CylanceOPTICS™の分散型の検索と収集のアーキテクチャ

機能紹介

CYLANCE

分散型の検索と収集

組織がエンドポイントの検知と対応（EDR）テクノロジーを導入する際の大きな課題の 1 つに、一般的な EDR 製品が収集する大量のデータの処理があります。

このデータは通常、クラウドのストレージ環境かオンプレミスの物理サーバーのいずれかに集約されます。どちらにしても、組織には EDR テクノロジーの使用に伴って継続的なコストが追加で発生します。

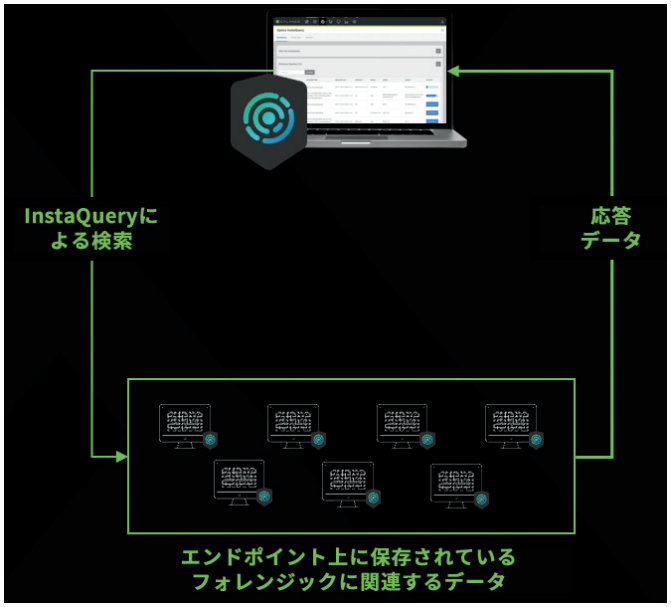
CylanceOPTICS では、そうしたコストを軽減するため、収集するデータのタイプと、データの収集、検索、分析方法を最適化するうえで、異なるデータ収集アプローチを取っています。

収集アプローチ

大容量のストレージが必要になる「すべてを収集する」データ収集アプローチを取る他の EDR テクノロジーとは異なり、CylanceOPTICS では、フォレンジックの観点からみて最も関連するデータだけに絞り込んで収集することに焦点を絞ったデータ収集アプローチを採用しています。例えば、ソリューションによっては、エンドポイントからすべてのレジストリ値を収集するものがありますが、これは、大局的な収集の見地からは合理的でも、セキュリティの見地からはあまり価値がありません。一般的なエンドポイントで有用なセキュリティ情報を提供するレジストリ値は、多くても 500 個程度です。CylanceOPTICS では、このようにより小規模なレジストリキーのセットに焦点を絞って監視します。それらのキーのいずれかが変更されると、CylanceOPTICS がそのデータを収集します。これは CylanceOPTICS のアプローチが他の EDR 製品とは異なる理由の一例にすぎません。さらに焦点を絞った重要なデータセットを提供することで、セキュリティアナリストが手動で検索し、自動的に脅威を検出するために利用できるようにします。

分散型の収集アプローチ

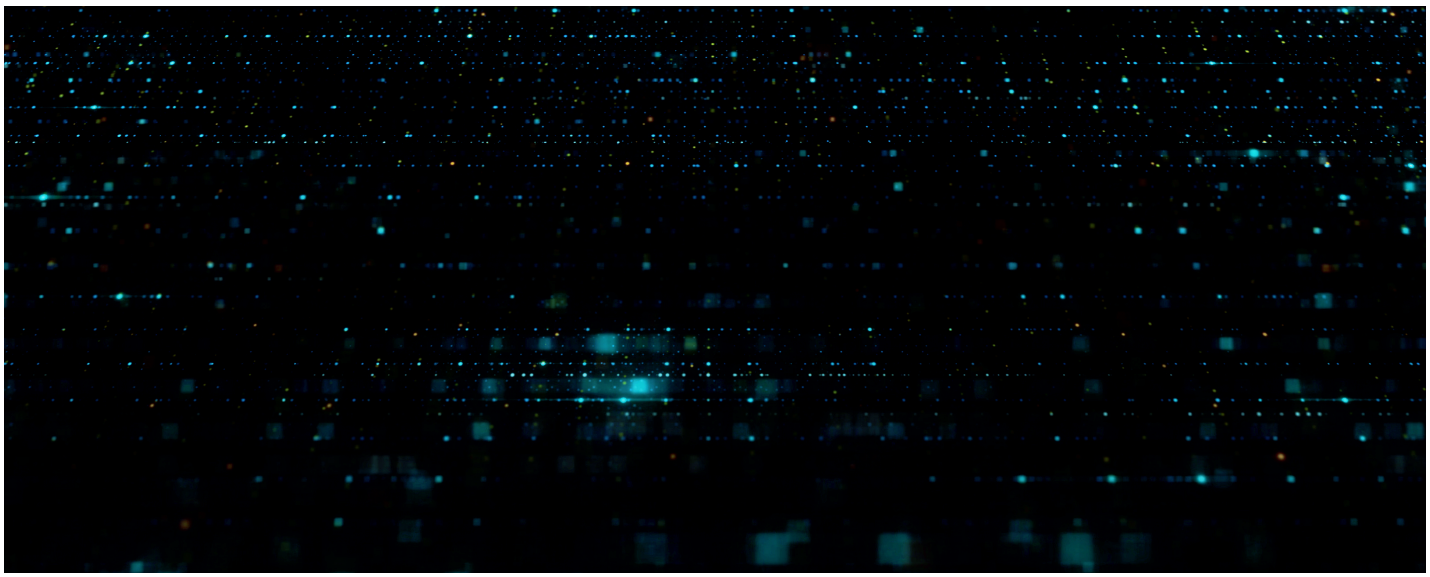
CylanceOPTICS は、フォレンジックに関連するエンドポイントデータの検索と収集の両方を最適化するために設計されました。エンドポイントで生成されるすべてのデータを強制的に収集し、クラウドやオンプレミスのサーバーに集約する他の EDR 製品とは異なり、CylanceOPTICS は各エンドポイントでローカルにデータを保存します。保存されるデータ容量はエンドポイント 1 台あたり



1 GB で、これは非常にアクティブなエンドポイントでのおよそ 10 日分のアクティビティ、そして、それほどアクティブでないエンドポイントでのおよそ 20 日分に相当します。このアプローチによって、組織は、他の EDR 製品を購入して使用する場合にかかることの多い追加のデータストレージコストを回避できます。

検索アプローチ

エンドポイントでローカルにデータが保存される CylanceOPTICS では、検索アプローチも他の EDR 製品とは異なります。CylanceOPTICS では、エンドポイントで検索が行われ収集された応答データのみがクラウドに保存されます。例えば、セキュリティアナリストが、会社のエンドポイントのいずれかで特定のファイルが高度な攻撃の兆候として検出されていないかどうかを確認したい場合、そのアナリストは、クラウドベースの管理コンソールの InstaQuery（IQ）インターフェイスから検索を行うことができます。そのクエリは、各エンドポイントで実行されている CylanceOPTICS サービスに送信されます。すると、CylanceOPTICS サービスが、エンドポイント上に保存されているデータの検索を実行し、すべての応答アイテムを収集します。そして、それらのアイテムだけがクラウド環境に送信され、セキュリティアナリストが調査を続行できるというわけです。これにより、検索を行うために必要な帯域幅とデータストレージを抑えることができます。



技術的な詳細の概要

CylanceOPTICS では次のデータが収集されます。

CylancePROTECT®	CylancePROTECT イベントからのバックトレースにより、デバイスで観測されたマルウェアまでたどれる「ブレッドクラムトレイル」をユーザーに提供
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一緒に収集 ファイル - プロセス関係を関連付け 代替データストリームを識別（MacOS でのリソースフォーク） リムーバブルデバイスのファイルを識別
プロセス	プロセスの作成および終了イベントを収集 モジュールロードを収集 スレッドインジェクションを収集 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 プロセスがデバッグされているかどうかを確認 プロセスがリムーバブルメディアを使用しているかどうかを確認
ネットワーク	IP アドレス レイヤ 4 プロトコル Wi-Fi 無線 可視アクセスポイント Bluetooth 無線およびデバイス HOST ファイルの入力と変更 DNS キャッシュ ARP キャッシュ 静的および動的ルート ネットワークインターフェイス
レジストリ	レジストリのキーおよび値の作成、変更、削除イベントを収集 120 個以上のパーシスタンスポイント（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場所）を識別 レジストリキー／値を、作成したプロセスと関連付け 遅延した削除ファイルを識別 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収集 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一緒に収集 デバイスの詳細を収集 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

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)

201803-FF010