CylanceOPTICS™

CylancePROTECT® 環境用の
インシデント防御 EDR

特長

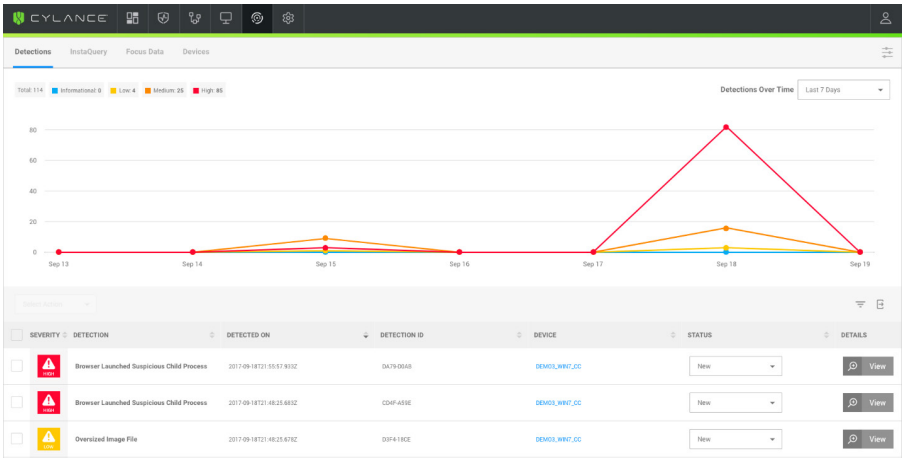
- **アラート量の削減**
  すべての領域にわたる脅威とインシデントの防御によりセキュリティアラートの量を削減し、チームの効率を向上
- **状況を的確に把握**
  環境全体にわたって攻撃対象領域を把握し、潜在的な弱点を解消
- **セキュリティチームにかかる負担の低減**
  セキュリティチームに負担をかけることなく、365 日 24 時間、識別された脅威に自動的に対処

予防ファーストのセキュリティ

シグネチャに依存する防御製品では、目まぐるしく変化する今日の攻撃に追従できず、セキュリティチームが日々大量のアラートの調査に追われる状況は変わりません。これではセキュリティ上の重大なリスクを見つけることはほぼ不可能であり、攻撃者は企業全体に蔓延したままです。

予防ファーストのセキュリティであれば、セキュリティスタックによって生成されるアラートの数を大幅に減らし、終わりのない無駄なアラート調査に伴う負担とフラストレーションを軽減できます。

CylancePROTECT がマルウェア、悪意のあるスクリプト、不正なアプリケーション、ファイルレス攻撃がビジネスに被害を及ぼすのを防止するのに対し、CylanceOPTICS は、データとビジネスのセキュリティ確保に必要な、AI（人工知能）を活用した EDR 機能を提供します。



CylanceOPTICS は、AI を使用してセキュリティインシデントを特定、防止することによって、CylancePROTECT が提供する脅威防御を拡張するよう設計された EDR ソリューションです。

導入や維持管理が難しいだけでなく使いづらい他の EDR 製品とは異なり、CylanceOPTICS には次のような特徴があります。

- エンドポイントに数分でインストールでき、ハードウェアやネットワークインフラ増強は不要
- データをエンドポイントにローカルに保存、分析することで、継続的な更新が不要で、遅延のない検知と対処を実現
- 静的な検知ルールでは見つけにくい脅威を発見することを目的とした、機械学習による脅威検知モジュールと自動アクション機能を提供

CylanceOPTICS は、CylancePROTECT と連携して、攻撃者の一歩先を行くために必要な検知および防御機能を提供し、ビジネスのセキュリティを確保します。

一般的な使用事例

- **悪意のあるアクティビティの阻止：**CylanceOPTICS の基盤を提供する CylancePROTECT は、エンドポイントを標的にした攻撃の成功を阻止することに特化して設計されています。
- **攻撃とアラートデータの調査：**あらゆるアラート関連アクティビティをわかりやすく可視化して、CylancePROTECT を含む他のセキュリティコントロールからのアラートを調査し、エンドポイントから有益な情報を取得できます。
- **企業全体の脅威の探索：**ネットワークエンドポイント全体でファイル、実行可能ファイル、ハッシュ値、および他の IOC を元に素早く検索し、隠れた脅威を発見できます。
- **エンドポイントでの脅威検知：**疑わしい動作や、エンドポイントの潜在的な侵害を示す他の指標は自動的に発見されます。
- **インシデントへの迅速で自動的な対処：**影響を受けたエンドポイントから重要なフォレンジック情報を取得できるほか、有害なエンドポイントが発見された場合は積極的な封じ込めを実施できます。さらに、事前定義ルールがトリガーされた場合、自動的に対処アクションを実行することもできます。

CylanceOPTICS の機能

AI 駆動型のインシデント防御
機械学習型脅威検知モジュールを使用して、行動ルールでは特定しにくい脅威を発見

企業全体での脅威ハンティング
疑わしい／悪意のあるアクティビティがないかどうかエンドポイントデータを簡単に検索して、隠れた脅威を発見

クロスプラットフォームでの一貫した可視性
Microsoft Windows と Apple MacOS の両プラットフォームでインシデントを検知、防御

動的な脅威検知
サイランスが提供する検知ルールやカスタムルールを使用して、リアルタイムでの脅威検知と対処を自動化

オンデマンドでの根本原因分析
攻撃が環境へ侵入する手口を把握して是正処置を講じることができるようにし、攻撃対象領域を縮小

迅速で自動的な対処
自動対処アクションをカスタマイズして、インシデントの拡大リスクを最小化

リモートフォレンジックデータの収集
疑わしいイベントやセキュリティインシデントに関連する重要な情報を高速にキャプチャ

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-DS002