CylancePROTECT®

AI を活用した予測型の脅威防御

特長

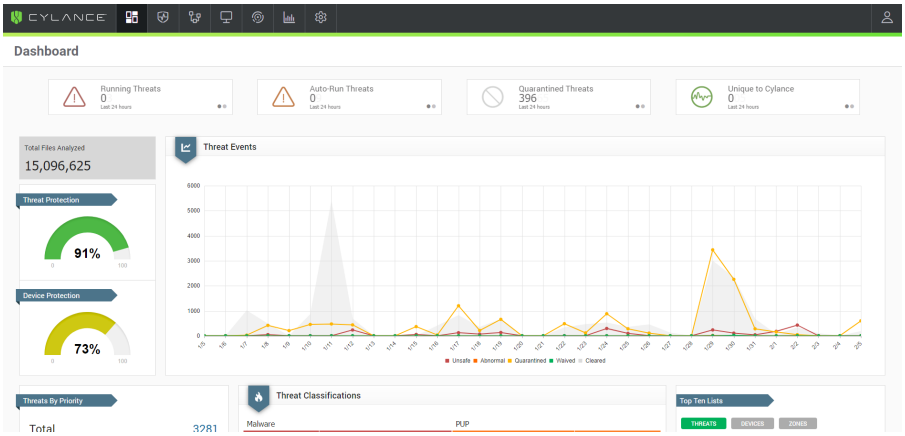
- **AI（人工知能）を活用した防御**により、従来のソリューションと比べてエンドポイントへの負荷を軽減
- **シグネチャが不要**であるため、管理の負担が軽減
- **クラウドや新しいハードウェアが不要**であるため、総所有コストを最小化

従来のアンチウイルスの一歩先を見据えて

何年にもわたり、防御製品の主要な脅威防御はシグネチャを基にしていました。企業への攻撃がすべて以前に確認されたものであるなら、シグネチャを使用するのは意味のあることです。しかしながら、現在ではマルウェアは数時間で形を変えることさえあるため、シグネチャベースの防御ツールは時代遅れになりつつあります。

今こそ、従来型アンチウイルスの一歩先を見据えて考えるときです。

CylancePROTECT をぜひご検討ください。



CylancePROTECT は、マルウェアへの感染をブロックする AI の能力と、スクリプトベース、ファイルレス、メモリ、外部デバイスベースなどの各種攻撃を防御する追加のセキュリティコントロールを組み合わせた、統合型の脅威防御ソリューションです。

シグネチャと振る舞い分析に頼って環境内の脅威を検出する従来のエンドポイントセキュリティ製品と異なり、CylancePROTECT は次の特長を備えています。

- シグネチャではなく AI を使用して既知および未知のマルウェアを識別し、エンドポイントでの実行をブロック
- クラウドに接続することなく、既知および未知（ゼロデイ）の脅威を阻止
- エンドユーザーの操作を妨げることなく継続的にエンドポイントを保護

CylancePROTECT は、システムへの影響を最小限に抑えつつ比類ない効果を発揮し、ゼロデイ防御機能を提供して、エンドポイントと組織を侵害から保護します。

CylancePROTECT の機能

真のゼロデイ防御

回復力に優れた AI モデルがゼロデイペイロードの実行を阻止します。

AI を活用したマルウェア防御

実際の現場で実証された AI が、エンドポイントでの実行を試みるあらゆるアプリケーションを、実行前に検査します。

スクリプト制御

環境内でスクリプトを実行できる場所やタイミングを完全にコントロールします。

デバイス制御ポリシーの適用

環境内で使用できるデバイスを制御し、外部デバイスを潜在的な攻撃ベクトルとして排除します。

メモリエクスプロイトの検知と防御

悪意のあるメモリの使用（ファイルレス攻撃）を防御するために迅速かつ自動的に対処して、未然に識別します。

特定用途デバイスに対するアプリケーション制御

特定業務用途のデバイスが常に正常な状態に保たれるよう、実行できるアプリケーションを限定するホワイトリスト運用を実現します。

CylancePROTECT の一般的な使用事例

CylancePROTECT は、次のようなセキュリティに関する一般的な使用事例に対応し、すべての領域にわたる脅威防御を提供します。

- 悪意のある実行可能ファイルを識別してブロックする。
- スクリプトを実行できる場所、方法、およびユーザーを制御する。
- USB デバイスの使用法を管理し、不正なデバイスの使用を禁止する。
- 保護されたエンドポイントで攻撃者がファイルレスマルウェア攻撃の手法を使用できないようにする。
- 悪意のある電子メール添付ファイルのペイロードのデトネーションを防止する。
- ゼロデイ攻撃を予測し、その実行を防止する。

CylancePROTECT の利点

包括的なセキュリティ	スムーズな業務利用	ゼロデイペイロードの防止
エンドポイントにおける効果的な脅威防御によりセキュリティスタックを簡素化	「静か」な防御により、セキュリティソフトによる業務の中断を防止	ゼロデイを悪用した攻撃が成功するリスクを排除

Cylance Japan株式会社
〒100-6510
東京都千代田区丸の内1-5-1　新丸の内ビルディング10F
www.cylance.co.jp
03-6386-0061 (代表)

201807-DS001