データシート

Endpoint Detection and Response Cloud

エンドポイントを可視化し、脅威検出を自動化

概況

検出 – 環境にそぐわないアノマリーを検出

- 基準となる活動から逸脱しているソフトウェア、ユーザー、ネットワークのアノマリーを検出
- タイムラインとパス分析を使用して複数フェーズ攻撃を検出
- プロセスメモリの分析により、メモリベースの攻撃を特定

自動化 – 熟練した調査員のベストプラクティスを活用

- 自動化されたインシデント対応プレイブックルールにより、熟練した調査員のベストプラクティスと分析を再現
- アーティファクトを自動収集し、エンドポイントでの活動を詳細に把握
- サイバーセキュリティ機能を開始し、ビルトインされたプレイブックで専門家の調査方法を学習

可視化 – 大量のサイバーデータを実用的な結果に変換

- ビジュアルリンク分析により、関連づけられていないデータタイプ間のコンテキスト関係を把握
- グラフィカルな警告を使用してインシデントの発生源、タイミング、影響を迅速に確認
- 関連性のある活動に集中できるよう、エンドポイントに関する大量の測定データをインタラクティブなグラフィックに変換

はじめに

セキュリティ部門は、時には 190 日も自社のの環境に潜伏する高度な攻撃に直面しています[1]。さらに、盗まれた資格情報を利用して正当なユーザーを装うなど、ステルス技術を利用して企業の環境内で自由に行動する攻撃者が増加しています。ゼロデイ脆弱性の発見がわずかに減少する一方で、従来のような脆弱性の組み合わせに依存しない「ツールの現地調達」戦術をとるマルウェアが増加しています。これらの戦術では正当なツールが使用されるため、検出は困難を極めます[1]。

企業は脅威を気づかずに放置することがないよう、新しい検出のアプローチを必要としています。さらに、深く掘り下げた調査を実施できる熟練した担当者を採用するのは難しく、費用もかかります。たとえそのようなスキルを持つ従業員が在籍していても、慰留できるとは限りません。

EDR Cloud の概要

Symantec Endpoint Detection and Response（EDR）Cloud は企業全体でエンドポイントを詳細に可視化し、脅威検出とセキュリティ侵害への対応を自動化します。Symantec EDR Cloud は、わずか数分で配備できるクラウドベースのサービスであり、サイバー攻撃に対する企業のセキュリティ体制を強化します。経験豊富なセキュリティアナリストのスキルとベストプラクティスをすべての企業にもたらすさまざまなルールやユーザーふるまい分析が搭載されているため、調査担当者の生産性が向上し、大幅なコスト削減が実現します。

セキュリティチームは、フォレンジック分析やステルス性の高い脅威を検出できるビルトインされたプレイブックを使用して設定変更が可能なポイントタイムスキャン機能により迅速に調査を開始できます。また、エージェントを追加で配備する必要はありません。

環境にそぐわないアノマリーを検出

Symantec EDR Cloud は、ソフトウェア、メモリ、ユーザー、ネットワークの基準となる活動の全体像を提示するため、環境内に潜む攻撃者を簡単に検出できます。攻撃者が環境内で活動すると、そのマルウェアやユーザー活動がアノマリーとして浮き上がります。Symantec EDR Cloud は、環境内で以下のようなアノマリーを検出します。

- ソフトウェアのアノマリー – 一般的ではないソフトウェアがインストールされている、ビルドの不一致、パッチ未適用、オペレーティングシステム（OS）のリリースが古いといった問題があるエンドポイントを検出
- メモリのアノマリー – プロセスメモリ、ファイルおよび OS オブジェクト、システム設定のフォレンジック調査により、メモリに存在するアノマリーを検出
- ユーザーのアノマリー – ユーザーふるまい分析により、正当なユーザーを装う攻撃者の不審な活動を検出
- ネットワークアノマリー – 統計分析を活用して異常な IP アドレスを特定。レピュテーション検索により情報漏えいに関連している IP アドレスとドメインを特定

これに加え、Symantec EDR Cloud にはファイル、ユーザーアカウント、ネットワーク接続のリスクスコアを測定する複数の脅威エンジンが含まれています。検出機能には以下の機能もあります。

- 数百万件もの安全なファイルと悪質なファイルを使用したニューラルネットワークベースの機械学習
- 顧客から提出された脅威インテリジェンスソースと第三者の脅威インテリジェントソース
- レジストリの変更の調査とスケジュールされたタスクによる持続的な脅威の特定
- 複数のマルウェア対策エンジン

熟練した調査員のベストプラクティスを活用

Symantec EDR Cloud は、セキュリティアナリストがとる複数のステップで構成された複雑なワークフローを自動化するプレイブックをサポートしています。ビルトインされたプレイブックにより、疑わしいふるまい、未知の脅威、水平移動、ポリシー違反が迅速に検出されます。セキュリティ担当はプレイブックを確認して、専門家の捜索手法や調査手法を学ぶことができます。さらに、調査担当者は独自のプレイブックを作成して、ベストプラクティスやドキュメント固有の脅威検出シナリオを自動化できます。

大量のサイバーデータを実用的な結果に変換

Symantec EDR Cloud は視覚的にも優れています。インタラクティブなグラフィックを備えたビジュアルリンク分析を搭載しているため、セキュリティ専門家は新たな方法でコンピュータとネットワークのデータを使用し、関連付けることができます。

機械支援の分析により、あらゆる関連データを大規模に操作できます。また、リンク分析により、異なるデータタイプ間の複雑な関係から概念的な関連付けを迅速に実行できます。

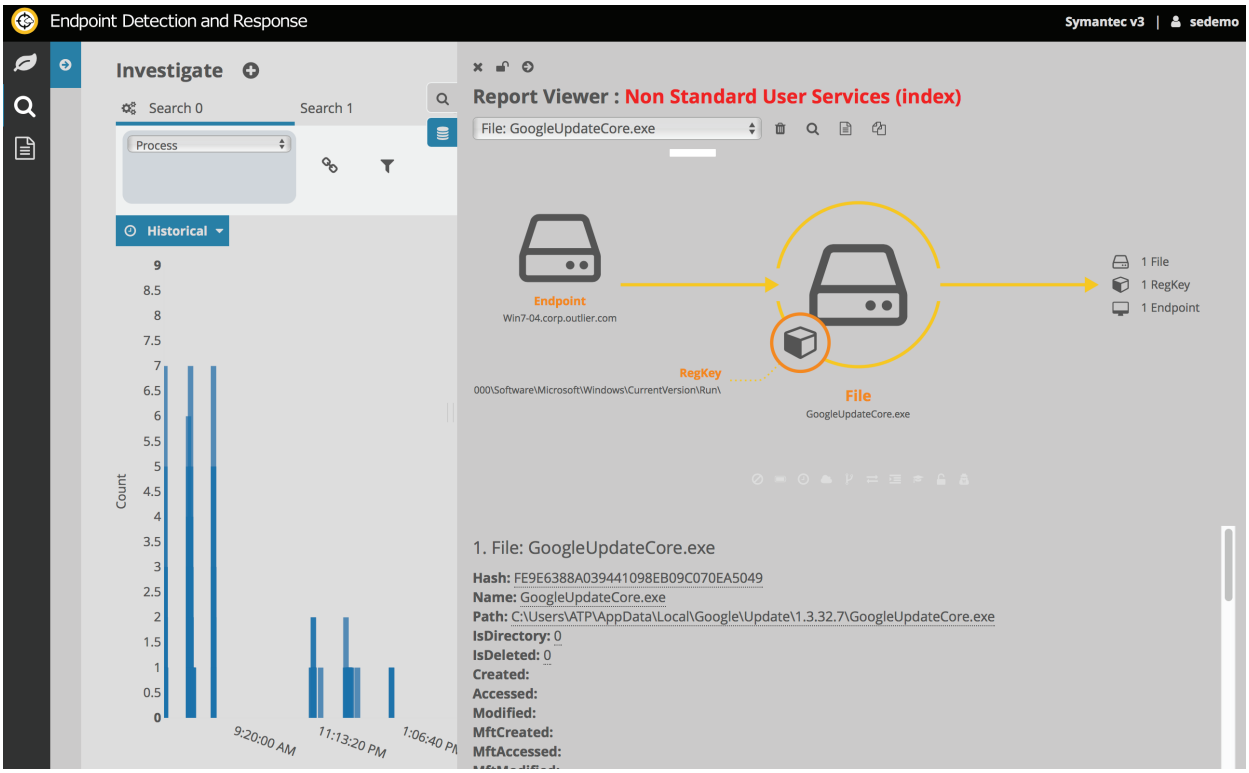
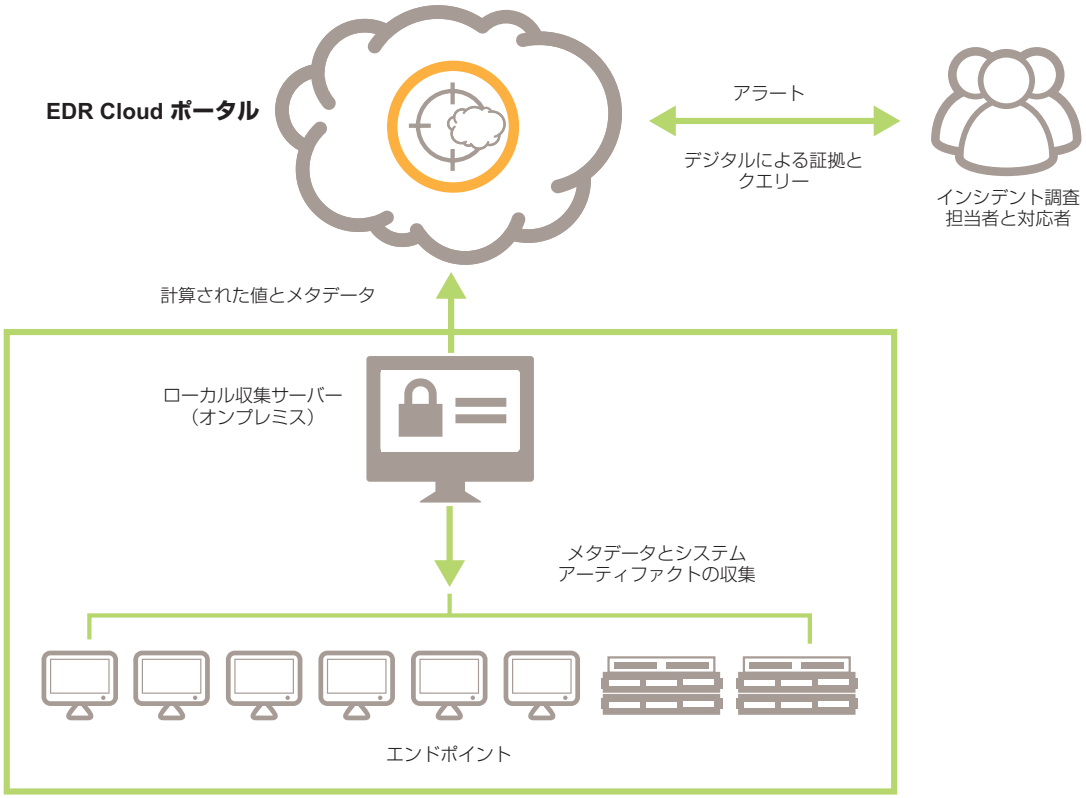


図 1.複雑なサイバーデータを可視化する Symantec EDR Cloud の強力なツール

しくみ

以下の図に示すように、Symantec EDR Cloud は調査担当者用のポータルと 1 台以上の収集サーバーで構成されています。ポータルは調査担当者のインターフェースとなり、セキュリティ分析を実行します。このソリューションはエンドポイントからデータを収集し、検出のためにそのデータを分析して、企業への問い合わせや感染システムの修復に使用できるツールを提供します。

Endpoint Detection and Response Cloud



オンプレミスのサーバーがコンピュータから重要なフォレンジックデータを継続的に収集します。収集対象のデータには、不明なファイル、プロセスのメタデータ、プログラム、サービス、モジュール、ファイル、自動実行、ユーザーのふるまい、ネットワーク接続、タイムラインなどがあります。データ収集はパッシブであり、60 秒以内に行われ、エンドユーザーの環境には影響しません。

要件

ブラウザの UI の要件

バージョン 2.9 は Silverlight に依存し、Microsoft Internet Explorer 11 以降が必要

バージョン 3.0 は Mozilla Firefox 26 以降と Google Chrome 32 以降にも対応

収集サーバーの要件（データ保管庫）

Windows 7 から Windows Server 2016

VMware、HyperV の仮想サポート

エンドポイントの要件

Windows XP 以降

macOS Sierra、El Capitan、Yosemite

Redhat Linux 7.0 以降、32 ビット版および 64 ビット版

CentOS、Mint、Cinnamon、32 ビット版および 64 ビット版

参照情報:

1. シマンテックインターネットセキュリティ脅威レポート vol.22

シマンテックについて

シマンテックコーポレーション（NASDAQ: SYMC）はサイバーセキュリティ業界をリードする世界的企業です。さまざまな場所に保管されている大切なデータを守るため、企業や政府機関、個人のお客様を支援しています。エンドポイントからクラウド、インフラまでを高度な攻撃から守るため、世界中の企業がシマンテックの戦略的統合ソリューションを選択しています。また、世界中で 5 千万以上の個人やご家庭が、自宅などで使用するデバイスそしてデジタルライフを守るために、ノートンと LifeLock 社の製品を使用しています。シマンテックのサイバーインテリジェンスネットワークは民間が運営するネットワークとしては世界最大規模を誇ります。このネットワークが、先進的な脅威をいち早く発見し、お客様を守ります。詳しくは www.symantec.com/ja/jp/ をご覧ください。

〒107-0052 東京都港区赤坂1-11-44 赤坂インターシティ | www.symantec.com/ja/jp/

SYMC-DS-EDR_Cloud-JP-v1-bb