# CylancePROTECT® と CylanceOPTICS™：

AI 駆動型の脅威防御、検出、対応ソリューション

CYLANCE™

セキュアな環境を維持しながら、同時にエンドポイントセキュリティスタックを簡素化することによって、セキュリティチームの作業が容易になり、セキュリティに対する取り組みが一層効果的になります。CylancePROTECT と CylanceOPTICS によって構成される Cylance Security Platform は、セキュリティチームが使用するセキュリティツールを整理統合して管理可能なセットにするのに役立ちます。また、冗長性を排除し、インフラストラクチャの費用を低減し、エンドポイントのセキュリティをプロアクティブに維持する能力を高めます。

CylancePROTECT と CylanceOPTICS によって、リアルタイムの予測的脅威防御と、防御にフォーカスした EDR 機能の組み合わせを利用できるようになります。革新的な技術で設計されたこのソリューションは、ビジネスに合わせて容易に拡張できます。

| CylancePROTECT | CylanceOPTICS |
|---|---|
| AI をベースとした<br>マルウェア防御 | AI をベースとした<br>根本原因分析 |
| リアルタイムの<br>メモリ保護 | 企業全体での<br>脅威ハンティング |
| 統合されたスクリプト<br>およびアプリケーション<br>制御 | 動的な脅威検出 |
| デバイス使用ポリシーの<br>適用 | 自動インシデント対応 |

## 様々なセキュリティの要件に対応 —利用用途の例

CylancePROTECT と CylanceOPTICS によって対応、解決できるセキュリティ上の要件の一例を紹介します。

## 脅威や悪意のある活動の停止

**悪意のある実行可能ファイル**

エンドポイントを攻撃者から保護する最良の方法は、攻撃が開始される前にそれを特定し、くい止めることです。

CylancePROTECT は、実際の現場で実証された AI を使用し、エンドポイント上で実行が試みられるアプリケーションを、実行前に検査します。実行可能ファイルが悪性であるか安全であるかを、エンドポイント上で実行される機械学習モデルがミリ秒単位で判断します。実行可能ファイルが悪性である場合は実行がブロックされ、攻撃者によるエンドポイントセキュリティ侵害の試みは撃退されます。99% を超える有効性を備えた CylancePROTECT は、業界最高の AI 駆動型マルウェア防御ソリューションです。

**不正なスクリプト**

さまざまな理由により、スクリプトは多くの攻撃者が利用するツールとなっています。第一に、経験の浅い攻撃者であっても、悪意のあるスクリプトはサイバー犯罪者が集う地下サイトで容易に入手可能であり、攻撃者のニーズに合致するスクリプトを簡単に見つけることができます。また、脅威以外の目的でもスクリプトは多く利用されており、セキュリティ製品によってはスクリプト検出が困難な場合があります。CylancePROTECT にはスクリプト保護機能が組み込まれており、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、攻撃者がこの攻撃ベクトルを利用してビジネスに被害を与える機会を削減できます。

**ファイルレスマルウェア**

メモリベースの攻撃が増加しています。これは、メモリを利用して容易に目的を達成できることを攻撃者が認識してきているためです。多くのセキュリティ製品にはこのタイプの攻撃を防止する機能が備わっていません。一方、CylancePROTECT にはメモリ保護機能が備わっています。攻撃者が特権昇格やプロセスインジェクションを試みたり、他の方法でエンドポイントのメモリを不適切に使用しようとすると、CylancePROTECT は、それを即座に特定して防止します。

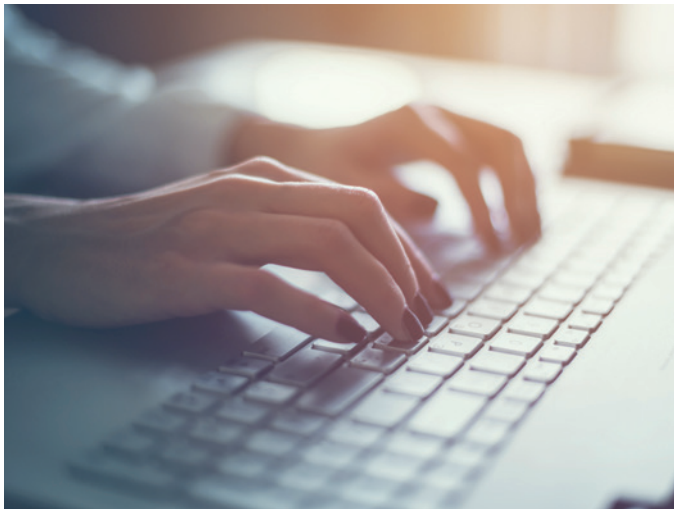
**悪意のあるメール添付ファイル**

攻撃者がエンドポイントへのアクセスやビジネスへの侵入を行おうとする場合に、フィッシング攻撃は、依然として最も効果的な方法の 1 つとなっています。従業員が正当なファイルだと思って悪意のある添付ファイルを開いてしまうと、攻撃者はあらゆる悪意のある行動を実行することが出来ます。

CylancePROTECT を利用することにより、武器化した添付ファイルは自動的に特定され、ブロックされます。たとえば、リスクのある VBA マクロがドキュメントに含まれている場合、そのマクロの実行はブロックされます。この保護によって、セキュリティに新たな層が加わり、従業員が攻撃者の犠牲となって環境にセキュリティ侵害を持ち込むことがないよう保護します。

**外部デバイスの使用**

ビジネスの多くの場面で、USB デバイスが使用されています。これらのデバイスの多くは便利なツールであり、従業員同士がファイルを迅速かつ効率的に共有できます。しかし、それらのデバイスに悪意のあるマルウェアが含まれていると、環境に大きな被害を与えることがあります。また、それらのデバイスは、機密性の高いデータを社外に持ち出すために使用されることもあります。この攻撃ベクトルに対処するため、CylancePROTECT には、外部デバイスの使用をポリシーで制御できる機能が組み込まれています。この機能を利用することにより、環境内で利用可能なデバイスをコントロールできます。この究極のコントロール機能によって、USB デバイスが攻撃実行やデータ持ち出しの手段となる可能性を抑制できます。



## 攻撃とアラートデータの調査

**アラートの調査**

エンドポイントは使用状況に応じて変化し続けています。通常、これらの変化は正常なものですが、ユーザーやセキュリティコントロールがエンドポイント上で悪意のある活動を識別した場合、それを検証するのはセキュリティチームの仕事です。CylanceOPTICS を利用することにより、識別されたファイル、プロセス、ネットワーク活動などを迅速に確認し、エンドポイントが実際にセキュリティ侵害を受けているかどうかを判断できます。CylanceOPTICS の脅威ハンティング機能に含まれる InstaQuery を利用すると、エンドポイントを数秒以内に調査し、犯罪につながる可能性のある情報を確認し、ビジネスを安全に保つために実行すべき手順を知ることができます。

**根本原因分析**

エンドポイントに影響を及ぼさないよう脅威をくい止めることは、機密性の高いデータの安全性を維持するうえで非常に重要です。これをさらに一歩進めて、脅威を撃退した際に、重要なデータをキャプチャし、将来の調査に備えて保存しておくことにより、攻撃者がエンドポイントのセキュリティ侵害をどのように試みたかを知ることができます。CylanceOPTICS はこの機能を備えており、ブロックした攻撃だけではなく、エンドポイントで検出される任意の脅威に対してこの機能を適用できます。1 回のクリックで簡単にフォーカスビューを作成できます。フォーカスビューには、脅威につながったイベント活動のタイムラインが生成されます。これにより、攻撃者が環境内のどの場所を突いて攻撃を試みようとしたかがわかり、セキュリティコントロールの脆弱な部分や攻撃面を削減するよう対策を取ることができます。

## 企業全体の脅威を検出

**活動ベース**

悪意のある活動の中には、特定が容易なものもあれば困難なものもあります。コンピューターが不規則な動作を行うようになった場合や、脅威ハンティングによってエンドポイントにセキュリティ侵害のリスクがあると判断された場合、確実な判断に必要な可視性がセキュリティツールキットによって提供されることが重要です。CylanceOPTICS を利用することにより、任意のエンドポイント上に脅威に関連するものが存在していないかアクティブに探索することができます。疑わしい活動が特定されたらすぐに検索と調査を実行して、ターゲットとなる脅威を特定できます。

## インシデントデータの検索と調査

**現在のデータと時系列のデータ（侵入の痕跡）**

脅威ハンティングとは、仮定を立て、それに応じて一連の検索／調査を実行する行為のことであり、その際、侵入の痕跡（IOC）を使用して、仮定を実証または反証します（IOC ではなく別の用語が使用される場合もあります）。このスキルを効果的に実行するには、正しいデータにアクセスできることが不可欠です。CylanceOPTICS には、ターゲットとなる脅威ハンティングと絞り込まれた結果が表示されます。その際、エンドポイントに関する現在のデータと時系列データの両方にアクセスできます。他のツールの中にはエンドポイントで生成されたすべてのデータを保存するものがありますが、CylanceOPTICS はそれとは異なり、フォレンジックに関連するデータのみを保存します。したがって、セキュリティチームは脅威を見つけるために、情報の山から無関係なデータをふるい分ける作業に時間を費やす必要がありません。

## エンドポイントでの脅威検出

**ルールベース**

脅威やセキュリティ侵害の可能性を特定するには、いくつかの方法があります。まず、セキュリティアナリストはエンドポイントを検索して、疑わしい生成物を特定できます。また、手動の調査によって、脅威が存在するかどうかを判断できます。このプロセスには非常に大きな価値があるものの、企業全体に適用できるようなスケーラビリティはありません。エンドポイントに隠れている脅威を根絶するには、自動化された脅威検出のアプローチを使用する必要があります。

エンドポイント上で実行されるルールベースのエンジンは、キュレーションされたルールセットとともに配布され、エンドポイントを継続的に監視して疑わしい動作を検出します。疑わしい動作が検出されると、セキュリティチームが介入することなく、カスタマイズされた対応アクションがリアルタイムで実行されます。

今後のリリースにおける CylanceOPTICS の脅威検出は、エンドポイントで実行されるように設計された AI ベースの脅威検出機能の導入により、大きく進歩すると予想されます。他のセキュリティテクノロジーの中には、機械学習の成果をクラウド環境で実行するものがあり、そのためには、エンドポイントの活動をクラウドへ継続的にストリーミングする必要があります。CylanceOPTICS はそうしたテクノロジーとは異なり、AI 脅威検出機能をエンドポイント上でローカルに実行します。これにより、エンドポイントが企業ネットワークやクラウド環境に接続されていない場合でも、脅威検

出が停止することはありません。この機能は、脅威検出のあり方を一変させ、中断のない保護を実現します。

## インシデント対応

**アグレッシブな封じ込めと自動化された対応**

どのようなセキュリティコントロールを導入していても、攻撃の発生をすべてくい止めることはできません。したがって、攻撃が検出された場合にそれに対処できるよう準備しておく必要があります。CylanceOPTICS では、完全に統合されたインシデント対応機能を利用できます。攻撃が特定された場合、わずか数回のクリックでファイルを検疫して、環境内のいかなる場所でもそのファイルを使用不可にすることが可能です。エンドポイントが有害であると判断された場合は、アグレッシブな封じ込めの処置を実行し、エンドポイントをロックダウンして、他のエンドポイントと通信できないようにすることが可能です。セキュリティに関する事項を特定することは重要ですが、それに対処する能力もまた重要です。CylanceOPTICS を利用することで、その能力を得ることができます。また、検出された脅威に自動的に対処するようソリューションを構成することもできます。これにより、滞留時間を減らし、攻撃対象領域を縮小することができます。

真のエンドポイントセキュリティは、事前防御または事後防御のいずれか一方によって作り出されるものではありません。現代の脅威のランドスケープによってもたらされる、変化し続ける絶え間ない攻撃に対処するには、これら両方の機能を装備して深く統合し、攻撃者のペースに対応できるようにする必要があります。

CylancePROTECT と CylanceOPTICS の組み合わせにより、これら両方の最良の機能を 1 つのソリューションで得ることができます。これにより、セキュリティスタックが簡素化され、アナリストの効率が向上し、ビジネスのセキュリティが高まります。

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.com/jp
03-6386-0061 (代表)



201711-SB001