



NETPROTECT

通信事業者およびISP向けESET NetProtect技術概要

モバイルネットワークと固定ネットワーク内の
接続デバイスのためのシームレスなネット
ワークセキュリティ

Progress. Protected

ESET NetProtectは、通信事業者およびISP企業向けのDNSフィルタリングソリューションを実装し、次のような特定の基準に基づいてドメインへのアクセスをフィルタリングおよびレポートすることで、ユーザーに追加のセキュリティレベルを提供します。

- ✔ ESETドメインフィード(マルウェア対策、フィッシング対策、望ましくない可能性のあるコンテンツ)
- ✔ 通信事業者およびISPの設定、設定、カスタムホワイトリスト/ブラックリスト
- ✔ エンドユーザー自身のホワイトリスト/ブラックリスト
- ✔ Webコンテンツフィルターは、アダルト、アルコール、ショッピングなどのカテゴリに基づいてWebサイトをフィルタリングするために使用されます。

主な特徴

- ✓ マルウェア対策保護
- ✓ フィッシング対策保護
- ✓ 望ましくない可能性のあるコンテンツの保護
- ✓ Webコンテンツフィルター
- ✓ ホワइटリスト/ブラックリスト
- ✓ セキュリティレポート
- ✓ ライブイベントと統計
- ✓ 顧客管理ポータル
- ✓ 通信事業者およびISP管理ポータル

保護設定

不正使用防止フィルター

DNSリゾルバーのパフォーマンスを損なったり、ユーザーエクスペリエンスを低下させたりする可能性のある不正なDNSトラフィックを防ぐために使用できる強力な機能。不正使用防止フィルターは、一連の構成可能なDNSトラフィックルールで構成されており、これらを連鎖させて、DNSパケットの内容と関連するメタデータに基づいて高度な動作を形成できます。

DNSフィルタリング用のオフネットアプリケーション(AndroidおよびiOSで利用可能)

通信事業者およびISPネットワークの外部(公共Wi-Fi、コーヒーショップなど)で接続している顧客を保護します。

ESET NETPROTECTで得られるもの



高いパフォーマンス



高可用性



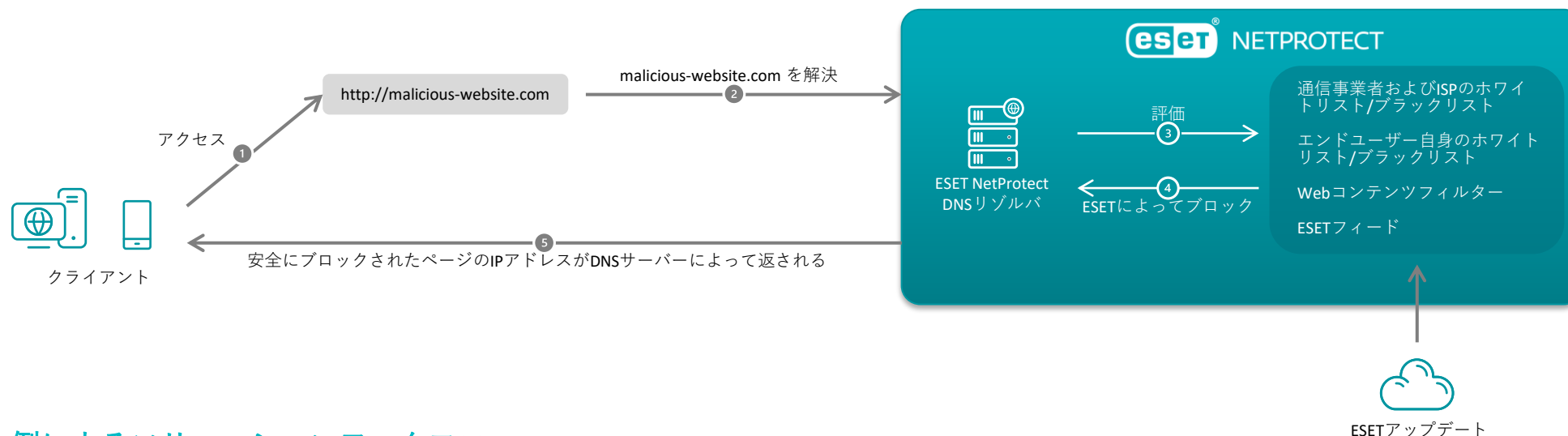
高い拡張性



受賞歴のあるセキュリティ

その他の機能

- **Kubernetes**プラットフォーム上に構築されたマイクロサービスを使用して、高性能、高可用性、高スケーラビリティを実現するソリューション
- 基盤となるインフラストラクチャやプラットフォームから分離された、**完全にコンテナ化された安全なアーキテクチャ**
- **Elastic-ELK**の業界標準ツール(Elasticsearch、Logstash、Kibana)を使用したりアルタイムのソリューション監視、アラート、データ分析
- あらゆる規模で簡単に導入可能
- のソリューションと対話できるカスタムモジュール(**マイクロサービス**)を作成する能力
- 当社のソリューションと対話するための**豊富な REST API** と gRPC API
- **保護の一時停止** – サイレントモードで実行するオプション機能(悪意のあるドメインは報告されるだけで、ブロックされません)
- ESET NetProtectは、セキュリティレポートを使用して顧客への定期的な電子メールを生成するための**SMTP**およびカスタムAPIをサポートします。
- **プライバシーへの強いこだわり** – 当社のソリューションは、お客様の個人データを必要とせず、匿名化された環境で作業できます



例によるソリューションワークフロー

DNS(Domain Name System)は、人間が読めるドメイン名をIPアドレスに変換したり、別の種類の情報を要求したりするために使用される分散データベースです。よく知られているドメインの例としては、`github.com`、`youtube.com`、`tiktok.com`、... などがあります。

たとえば、ユーザーが自分のインターネットブラウザから `http://malicious-site.com` にアクセスしたい場合(この例では、このドメインを悪意のあるドメインと見なします)、

- ブラウザは、事前定義されたDNSサーバーに、`malicious-site.com` からIPアドレスへの変換を実行するように要求します
- ドメイン名は有効なIPアドレスに正常に変換されます
- その後、ブラウザは解決されたIPアドレスに対してリクエストを実行します
- `malicious-site.com` のコンテンツがダウンロードされ、ユーザーに表示されます

ESET NetProtectでの同じシナリオ

- ブラウザーは、ESET NetProtect DNSサーバーに `malicious-site.com` からIPアドレスへの変換を実行するように要求します
- ドメインの評判を認識し、ユーザーと電話会社/ISPの設定を入力するために、さまざまなフィードが評価されます
- ブロックされたページのIPアドレスが返されます
- ユーザーは安全なWebサイト(ブロックされたページ)にリダイレクトされ、詳細な説明とリスクを受け入れて続行する可能性が表示されます

ESET NetProtectは、ユーザーまたはデバイスがアクセスする前にすべてのドメインの検証を実行し、悪意のあるドメインまたは特定の電話会社/ISPまたはユーザー条件に一致するドメインへのアクセスをブロックして報告します。

統合とデプロイ

ESET NetProtectソリューションは、Canonical microk8s、Red Hat OpenShift、Azure AKS、Azure ARO、Amazon EKS、Google Kubernetes Engineなど、すべての主要なKubernetesディストリビューションとクラウドソリューションをサポートする最新のKubernetesマイクロサービスアーキテクチャを使用して構築されています。

このソリューションは、次の規模であらゆる規模で簡単にデプロイできます。

- オンプレミス展開
- プライベートクラウド(仮想化環境)
- パブリッククラウド

一般的なデプロイメントでは、各コンポーネントは異なる物理ノードでペアで実行され、高可用性、スケーラビリティ、コンポーネントのアップグレード中のダウンタイム0%を実現します。

通常、ESET NetProtectは、簡単なインストールのためにHELMチャートとして配布されます。ESET支援デプロイメントを含む、ソリューションをデプロイするための多くのオプションがあります。

各通信事業者/ISPは、特定の領域で異なる技術スタックを展開し、異なる設定を持つことができます。既存のシステムとのシームレスな統合のための実装サポートを提供することができます。

以下に、カスタマイズが必要なコンポーネントを示します。

- AAA(Authentication, Authorization, and Accounting)システムとの統合:
 - RADIUSアカウント開始/停止パケットの処理、
 - RADIUSアカウント開始/停止ログの処理、
 - DIAMETERアカウント開始/停止ログの処理、
 - 他のAAAシステムとの統合が可能、
- 既定では、ISP/TelcoおよびCustomer Management PortalはESETによって提供されません
 - デザインのカスタマイズ可能
 - UI機能を有効/無効にすることが可能
- RESTおよびgRPC APIはESETによって提供され、ESETソリューションとの完全な相互作用を可能にします
 - ソリューションをTelco/ISPのカスタムWebポータル、モバイルアプリケーション、自動化システムと直接統合することが可能
- オフネットモバイルアプリケーションが利用可能
 - デザインのカスタマイズ可能
 - UI機能を有効/無効にすることが可能

DNSリゾルバの可能な構成

当社のソリューションの再帰DNS解決機能の設定方法には、複数のオプションがあります。

- ◆ デフォルトでは、当社のソリューションには、再帰的なDNS解決を実行するために使用される再帰的なキャッシングDNSリゾルバが付属しています
- ◆ 当社のソリューションがDNSクエリをTelco/ISP再帰DNSリゾルバに転送する構成は可能であり、検討する必要があります

Secure DNS リゾルバーは現在、次の DNS プロトコルをサポートしています (設定に基づくアクティブ化/非アクティブ化)

- DNS over UDP トランスポート (UDP ポート 53)
- DNS over TCP トランスポート (TCP ポート 53)
- DNS over TLS (TCP ポート 853)
- DNS over HTTP/2 (TCP ポート 443)

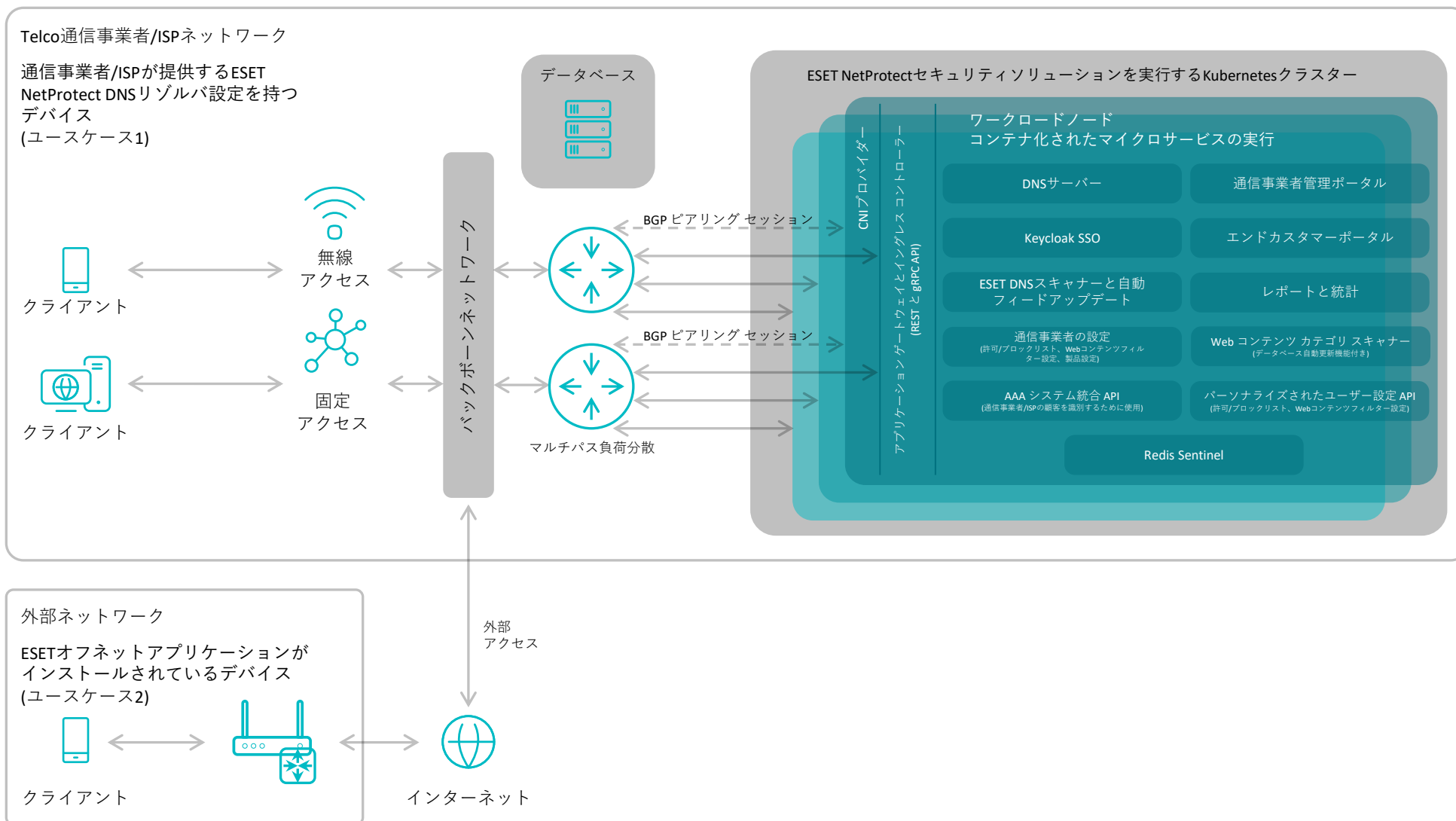
ハードウェアとソフトウェアの要件

最小ハードウェア要件は異なり、予想されるDNSサーバーの負荷(DNSクエリ/秒、DNSトラフィックの種類など)に直接関連しています。

最小限の技術要件は、以下に基づいています。

- ◆ 1秒あたりの DNS クエリの予想数 (既存の DNS サーバー統計が存在する場合は、その統計から)
- ◆ 1秒あたりの DNS クエリ数に関する統計がない場合、平均負荷を計算するには、予想される顧客数が必要です

高可用性を実現するには、少なくとも3ノードの Kubernetes クラスターが必要ですが、他のセットアップも可能です。お客様がソリューションをオンプレミスで実行することを希望し、Kubernetesを利用できない場合は、完全なセットアップ(Kubernetes + ESET NetProtect)を提供できます。



用語集

◆**マルウェア対策保護** — 悪意のあるソフトウェアとして分類されたファイルを含むドメインへのアクセスからユーザーを保護します。これらのファイルは、インストール後に、感染したデバイスへのリモートアクセスを提供したり、デバイスから機密データを漏洩させたり、ターゲットデバイスに損害を与えたり、デバイスの所有者にその他の損害を与えたりする可能性があります

◆**フィッシング対策保護** — 不正なWebサイトがユーザー名、パスワード、銀行の詳細などの機密情報を取得したり、一見信頼できるソースからフェイクニュースを配信したりしようとする試みから、プライバシーと資産を保護します。ホモグラフィ攻撃(リンク内の文字を似ているが実際には異なる文字に置き換える)からユーザーを保護します

◆**望ましくない可能性のあるコンテンツ保護** — 疑わしいドメインや不要なコンテンツをホストしているWebサイトからユーザーを保護します

◆**DNS(ドメインネームシステム)** — 人間が読めるドメイン名をIPアドレスやその他の情報に変換するために使用される分散型データベース

◆**IPアドレス** — 192.0.2.1などの数値ラベルで、以下に接続されています。通信にインターネットプロトコルを使用するコンピュータネットワーク

◆**通信事業者/ISP** — インターネット接続サービスを提供する電気通信会社

◆**通信事業者/ISP管理ポータル** — 通信事業者/ISPがESET NetProtectの動作を設定するためのWebアプリケーション

◆**顧客管理ポータル** — エンドユーザー(通信事業者/ISPのお客様)がESET NetProtectの動作を設定するためのWebアプリケーション

◆**オフネットアプリケーション** — 通信事業者/ISPネットワーク(公共Wi-Fi)の外部で接続するユーザーに追加のセキュリティを提供するAndroidおよびiOSアプリケーション

◆**Webコンテンツフィルタ** — ドメインを分類して、特定のドメインカテゴリをブロックまたは許可できるようにするために使用されます。ドメインカテゴリの例としては、アダルト、アルコール、ショッピングなどがあります。

◆**ドメインフィード** — カテゴリに属するドメインのソース

◆**Kubernetes または K8s** — コンテナ化されたアプリケーションのデプロイ、スケーリング、管理を自動化するためのオープンソースシステム

◆**コンテナ** — コードとそのすべての依存関係をパッケージ化するソフトウェアの標準単位であり、アプリケーションをあるコンピューティング環境から別のコンピューティング環境へ迅速かつ確実に実行できます

◆**マイクロサービス** — ソフトウェア開発に対するアーキテクチャ的および組織的なアプローチで、ソフトウェアは明確に定義されたAPIを介して通信する小さな独立したサービスで構成されています

◆**HELMチャート** — 最も複雑なKubernetesアプリケーションもインストールおよびアップグレード



ESETは最先端のデジタルセキュリティで攻撃を未然に防ぎます。ESETのAIと人間の専門知識の組み合わせにより、既知および未知のサイバー脅威を防ぎ、企業、重要インフラ、そしてユーザーを保護します。AIを活用したクラウドファーストのESETのソリューションとサービスは、エンドポイント、クラウド、モバイルのいずれの分野においても、優れた効果と利便性を発揮します。ESETのテクノロジーには、堅牢な検知・応答、極めて安全な暗号化、そして多要素認証が含まれます。24時間365日体制でリアルタイムに攻撃を防ぎ、お客様一人ひとりに合わせた強力なサポートを提供し、ユーザーを保護し、サイバー攻撃による業務の中断を防止します。デジタル環境が常に進化し続ける中で、セキュリティにも先進的なアプローチが求められています。ESETは、研究開発センターと強力なグローバルなパートナーネットワークを活用し、世界最高クラスの調査研究と強力な脅威インテリジェンスを提供しています。

www.eset.com/jp