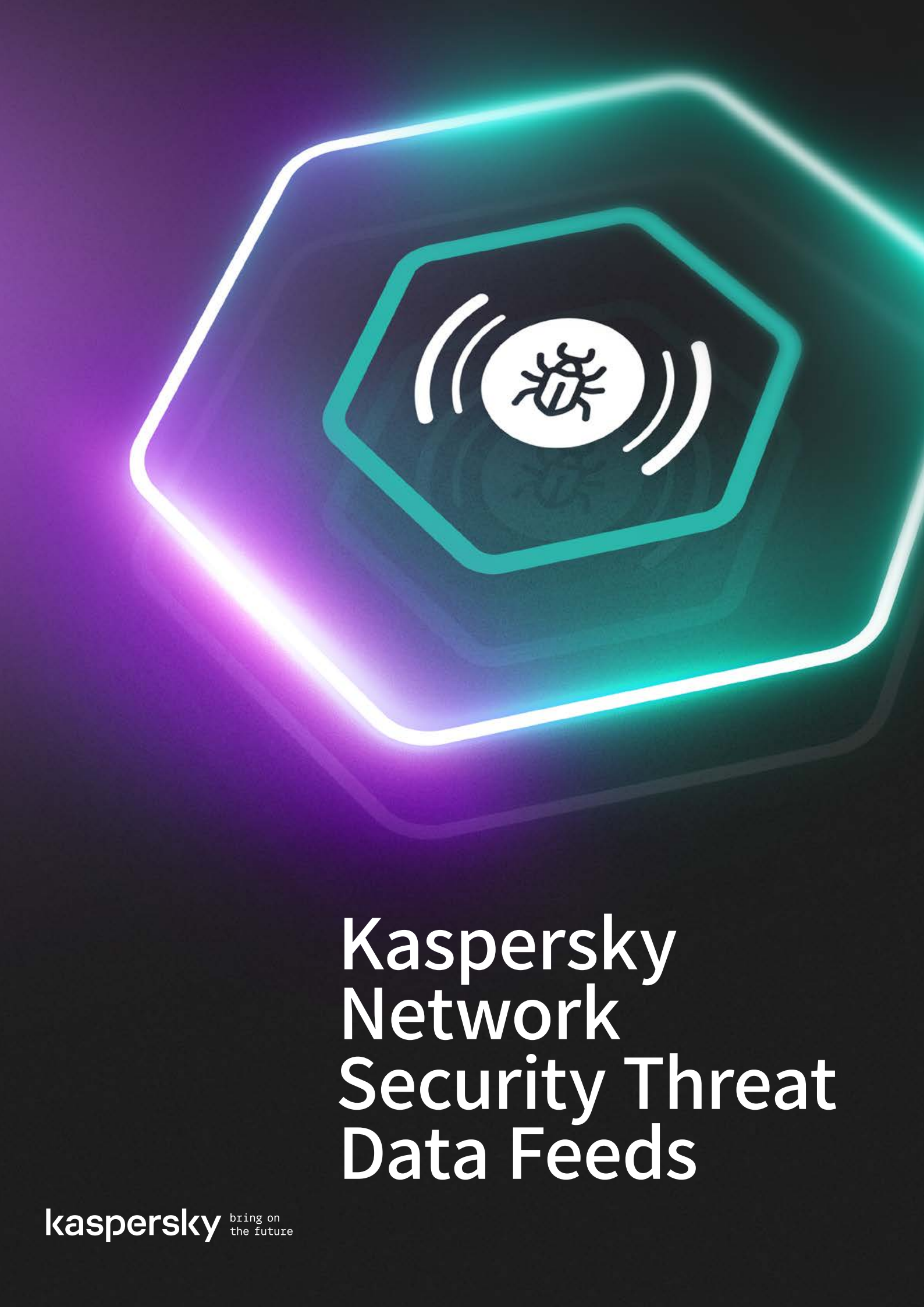


Kaspersky Network Security Threat Data Feeds

kaspersky bring on the future

エンドポイント保護だけでは、組織や企業を十分に保護することはできません。

ネットワークレベルでの保護も必要です。

その理由を説明します：

- 各種の攻撃からの保護は、多層構造で構成する必要があります
- 環境内のすべてのホストがエンドポイントセキュリティ保護機能を実装しているとは限りません。 たとえば、産業用ネットワーク上の一部のビジネス上の重要度が高いサーバーやホストには実装されていない可能性があります
- 一部の「保護対象」のホストは、シグネチャ/ハッシュ/検知ルールが最新の状態に更新されていない可能性があります

Kaspersky Network Security Threat Data Feeds

今日では、ほとんどすべての企業が次世代ファイアウォール（NGFW）を導入しています。これは、サイバー攻撃に対する企業ネットワークの保護レベルを向上させる、最も効果的な最新のネットワークセキュリティ対策の1つです。

NGFWの大半は、サイバー脅威に関する社内の知識を活用できるだけでなく、外部ソースからのセキュリティ侵害インジケーター（IoC）の動的リストを使用して、サイバー脅威をリアルタイムでブロックできる機能を搭載しています。

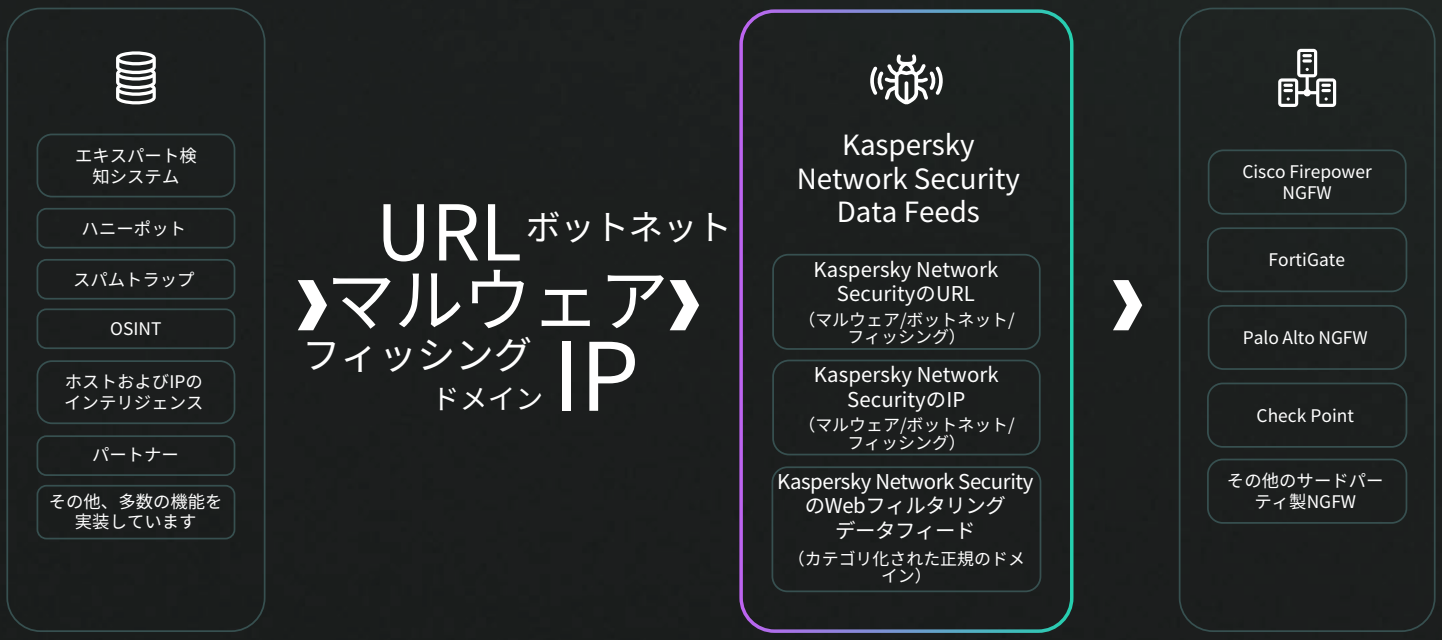
攻撃者の機先を常に制することが可能なほど迅速に、NGFWの検知ルールを設定するという運用は、実現性が極めて乏しい話です。そのため、外部の脅威インテリジェンスの知識が不可欠となります。これにより、組織の環境を保護する重要な要素が1つ追加されることになりますが、この事実を見落としている場合もあるかもしれません。

Kasperskyは、専用のIoCのコレクションを作成しています。これをNGFWにインポートすると、最も蔓延している脅威から企業ネットワークを保護するセキュリティレベルが大幅に向上します。複雑な組み込み作業や設定は不要であり、現在のネットワーク構成も維持したままの導入が可能です。

Kaspersky Network Security Threat Data Feedsは、Kaspersky Threat Intelligence Data Feedsを基にしており、各種のIoC（IPアドレスとドメイン）のリストを定期的に更新して提供しています。この情報を使用することで、危険なネットワークリソースへのユーザーアクセスを監視/ブロックすることができます。

詳細はこちら

Kaspersky Network Security Threat Data Feedsとの連携



データ収集と処理

Kaspersky Network Security Data Feedsは複数のリストで構成されており、それぞれ特定の種類のサイバー脅威に重点を置いています。フィードには、最も高い脅威スコアを持つIPアドレスのリストと、マルウェアの配信、ボットネットのコマンド&コントロールセンター（C&C）としての動作、フィッシングリソースのホスティングなどの挙動が知られているリソースのトップレベルドメインとセカンドレベルドメインが含まれています。

データフィードは、Kaspersky Security Network、当社のプロアクティブなWebクローラー、ボットネット監視サービス（ボットネットとその標的および活動を24時間365日監視）、ホストとIPインテリジェンスサービスなど、多様かつ信頼性が高い複数の情報源を組み合わせて集約されます。

集約されたすべてのデータは、リアルタイムで慎重に検査され、統計的基準、サンドボックス、ヒューリスティックエンジン、類似サンプル検索ツール、ふるまいのプロファイリング、アナリストによる検証、許可リストの検証など、複数の再処理技術を使用して精製されます。

主な機能

リアルタイムの更新

データフィードは、世界中の調査結果に基づいてリアルタイムで自動的に生成され、高い検知率と精度を実現します。

Kaspersky Security Networkはインターネットトラフィックの大部分を可視化し、そのユーザー数は213か国以上で数千万人に上ります

ネイティブサポート

最も普及しているNGFWのネイティブサポート：

- Cisco
- FortiGate
- Palo Alto
- その他のサードパーティ製NGFW（外部動的リスト機能と基本的な認証サポート機能付き）

セキュアな認証

データフィードには幅広い種類の認証方法があり、多様なセキュリティニーズや統合の好みに応じた選択が可能です

容易な設定

サポート対象の各種NGFWを補足する段階的な設定ガイドとKasperskyのテクニカルサポートにより、設定作業に時間をかけることなく、本サービスの真価をすぐに体感いただけます

継続的な可用性

すべてのフィードは、高度な耐障害性を持つインフラによって生成および監視されており、継続的な可用性を確保しています

100%検証済みのデータ

誤検知が多いデータフィードは、正当なリソースをブロックしてしまう可能性があるため、有害です。

Kaspersky Network Security Data Feedsは、フィードを公開する前に広範なテストとフィルタリングを適用し、100%検証済みのデータが配信されます

メリット

ネットワーク防御ソリューションを強化

継続的に更新されるIOCにより、最も蔓延しているサイバー脅威を自動的にブロックします

資産の流出を防止

感染したマシンから、機密性が高い資産や知的財産が組織外へ流出するのを防止します

サイバー脅威を迅速にブロックして組織を保護

組織をサイバー脅威から保護し、事業継続性を維持します

Kaspersky Threat Data Feeds

詳細はこちら

www.kaspersky.co.jp

#kaspersky
#bringonthefuture