BlackBerry

HITACHI
Inspire the Next

次世代マルウェア対策製品

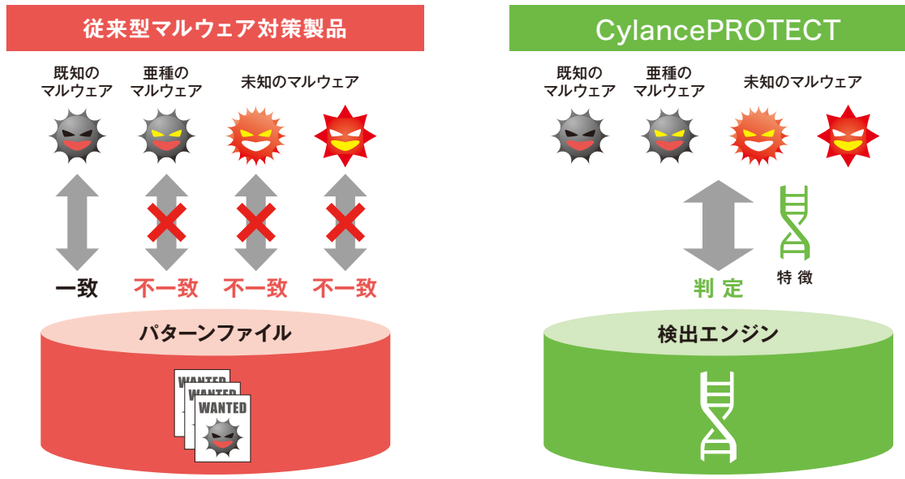
CylancePROTECT®

株式会社 日立ソリューションズ

AIを活用した先進技術で、マルウェアが実行される前に脅威を高精度に検知し、エンドポイントを守ります。

今ご利用のマルウェア対策製品は、未知のマルウェアを検知できていますか?
未知のマルウェアに対応していない従来型の対策製品の場合、
マルウェアのすり抜けを許してしまうため感染の危険性が高まり、
管理者は侵入経路の調査や感染拡大の防止といったインシデント対応に追われることになります。
それを避けるには、マルウェア検知率の高い対策で感染リスクを抑えることが不可欠です。
CylancePROTECTは、従来型のマルウェア対策製品では難しかった新種や亜種のマルウェアにも対応。
検知率99%以上[*1]で未知・既知の区別なく高精度にマルウェアを検知し、エンドポイントを守ります。 *1 2018年4月 NSS Labs調べ

CylancePROTECT®



既知・未知にかかわらず、実行される前にマルウェアを高精度かつ迅速に検知。
強固なエンドポイントセキュリティを実現します。

Point 1 AIで、未知のマルウェアも99%以上の高精度で検知

特許取得技術により、10億個以上のファイルやプログラムを人工知能システムに学習させています。一つひとつのファイルから約700万の特徴を抽出し、マルウェアと判断するルールを作成。それにもとづき、ファイルの特徴からマルウェアかどうかを高精度に判定します。ランサムウェア対策にも効果的です。

Point 2 マルウェアが実行される前にすばやく検知

振る舞い検知方式(マルウェア実行後の不審な挙動による検知)とは異なり、ファイルの特徴からマルウェアを予測するため、マルウェアの実行前に検知が可能。感染リスクを軽減します。

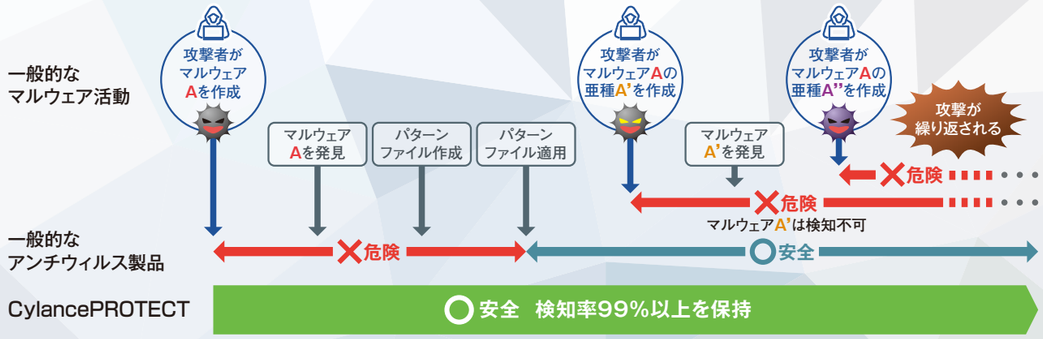
Point 3 クラウドによる集中管理で、運用の負荷とコストを低減

クラウド上で管理できるため、管理サーバーの構築や保守・維持の必要がありません。管理負担や運用コストを低減できるうえ、スキャン時の負荷が低いため、業務効率への影響も抑えられます。
また、CylancePROTECTはモバイル端末でも利用可能。PCとモバイル端末を一元的に管理できます。

これからのマルウェア対策のポイントは 次々と迫るマルウェアの脅威に対応できること。

マルウェアを使った攻撃の手口は日々高度化・巧妙化しており、コードをこまめに変えるなど、攻撃のたびに新たなマルウェアを用意する攻撃手法も生まれています。従来のパターンマッチング形式のマルウェア対策製品の場合、新たに作成されたマルウェアで攻撃されてからパターンファイルを作成・適用するため、検知にどうしてもタイムラグが発生してしまいます。

そのため、ようやくパターンファイルを適用できたとしても、そのときにはすでに新たなマルウェアの脅威が迫っているのが現状です。CylancePROTECTは、マルウェアかどうかをファイルの特徴から判断する検知方式のため、パターンファイルの有無に影響されることなく、新種・亜種のマルウェアであってもすばやく検知できる状態を保持します。



Hitachi Solutions × BlackBerry

■メーカーとの確かなパートナーシップ

定期的にお客様のニーズや課題を共有するなど、密接に連携しています。

■製品と技術を熟知した、高いサポート力

豊富なノウハウと高度な技術を持つエンジニアがお客様をサポートします。
きめ細かいサポートが高い顧客満足度に寄与したとして、メーカーからも評価されています。[*2]

■セキュリティ分野での豊富な実績

先進の技術とノウハウを適用したミッションクリティカルなシステムを数多く構築し、運用・サポートをしてきた豊富な実績があります。

*2: 4年連続でJapan Excellence Support Partner of the Year を受賞(2016、2017、2018、2019)

オプション

CylanceOPTICS®

CylanceOPTICS*3は、CylancePROTECTと連携したEDR（Endpoint Detection and Response）により、マルウェアの侵入経路や潜伏状況などを調査・解析します。CylancePROTECTと同一コンソールで管理できるため、簡単に運用できます。

Point 1 迅速なインシデント対応で、感染の拡大を防止

マルウェアに感染した端末が見つかった場合、感染端末を遠隔操作でネットワークから隔離し、感染の拡大を防ぎます。さらに、社内の他の端末に脅威が潜伏していないかを調査する脅威ハンティング機能により、インシデントの発生範囲をすばやく特定し、迅速な対応につなげることができます。

Point 2 マルウェアの侵入経路を特定し、再発防止を支援

AIを活用した原因分析により、マルウェアの侵入経路を時系列で可視化できます。侵入の契機を特定できるため、再発防止策の検討に活用できます。

Point 3 AIを活用し、端末上の振る舞いから疑わしいアクティビティを特定

新たな攻撃手法をAIが日々学習し、端末上の振る舞いから、脅威の可能性があるアクティビティを特定して検知できます。疑わしい振る舞いをあらかじめルールとして登録し、それに対するアクションまで自動化できます。

CylanceGATEWAY™

CylanceGATEWAY*3はAIを活用し、社外からのクラウドサービスやWebサイト、社内システムなどへのアクセスを動的に制御、セキュアなリモートアクセス（ゼロトラストネットワークアクセス）を実現します。エンドポイントセキュリティ製品のCylancePROTECT、CylanceOPTICSと組み合わせて利用することにより、デバイスやネットワークを標的とした脅威に対して包括的な防御が可能です。

*3: CylancePROTECTのオプション機能

Cylance 製品の運用支援

セキュリティの専門技術者が外部脅威対策をサポートします。
Cylance製品などからのイベント情報を分析し、インシデントの監視から対応までをワンストップで支援。
これにより、管理者の業務負荷を軽減すると同時に、高度で安心なセキュリティ対策を実現可能です。
日立ソリューションズではBlackBerry社が提供する【CylanceMDR】と、当社の【MDRサービス for BlackBerry】の2種類を提供しています。

- **知識と技術力が豊富な専門家が初動対応やアラート調査などをサポート**
- **24時間365日のアラート監視**
- **脅威イベントに関する情報をまとめ、定期的に報告**

※各社でサービスの詳細は異なります。

詳しくは製品情報サイトへ　Cylance 日立　検索

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/cylance/

S16K-04-08　2024.08