KASPERSKY

Kaspersky Web Traffic Security

社内ネットワーク全体に対する戦略的防御

プロキシサーバーは、企業のインフラストラクチャと外界の間を行きかう Web トラフィックの通り道です。ここにセキュリティソリューションを戦略的に配置することで、脅威を早期かつ比較的容易に封じ込めるチャンスが生まれます。

Kaspersky Web Traffic Security は、プロキシサーバーと一体化されるアプリケーションで、企業の IT ネットワークを、World Wide Web の危険から保護すると同時に、インターネットの利用を統制し、生産性を向上させます。また、企業のセキュリティポリシーに従って、行きかう Web トラフィックを処理し、危険なものをすべてブロックします。Kaspersky Web Traffic Security は、境界セキュリティとしての機能の幅広さと脅威からの保護における卓越した品質で企業のインフラストラクチャを守ります。

特長

- リアルタイムのマルウェアやフィッシングに対抗する次世代の保護ソリューション
- 危険なファイルの侵入やデータ漏洩を防ぐコンテンツフィルタリング
- 負荷の高いネットワークに合わせた拡張が可能
- ゼロアワー脅威に対する保護
- Kaspersky Security Network のグローバルな脅威インテリジェンスによる支援
- Microsoft Active Directory のサポート
- 管理範囲を各ロールごとに設定
- Web リソースの利用をウェブコントロールで管理
- ランサムウェアは、ネットワーク侵入前にブロック
- MSP や多様化した企業に向けたマルチテナント管理機能のサポート

利点

感染のリスクを大幅に下げ、業務への悪影響を回避

Kaspersky Web Traffic Security は、侵入してくる脅威の大半をゲートウェイレベルで食い止めることにより、エンドポイントへの到達を阻止し、エンドユーザーやワークステーションへの潜在的影響を大幅に緩和します。

企業ゲートウェイの保護効率を劇的に強化

セキュリティ業界最強の保護テクノロジーを備え、卓越した検知率とほぼゼロに近い誤検知率を誇る Kaspersky Web Traffic Security アプリケーションは、ご使用中の Web ゲートウェイ対策にとって最高の援軍となり、保護の強度をめざましく向上させます。この保護品質は、機密性の高いデータを取り扱う企業やセキュリティインシデントが許されない団体にとって特に重要です。

IT 部門および IT セキュリティスタッフへのオーバーヘッドを削減

エンドポイント到達前に脅威がブロックされ、エンドポイントレベルでの警報が少なくなればなるほど、パニックに陥るユーザーも少なくなり、インシデントの調査に費やされる時間も短くなります。

生産性の向上

Kaspersky Web Traffic Security は、インターネットリソースの利用を統制することにより、サイバー攻撃のリスクを軽減するだけではなく、ビジネスの阻害要因も排除します。企業や情報システム部門の目の届かない私的なIT資産利用の入り込む可能性を軽減し、生産性を向上させます。

ユーザーの事業規模に応じて自在に対応

システムそれぞれの負荷に応じて、複数のノード管理や、階層的な展開を実現できます。

システム要件

最小ハードウェア要件(ワーカーサーバー・マスターサーバー)

- Intel Xeon E5606 (4コア) 1.86GHz 以上
- 8 GB の RAM
- 4 GB 以上のスワップパーティション
- 100GBのハードディスク空き容量

Kaspersky Web Traffic Security 6.0 のインストールに使用されるサーバーのソフトウェア要件

- RHE Lバージョン 7.5 x64 以上
- Cent-OS バージョン7 .5 x64 以上
- SUSE Linux Enterprise Server 12 SP3以上
- Ubuntu 18.04.1 LTS以上
- Debian 9.5以上

Kaspersky Web Traffic Security の Web インターフェイスを実行するには、以下のいずれかのブラウザーをコンピューターにインストールする必要があります。

- Mozilla Firefox 39 以降
- Microsoft Internet Explorer 11 以降
- Google Chrome バージョン 43 以降
- Microsoft Edge 40以降

その他の付加的な要件:

- Ngnix v.1.10.3、1.12.2、または 1.14.0
- Load Balancing Haproxy v.1.5 (別途構成が必要)
- Squid 3.5.20 (ワーカーサーバーに Squid サービスをインストールする場合)

ファイルのタイプ別送受信制限により、感染の予防とデータ漏洩のリスク軽減を実現

セキュリティ強化のため、Kaspersky Web Traffic Security は、特定のファイルタイプの送受信を制限します。これにより、ドキュメントに埋め込まれた悪意あるコンテンツによる感染を予防すると同時に、ファイル送信によるデータ漏洩のリスクを軽減することができます。また、メディアファイルにアクセスする必要のないユーザーがそのようなファイルにアクセスできないようにして、生産性を向上させることもできます。

マネージドサービスプロバイダ(MSP)へ利便性を提供

Kaspersky Web Traffic Security は、バリュープロポジションにサイバーセキュリティを加えたいMSPや、多様化した企業向けにマルチテナント管理機能と柔軟なライセンス管理を提供します。管理者は各テナントの管理者に適切なレベルのコントロールを委任できます。

機能

脅威に対する多層型保護

カスペルスキーの次世代マルウェア保護は、機械学習アルゴリズムを基盤とする層や、クラウドベースの強力なメカニズムに支援された層など、複数のプロアクティブなセキュリティ層を内蔵し、送受信トラフィックに潜むマルウェアやランサムウェア、不要な可能性のあるプログラムを除去します。

グローバルな脅威インテリジェンス: Kaspersky Web Traffic Security は、世界中から収集されるデータを駆使して、進化しつつある最新の脅威状況に対抗します。

HuMachine™ :機械学習アルゴリズムの能力と人間の専門知識を結集して、グローバルな脅威インテリジェンスのビッグデータを処理し、誤検知を最小限に抑えながら、定評のある、高い検知レベルを実現します。

サンドボックスでのエミュレーション

極めて高度で、難読化されたマルウェアに対する保護を実現するため、安全なエミュレーション環境で添付ファイルを実行、解析し、危険なサンプルが企業システムに入り込まないことを保証します。

スクリプトの検知

Web ベースの攻撃と、一見無害な Office ファイルに埋め込まれたマルウェアの両方で、スクリプトを使用する例が増えています。Kaspersky Web Traffic Security は、これらの両方に対応して、ドライブバイ攻撃を阻止し、致命的なマルウェアがエンドポイントに到達する前に、その実行を食い止めます。

サイバー攻撃関連ホストのデータベース照合

このクラウドベースのサービスは、危険なリソースとの接触のリスクを少しでも回避するため、要求されたリソースを、活動中のサイバー攻撃者のC&Cサーバー、ゼロデイエクスプロイトの含まれるオブジェクト、有害な Web サイトや侵害の意図があると判断されたマルウェア配信ポイントなどが記録された膨大なデータベースと照合します。このデータベースは、Kaspersky Lab の名高い**GREaT team** が提供する情報を使って、リアルタイムに更新されているので、出現したばかりの危険なリソースによるリクエストさえも、実行前にブロックされます。

レピュテーションベースのフィルタ

Kaspersky Web Traffic Security は、Kaspersky Security Network が継続的に更新しているクラウドデータベースに記録されているファイルやアドレスのレピュテーションをリクエストできます。これにより、詳細な分析をしなくても、不審なファイルや不要なインターネットリソースを即座にブロックできるようになります。

Kaspersky HuMachine™ Approach

ビッグデータによる脅威インテリジェンス、ロボットを使ったマシンラーニング機能、専門的な経験を積んだ人間に支えされた Kaspersky HuMachine™ は、さまざまな利益をもたらし、より効果的な保護を提供します。それぞれの要素を組み合わせることにより、個々のコンポーネントが強化され、全体の効果や効率が一段と高まります。

高度なアンチフィッシング

カスペルスキーの高度なアンチフィッシングシステムは、ニューラルネットワーク分析に基づいて、効果的な検知モデルを提供します。画像や言語チェック、特定のスクリプトなど 1000 個を超える基準を使用したこのクラウドを利用したアプローチは、世界中から収集された悪意ある URL やフィッシング URL に関するデータに基づき、ダウンロードしたファイルに含まれる既知、未知、ゼロアワーなどあらゆるフィッシング URL からユーザーを保護します。

コンテンツフィルタリング

ファイルのタイプ別に送受信を制御できます。フィルタリングは、名前、拡張子やタイプ（スプーフィングされた拡張子を持つファイルについてはフォーマット認識機能を使用）、サイズ、MIME タイプ、ハッシュなど、多数のパラメータに基づいて行われます。これは、サイバー攻撃のリスク低減、データ漏洩の阻止、トラフィックの軽減、生産性向上など、さまざまな目的に対応します。

カテゴリを用いたウェブコントロール

すべての Web リソースが、すべての従業員の業務に必要というわけではありません。また、マルウェアのホストや海賊版製品を提供するホストなど、アクセス自体が企業のセキュリティや評判に大きな危険をもたらしかねないリソースも多数あります。ウェブコントロールは、特定のカテゴリに属する Web リソースへのアクセスを制限してリスクを低減し、余計な邪魔の入ることのなく、集中して仕事ができるようにします。また、必要に応じて、「デフォルト拒否」シナリオを実装し、特定のユーザーやグループの業務に必要不可欠なものを除くすべての Web リソースの使用を制限することもできます。

SSL で暗号化されたトラフィックも確実に監視

このソリューションのアーキテクチャでは、企業のトラフィックの監視（別名「corporate man-in-the-middle」）を簡単に実装できます。SSL で暗号化された Web トラフィックがインターネットコミュニケーションの事実上の標準となりつつある今、この機能は必須です。

ICAP 対応システムの保護

カスペルスキーのソリューションは、プロキシサーバーに加え、ICAP プロトコルをサポートしているあらゆるデバイス上のトラフィックを保護します。たとえば、内部のセキュリティソリューションでは保護できない Network-Attached Storages（NAS）などのシステムを保護することができます。

SIEM との連携

Security Information and Event Management（SIEM）システムを使用して、企業ネットワーク全体の活動を追跡している企業には、Kaspersky Web Traffic Security が、Common Event Format（CEF）形式での情報のエクスポートや、広く利用されている syslog など、セキュリティコンテキストに豊かな機能を提供します。

使いやすい管理システム

Kaspersky Web Traffic Security には、柔軟で使いやすいWebベースの管理システムが用意されています。

集中管理コンソール：セキュリティ管理者は、可視性と管理性に優れた単一の Web インターフェイスによって、プロキシサーバーやストレージを含む ICAP 対応システムのセキュリティをすべて制御できます。

利便性の高いダッシュボード：ゲートウェイレベルでの企業セキュリティの現状を正確に判断するために必要なものがすべて、1 つのダッシュボードにまとめられています。このダッシュボードから、緊急イベントを含む現状の全体像を瞬時に見て取れます。

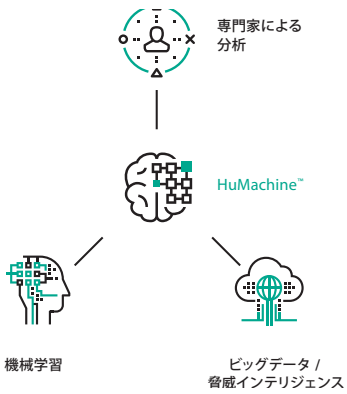
イベント管理：イベントを中心としたアプローチを使って、脅威の分析結果を表示します。この結果は、活動をリアルタイムで示すものです。また、インターネットでのユーザーのふるまいも分析されます。

柔軟なルール構成システム：強力なソリューションのセキュリティ層に加え、きめ細かに調整されたセキュリティポリシーは、このソリューションの有効性の基盤であり、既存のビジネスプロセスと合致するように構成されています。Kaspersky Web Traffic Security の提供するルール構成システムは柔軟で使いやすく、管理者はそれほど時間をかけずに操作方法を習得し、ゲートウェイセキュリティをきめ細かく管理できるようになります。

ロールベースのアクセスコントロール：管理者はロール（役割）を定義して、さまざまな管理者カテゴリに対する管理権限を制限することができます。内部でタスクを委任したり、MSP の場合に、サービス対象クライアントに対する必要なレベルの制御権を提供したりするには、この機能が便利です。

Active Directory の統合：Kaspersky Web Traffic Security は、企業ドメインエンティティ（ユーザー、ユーザーグループ、コンピューターなど）の情報を入手して、企業の IT ネットワークで運用されている既知のオブジェクトに関連するロールベースのアクセスルールやセキュリティポリシーを構成します。こういったオブジェクトを表すデータは、Active Directory と本アプリケーションのあいだで常に同期されるため、企業インフラストラクチャで行われた変更が確実に反映されます。

マルチテナント：MSP や多様化した企業向けの特別なモードで、さまざまな部署や管理対象企業に専用のエリア（ワークスペース）を割り当て、必要に応じて「グローバル」や「ローカル」ポリシーを組み合わせながら、これらを個別に管理できます。



株式会社カスペルスキー

Kaspersky Web Traffic Security は、以下の製品に含まれるアプリケーションです。

- Kaspersky Security for Internet Gateway

ご購入相談窓口：　jp-sales@kaspersky.com

www.kaspersky.co.jp

PMM-1033-201810