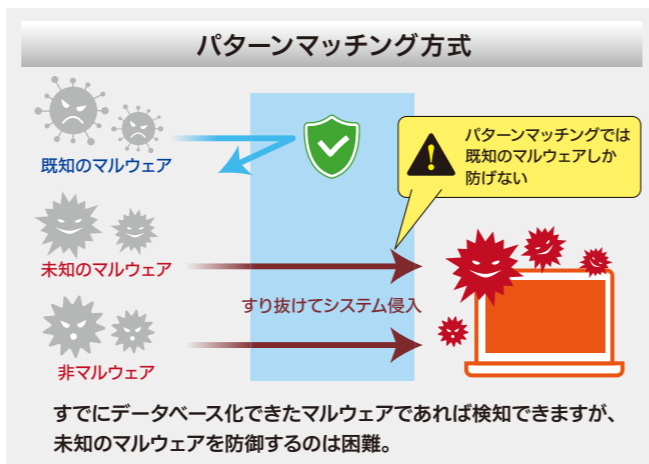
同じ監視に見えても、やっている内容は異なります



従来型アンチウイルスソフト EPP (Endpoint Protection Platform)

EPPは、悪意をもってPCに侵入しようとするマルウェアを水際で検知し、サーバーやPC、スマートフォンなどを含む末端機器を保護することを目的としています。

これまでに見つかったウイルスのデータパターン脅威情報から、ソフトウェアメーカー各社が作成したシグネチャ（ウイルスパターン）ファイルが搭載されており、そのパターンに合致するファイルを検知して防御します。

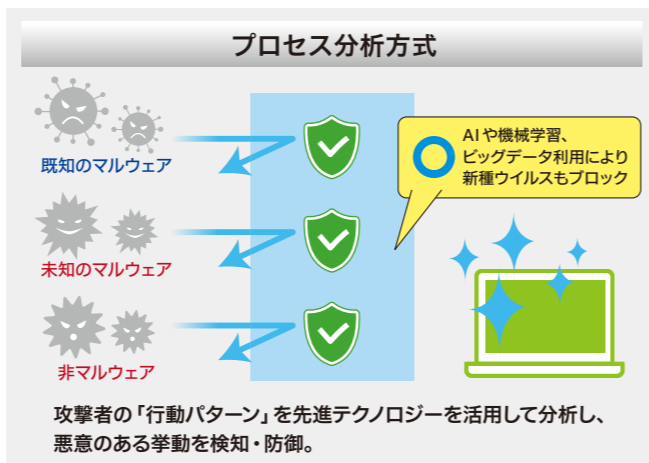


課題

- 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。
- ゼロデイ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。
- ファイルを使わない攻撃は防御できない。

次世代型アンチウイルスソフト NGAV (Next Generation Anti-Virus)

NGAVは、AIや機械学習などを活用し、ファイルや挙動の精査を行い、既知および未知の脅威からエンドポイントを保護します。従来のアンチウイルスソフトでは、防御ができなかった未知のマルウェアや、プログラムを入れることなく攻撃を実行する非マルウェア攻撃（ファイルレス攻撃）への対策が可能です。



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、ランサムウェア、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。
- 軽量のエージェントとメンテナンス不要のクラウド環境。

二つの製品を犯人逮捕にたとえると…



EPP

指名手配犯リストで犯人を検挙、リストにない犯罪者は捕らえられない



NGAV

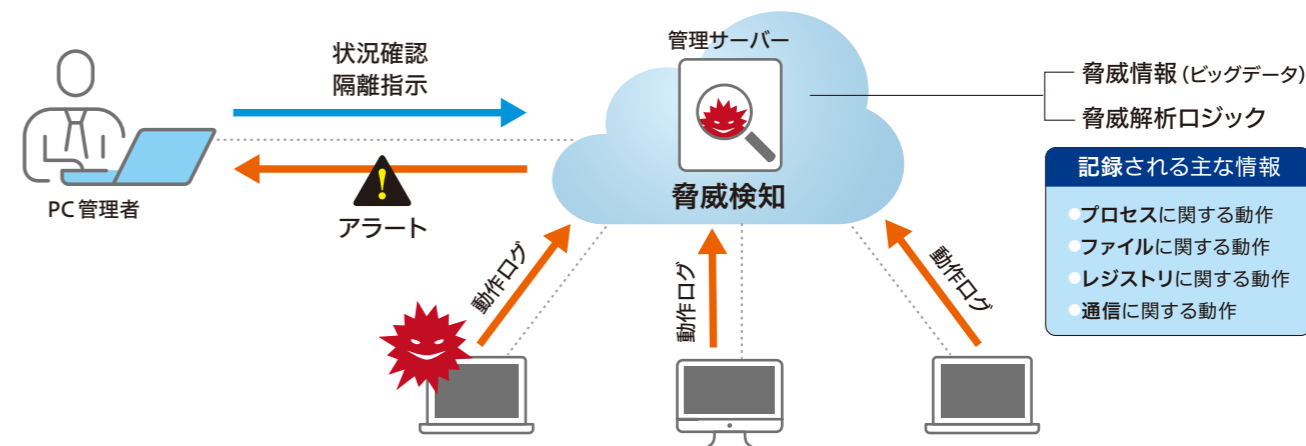
変装、整形を見破ったり、不審な動きや危険な動きを監視して検挙

検知・封じ込め ・調査・復旧

攻撃は100%防げません。被害を最小限に抑え込む能力が求められます

EDR (Endpoint Detection and Response)

攻撃は100%防げない、という脅威の侵入を前提とした製品です。社内外のネットワークに接続されたエンドポイントの振る舞いを監視して異常を検知し、組織内での拡散を防ぎ、被害を最小限に抑えます。



お勧めの組合せ

侵入前対策 NGAV

- マルウェア
- ファイルレス
- ランサムウェア

怪しい振る舞いを検知・防御

侵入後対策 EDR

EDR (Endpoint Detection and Response)

検知 → 駆除 → 解析 → 復旧

遠隔からの迅速な対応

EDR 製品を選ぶときのポイント

★ログの記録方式が「常時録画」タイプをお勧め



常時録画タイプ

- 24時間監視が可能な監視カメラ 常時録画のように、万一の時の検証や証拠に利用できるタイプ。
- 端末上の動きは、脅威であるかどうかに関わらずすべての挙動を記録し、可視化することで、新たな未知の脅威ハンティングや、過去にさかのぼったログの調査が可能。



イベント録画タイプ

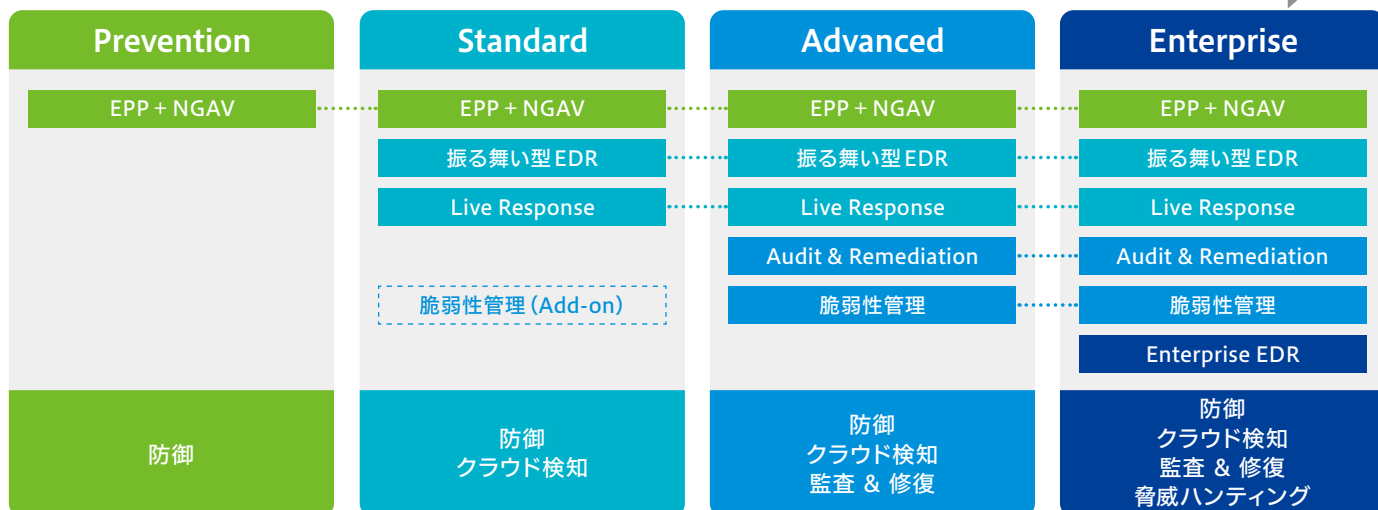
- センサーが感知したときにのみ録画するイベント録画のように、検証したい時間帯が録画されていない可能性がある。
- EDRの中には「イベント記録タイプ」しかない製品があり、不審通信を検知しても、ログが存在しないため調査不能になる。

次世代アンチウイルス+EDR ソリューション

Carbon Black Cloud

VMware Carbon Black Cloud は、お客様のセキュリティレベルに合わせて柔軟に選択できる、次世代アンチウイルス+EDRソリューションです。たとえば、エンドポイント向けセキュリティ強化の第一歩として Prevention を導入し、将来的に EDR 機能等の追加として、Endpoint Std/Adv/Ent へのアップグレードが可能になります。

エージェント、クラウドインスタンス変更なしでアップグレード可能



VMware エンドポイントセキュリティを特集した Web サイトをご参照ください。

■ Prevention (NGAV) 製品概要

EDR 導入への第一歩！
VMware Carbon Black Cloud
Prevention で始める
次世代のセキュリティ

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

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

■ EDR

Carbon Black Cloud

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します。

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

■ EDR

EDR

これからのエンドポイントセキュリティに必要な検出、
解析、運用面のすべてで高水準の性能を提供する EDR の
優位性を解説。

<https://licensecounter.jp/vmware/solution/next-gen-security-edr.html>

■ EDR

侵入された時の備えは
できていますか？

エンドポイントが増え続ける時代。
VMware Carbon Black が提供する 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します。

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

Copyright © SB C&S Corp. All rights reserved.

※VMwareは、米国およびその他の地域におけるVMware, Inc.の登録商標または商標です。その他、記載されている会社名および商品・サービス名は各社の登録商標または商標です。※本書の記載は2022年6月現在のものです。記載されている仕様・価格・内容は予告なく変更される場合があります。



お問い合わせ先