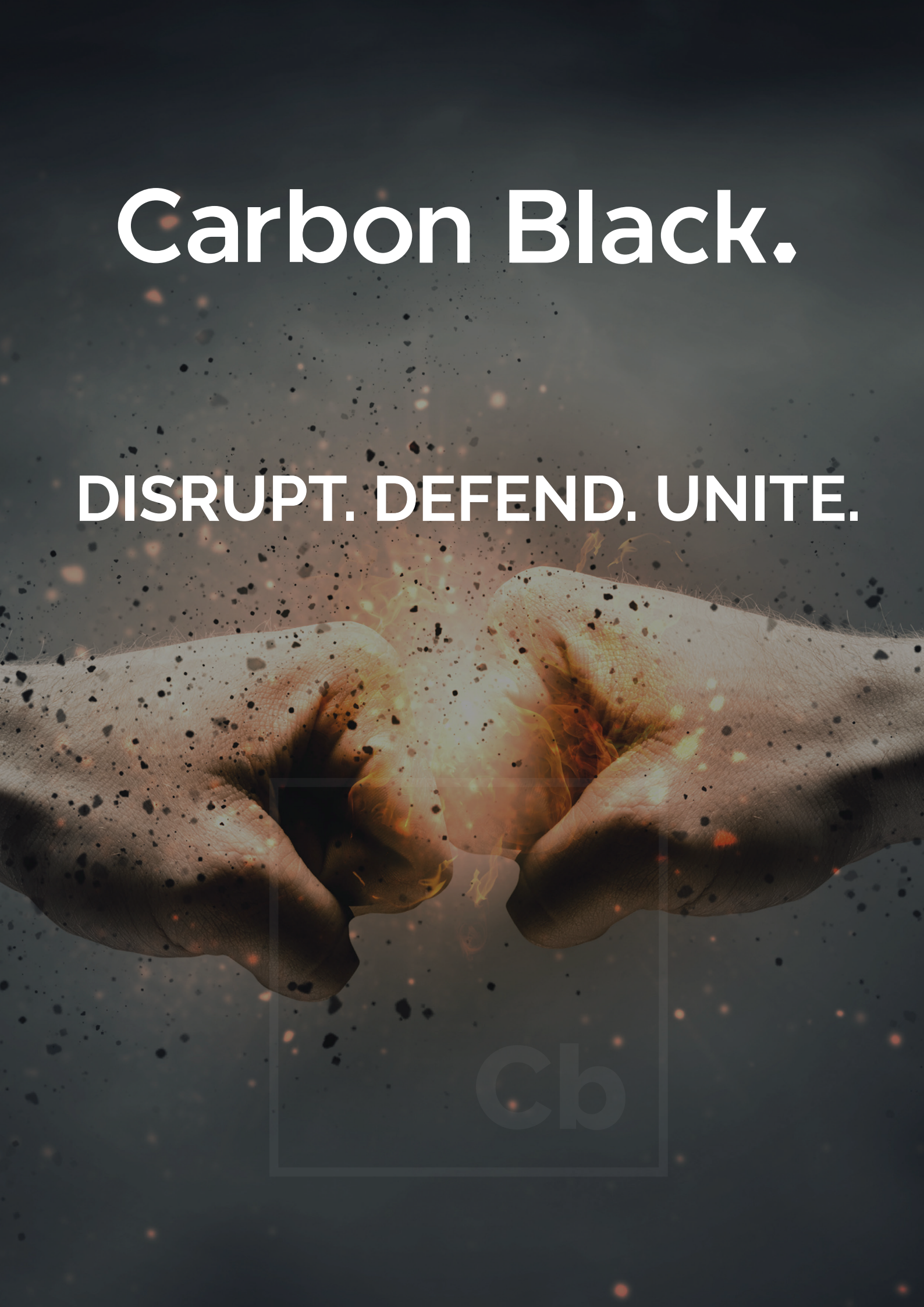
Carbon Black.

DISRUPT. DEFEND. UNITE.



Cb Endpoint Security Platform

システムのロックダウンからEDR、次世代アンチウイルスまで複数の機能を単一ベンダーで実現

次世代 アンチウイルス
Cb Defense

検知 & レスポンス EDR
Cb Response

アプリケーション コントロール
Cb Protection

多様な攻撃を阻止

- マルウェアやランサムウェアなど、ファイルベースの攻撃を防止
- オンメモリ攻撃や難読化されたマルウェア、パワーシェルやスクリプトを悪用する攻撃といった次世代の攻撃を阻止
- より広範なエンドポイントデータを収集し、クラウド上で攻撃パターンを解析
- 振る舞いやレピュテーション、AI、機械学習を用いたフルスペクトル解析

あらゆる脅威を検出し、セキュリティギャップを解消

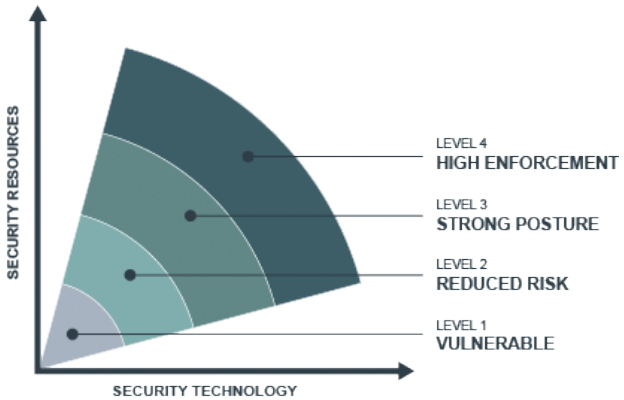
- ブロックした攻撃に関する完全な可視性
  - 何が起きたか、そしてどんな影響を受けたか
- 単一のUIで復旧対応を簡素化
- 問題に対する迅速な封じ込めと除去
- 不要なソフトウェアの削除
- 継続的なコンプライアンスの実現

規模を問わない クラウドやオンプレミス環境への展開

- 15分程度での容易なエンドポイントへの導入
- 利用端末のパフォーマンス影響を利用者に感じさせない軽量さ
- およそ1%のCPU影響と、従来のアンチウイルスよりも90%小さな負荷
- クラウド及びオンプレミス環境での展開
- MSSPによるサービス提供

防御能力の向上と革新

- 次世代アンチウイルスでデバイスを防御
- 市場をリードするアプリケーションコントロール技術でシステムをロックダウン
- シェア#1のEDRソリューションで確かなインシデント対応を実現
- オープンAPIを利用した40以上の技術パートナーとの連携
- 1万人以上のセキュリティ専門家との情報共有と協力



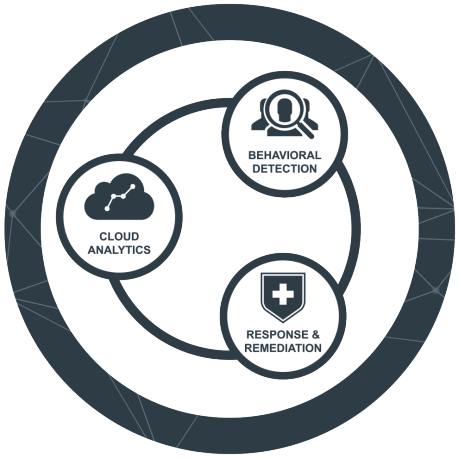
Cb Defense

最強の次世代アンチウイルスソリューションによるウイルス対策の刷新

従来のアンチウイルスソリューションによる対策だけでは、もはや不十分です。
知的財産を人質にするようなランサムウェアや、オンメモリ攻撃や難読化されたマルウェア、パワーシェルやスクリプトを悪用する攻撃といった次世代の攻撃によるセキュリティリスクに直面しています。
今日のエンドポイントには、全方位のより高度な脅威を阻止し、対策するためのソリューションが必要です。

あらゆる攻撃を阻止

- マルウェアやランサムウェア、ゼロデイ攻撃、非マルウェア攻撃といったあらゆる攻撃を自動で阻止
- エンドポイントとクラウドベースの技術を合わせることで、他の次世代アンチウイルス製品よりも多くの攻撃を阻止



あらゆる脅威の検出・可視化

- 全アクティビティをクラウド内で継続的に収集・分析を行い、攻撃の兆候や痕跡を即座に検出、可視化
- ブロックした攻撃や、検出した脅威に関するキルチェーンや影響範囲、根本原因、攻撃者の目的といった詳細情報を直ちに提供

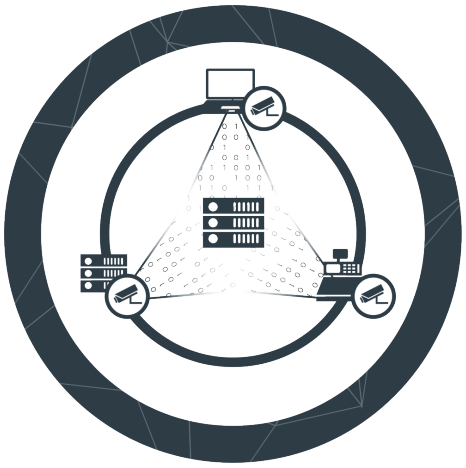
セキュリティギャップの解消

- 収集・可視化されたエンドポイントのアクティビティや、Cb Collective Defense Cloudから提供される詳細な脅威情報をインシデントレスポンスへ活用
- エンドポイントのネットワーク隔離機能や、リモート操作機能によりインシデントレスポンスを効率化

Cb Response

シェアNo1のEDR製品によるインシデントレスポンスとスレットハンティング

すべての悪意のある振る舞いを事前に識別し、防ぐことは不可能です。
93%の攻撃では、システムの攻略は数分以下で完了することから、脅威の検出と正確な対応を即時に行うことが非常に重要になっています。
侵入した脅威を迅速に検出し、正確な対応を行うためには、全アクティビティをもれなく収集し、高速な分析及び検索性能と可視性を要するソリューションが必要不可欠です。



継続的な記録による完全な可視性

- 管理サーバ上ですべてのアクティビティを継続的且つ完全に記録
- 調査時にオフラインの端末に対しても完全な可視性を提供
- あらゆる脅威の影響範囲や根本原因を即時に特定

インシデントレスポンスとスレットハンティング

- Cb Collective Defense Cloudの豊富な脅威情報と高い検索性能により、積極的な不審なアクティビティの検出を実現
- インシデント対応時間を大幅に削減：78h → 15min ※Cb社パートナー実績
- ネットワーク隔離機能や、プロセスの強制停止、ファイルの起動禁止ルールによって、脅威の感染拡大防止を即時に実施可能
- リモート操作機能により、感染したシステムに対するリモートからの完全な修復対応を実現

自動化と統合によるインシデントレスポンスの効率化

- API連携により、他社の様々なセキュリティ対策製品との連携が可能
- 3rdパーティの脅威情報や、各企業で独自に収集している脅威情報との自由な連携も可能
- 75社以上のIR/MSSPパートナーに選ばれ、使われ続けている実績

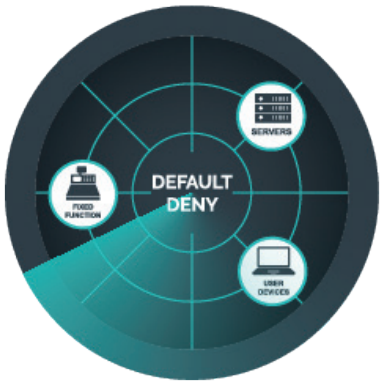
Cb Protection

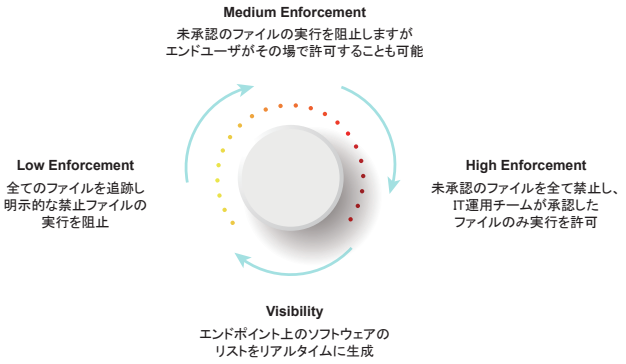
市場をリードするアプリケーションコントロール技術によるシステムのロックダウン

サーバや重要システムのセキュリティ対策として、シグネチャベースのアンチウイルス製品では不十分です。
ホワイトリストベースのアプリケーションコントロールによりセキュアな環境を維持し、攻撃が成功するリスクを低減します。これによりシステムのダウンタイムを最小化し、継続的なコンプライアンスを実現します。
アプリケーションコントロールは、重要なシステムに対する最適なセキュリティ対策です。

重要なシステムをロックダウン

- アプリケーションコントロール、ファイル整合性監視、デバイス制御、メモリ保護により、他の製品にはない強力なシステムのロックダウンを実現
- マルウェアのみではなく、非マルウェア攻撃への強力な予防が可能
- 多彩なシステムに対応し、用途に合わせたグループ別の管理、運用
- 主要機関が一般的に要求するコンプライアンスの実現を支援
  - PCI-DSS, HIPAA/HITECH, SOX, NERC CIP, NIST 800-53など





自動化による容易な運用

- 1万エンドポイントあたり一人の運用者で管理可能
- Cb Collective Defense Cloudから得たレピュテーションや信頼度、利用情報を元に、ホワイトリスト作成の自動化や、既知の脅威の自動ブロックが可能
- 多彩なホワイトリスト自動化機能
- API連携により、他社の様々なセキュリティ対策製品、特にSandbox製品との連携が可能、未知のファイルの解析や、実行禁止リストの強化などを自動化

Cb Collective Defense Cloud

インテリジェンスと分析力を備えたCarbon Blackの次世代型脅威解析エンジン

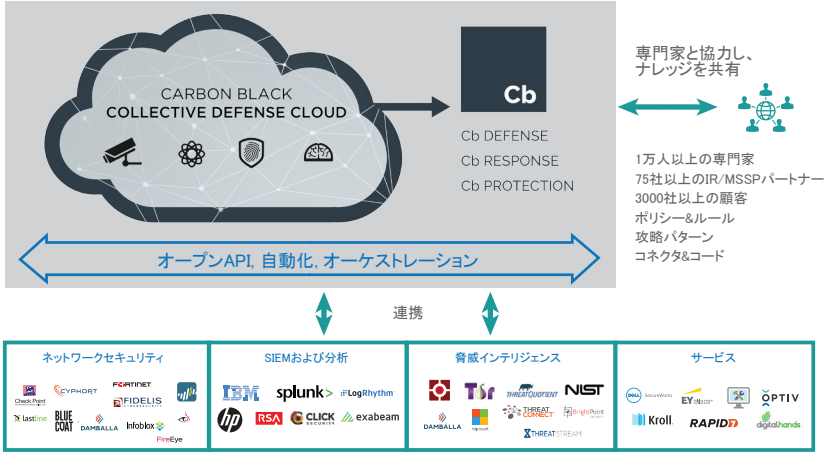
Cb Collective Defense Cloudは、Cb Endpoint Security Platformの重要な情報源です。
Carbon Black製品が保護している1000万以上のエンドポイントからの生の情報を継続的に収集し、振る舞いやレピュテーション、AI、機械学習を用いた高度なフルスペクトル解析を行なっています。パートナーや専門機関などの幅広いソースから集積された脅威インテリジェンスも活用しています。

様々な情報を元にした高度な脅威解析

- Carbon Black製品が保護する1000万※以上のエンドポイントアクティビティ情報の収集
- 75社※以上のIR/MSSPパートナーや3000※以上の顧客、3rdパーティの脅威調査機関と情報を共有
- ユーザポータルとして専門家同士が最新の情報を共有するために活用
- 収集した全情報に対するAIや機械学習を用いた高度な解析

攻撃情報の提供

- 検出した脅威に対する様々な補足情報を提供
- 攻撃者のタイプ、発信国やドメイン、関連する攻撃パターン、好む戦術、ターゲット業種、など



※2017年5月現在

NVC NETWORK VALUE COMPONENTS

株式会社ネットワークバリューコンポネンツ

〒144-0035 東京都大田区南蒲田2-16-2
電話: 03-5714-2050　　http://www.nvc.co.jp/