CylanceOPTICS™

よくあるご質問

質問	回答
CylanceOPTICS とは何ですか？	CylanceOPTICS は、CylancePROTECT に新たに追加された AI ベースの EDR (Endpoint Detection and Response) 機能コンポーネントです。一貫性のある可視性、根本原因分析、拡張性の高い脅威ハンティング、自動化された脅威検出など、検知＆対処において必要なセキュリティ機能を提供します。CylanceOPTICS は CylancePROTECT の追加機能であり、CylancePROTECT で仮に検出ができずにすり抜けた脅威であっても、自動的に検出し、それに迅速に対処することに重点を置いています。
CylanceOPTICS の主な特長を教えてください。	• **分散型の検索とデータ収集：**データ収集、検索、分析を最適化する当社独自のデータ収集アプローチ • **根本原因分析：**CylancePROTECT によってブロックされた攻撃、およびエンドポイントで特定された他の注意を要する生成物に関する、Web ベース、オンデマンドの根本原因分析 • **企業全体での脅威ハンティング：**エンドポイントデータを即時に検索し、エンドポイントに隠れている潜在的な脅威を見つける • **迅速なインシデント対応：**検疫、疑わしいファイルの取得、セキュリティ侵害を受けたエンドポイントのネットワークからの隔離など、インシデント対応アクションを迅速に実行 • **動的な脅威検出と対処：**キュレーションされた検出ルールを使用して、潜在的な脅威のリアルタイム検出から適切なアクションまでを自動化
CylanceOPTICS のユニークな点はどこにありますか？	大きく以下の 3 つのポイントがあります。 • 予防にフォーカス – CylancePROTECT と同様に、人手を介することなく脅威を自動的に検知して対処することで被害を未然に防ぐことを重点としています。 • CylancePROTECT との統合 – アンチウイルスである CylancePROTECT に統合されており、EPP と EDR のシンプルかつ効果的なセキュリティ管理が可能 • 導入容易性 – クラウドベースのアーキテクチャにより、既存インフラの増強などをすることなく、容易に導入が可能
CylanceOPTICS は人工知能をどのように利用していますか？	OPTICS の FocusData では AI ベースの根本原因分析を実行して、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ているかを判断できます。将来のリリースでは、AI の利用は機械学習モデルに拡張され、エンドポイントのローカルで実行され、脅威イベントを予測モデルにより検知できるようになる予定です。

質問	回答
CylanceOPTICS は CylancePROTECT との組み合わせでのみ使用できる製品ですか？	はい、CylanceOPTICS を使用するには、CylancePROTECT が必要です。
CylancePROTECT が防御できない脅威に対して、CylanceOPTICS はどのように役立つのでしょうか？	CylanceOPTICS を利用することによって、すべてのエンドポイントを通じて一貫性のある可視性が得られ、ターゲットを絞った脅威ハンティングが可能になります。このターゲットを絞った脅威ハンティングは、実行前の防御から漏れる可能性のある、隠れた脅威を発見するのに役立ちます。また、イベントルールベースの動的脅威検知機能も搭載しており、さらに迅速な対処に必要なツールも提供されています。
CylanceOPTICS の管理や展開の方法を教えてください。	CylanceOPTICS は、CylancePROTECT と同じクラウドベースの管理コンソールを使用して管理ができます。現在、CylanceOPTICS と CylancePROTECT のエージェントインストールは個別に行います。CylanceOPTICS をインストールする前に、デバイスに CylancePROTECT の Agent バージョン 1400 以上をインストールしておく必要があります。CylanceOPTICS は管理コンソールから各エンドポイントに導入し、インストールできます。また CylanceOPTICS のインストールでも、コマンドラインオプションがサポートされています。

質問	回答 [1]	
	イベントタイプ	イベントの説明
CylanceOPTICS が収集するエンドポイントデータの種類を教えてください。	CylancePROTECT	• CylancePROTECT の検知または検疫イベントからのバックトレースにより、ユーザーデバイス上で観測された時系列イベントをたどれる「ブレッドクラムトレイル」を提供
	ファイル	• ファイルの作成、変更、削除、名前変更イベントを、メタデータおよびファイル属性とともにキャプチャ • それぞれのファイルとプロセスの関係を関連付け • 代替データストリームを識別 • リムーバブルデバイスのファイルを識別
	プロセス	• プロセスの生成と終了のイベントをキャプチャ • モジュールロード • スレッドインジェクション • プロセスを、その所有ユーザーおよびイメージファイルと関連付け • プロセスを、そのすべてのアクティビティ（ファイル、レジストリキー、ネットワーク接続など）と関連付け
	ネットワーク	• IP アドレス • レイヤ 4 プロトコル • 発信元と発信先のポート
	レジストリ	• レジストリのキーおよび値の作成、変更、削除イベントをキャプチャ • マルウェアがシステムの再起動後も存続するために使用する、120 個以上の「パーシスタンスポイント」を識別 • レジストリキー／値を、作成したファイルプロセスと関連付け • 専用のパーサーで永続レジストリキー／値を、存続しようとするファイルと関連付け
	ユーザー	• 以前デバイスにログオンしたことのあるすべてのユーザーをキャプチャ • ユーザーと実行したアクション（作成、変更、削除イベントを含む）を関連付け • ユーザーと悪意のあるアクティビティを関連付け
	リムーバブルメディア	• リムーバブルメディアの挿入イベントを、コピー先／元ファイルおよび実行されたファイルとともにキャプチャ • デバイスの詳細をキャプチャ • リムーバブルメディアを変更したか、リムーバブルメディアからファイルをコピーしたプロセスを識別 • CylancePROTECT で検知されたマルウェアがリムーバブルメディアから侵入したかどうかを識別

[1] 収集されるエンドポイントデータ

質問	回答
CylanceOPTICS が収集したデータはどこに保存されますか？	CylanceOPTICS のデータはデバイスにローカル保存され、リクエストに応じてコンソールから参照されます。クラウドではなくローカルにデータを保存することによって、以下のことが可能になります。 • より多くの、より多様なシステムデータをキャプチャできる • 必要なクラウドストレージの容量を削減でき、専用ストレージなども不要になる • フォレンジックに関連のあるデータのみがクラウドに送信されるため、ネットワークトラフィックを削減できる
CylanceOPTICS は、EDR ソリューションと一緒に使用できますか？	技術的には、CylanceOPTICS を他の EDR 製品と一緒でも動作します。しかしながら CylanceOPTICS の利用を開始すると、CylanceOPTICS から得られる価値は他のセキュリティソリューションから得られる結果をはるかに凌駕していることにすぐ気付くでしょう。
CylanceOPTICS は、McAfee や Symantec などの製品と一緒に使用できますか？	CylancePROTECT はもともとレガシーのアンチウイルスプロバイダーなど他のセキュリティ製品と一緒に使用できるように設計されており、OPTICS を追加した場合でも同様です。

CylanceOPTICS の最小システム要件を教えてください。	• **メモリ** – 4GB
	• **空きディスク容量** – 500MB 以上（1GB を推奨）。CylanceOPTICS のインストールは少ない容量で済みますが、ローカルに保存される CylanceOPTICS のデータは、負荷の高いシステムでは 1 日あたり 100MB を超えることがあります。
	• **その他の要件**
	  • .NET Framework 4.5 SP1 以上
	  • 製品を登録するためのインターネット接続
	  • 製品をインストールするためのローカル管理者権限

サポートされているオペレーティングシステムを教えてください。	現在のところ OPTICS がサポートする OS は Windows のみとなっております。 Windows 7（32 ビットおよび 64 ビット） Windows 8（32 ビットおよび 64 ビット） Windows 10（32 ビットおよび 64 ビット） ※現在 Windows の Server OS についてはサポートしておりません。

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)

201712-FA001