

暗号化通信に隠れたマルウェア対策

暗号化トラフィックに隠れた脅威を発見して阻止する、
A10のSSL可視化機能とOPSWAT METADEFENDERによる
連携ソリューション

A10 NetworksとOPSWATは、暗号化されたトラフィックに潜む悪意のある攻撃を発見してブロックする包括的なネットワークセキュリティソリューションを提供します。A10 Thunder CFWのSSL Insight®(SSLインサイト)テクノロジーが、すべてのTCPポートでSSL/TLS暗号化通信を復号することにより、OPSWAT MetaDefender ICAPサーバーは、平文化されたトラフィックに対して、マルチスキャンやコンテンツの無害化(CDR)、データ損失防止(DLP)によるデータサニタイズを適用できるようになります。



課題

検知されずに防御をすり抜ける、
暗号化された
サイバー攻撃、マルウェア、データ漏洩

ネットワークトラフィックの暗号化は急速に増加しており、インターネットトラフィックの大部分が現在暗号化されています。このような高い暗号化率により、組織は新しいセキュリティの課題に直面しています。多くのセキュリティデバイスは、ネットワークトラフィックを高速に復号/暗号化するように設計されていないため、ネットワーク内でボトルネックになってしまい、損失の大きいネットワーク障害を引き起こす原因となってしまいます。

暗号化されたトラフィックは、攻撃者が悪用することができるネットワーク上の盲点となります。この盲点内では、マルウェアやランサムウェアなどの悪意のあるコンテンツを簡単に隠すことができ、検出されずにネットワークに配信されます。攻撃者と悪意のある内部関係者は、暗号化された盲点を使用してネットワークからデータを持ち出すことにより、損失の大きいデータ侵害を引き起こす可能性もあります。さらに、マルウェア作成者は、Microsoft Wordなどのソフトウェアで作成

課題

SSL/TLS暗号化の増加により、サイバー攻撃者は、攻撃トラフィックを暗号化し、従来のセキュリティソリューションを回避できます。その結果、組織は、運用上および財務上の大きな影響を伴う、重大なデータ侵害およびダウンタイムを経験します。

ソリューション

A10のSSLインサイトとOPSWAT MetaDefender ICAPサーバーを組み合わせたソリューションは、組織に包括的なエンタープライズセキュリティを提供します。SSLインサイトの高性能なSSL/TLS復号は、MetaDefenderの高度なマルチスキャン、データ無害化、データ損失防止ソリューションに完全な可視化環境を提供します。

メリット

- 暗号化されたトラフィックを完全に可視化して、隠れた攻撃を発見
- マルチスキャンを使用して、脅威検出の精度をほぼ100%に向上
- コンテンツの無害化(CDR)により、埋め込まれた脅威を排除
- セキュリティインフラストラクチャ全体を強化し、ダウンタイムを削減することでROIを向上
- リアルタイムで入手できる実用的な情報により、展開や管理を簡素化

OPSWAT.

されたマクロ対応のドキュメントに実行可能なマルウェアやトロイの木馬を隠すような複雑な攻撃手法を考案しています。これらのファイルは、通常、従来のマルウェア検査、またはサンドボックスソリューションでは無視されてしまいます。

A10のSSLインサイトと OPSWAT MetaDefender ICAP ソリューション

暗号化トラフィックに隠れた 脅威を発見して防御

A10 Thunder CFWは、SSLインサイトテクノロジーにより、SSL / TLS暗号化によって引き起こされる盲点をなくし、プライバシー基準に準拠しながら、セキュリティデバイスからSSL / TLS復号と暗号化処理をオフロードします。このソリューションは、次世代FWやSWG、IPS、UTM、DLP、ATP、ネットワークフォレンジック製品といったすべてのタイプのエンタープライズセキュリティ製品と連携し、暗号化された脅威からクライアントのネットワーク全体が保護されるように強化します。このソリューションは、OPSWATのMetaDefenderの高度な脅威防止、データ損失防止、およびデータサニタイズ機能と統合することにより、進化するサイバー脅威環境に対する包括的で多面的な防御になります。

OPSWAT MetaDefender は、ICAP (Internet Content Adaptation Protocol) を使用してThunder CFWと連携します。Thunder CFWは、トラフィックを復号すると、HTTPリクエスト/レスポンスをICAPにカプセル化し、検査のためにMetaDefender ICAPサーバーに転送します。MetaDefenderは、転送されたデータに対して、マルスキャン検査を実行します。30種類を超えるマルウェア対策エンジンを活用することにより、従来のシグネチャベースや機械学習ベースの検知をはるかに超える、ほぼ100%に近い精度での高度な脅威検出を実現します。MetaDefenderは、CDRテクノロジーを使用して、Microsoft Wordやその他のソフトウェアで作成されたマクロ対応のドキュメントにマルウェアやトロイの木馬が隠れていないことを保証します。

ソリューション構成

ICAPを介して、A10 Thunder CFWと連携したOPSWAT MetaDefenderは、「安全な平文ゾーン」に配置され、マルウェアやトロイの木馬を発見するために受信トラフィックを検査しながら、送信トラフィックを検査してデータ侵害を監視し、高速なSSL / TLSの可視化環境を実現します。

暗号化されたトラフィックは、A10のSSLインサイトによって一旦復号されます。SSLインサイトによって平文化されたトラフィックは、安全な平文ゾーン内の経路に存在するセキュリティデバイスによって検査できるよう転送されます。平文のリクエスト/レスポンスのコピーもICAPを介してMetaDefenderに送信されます。

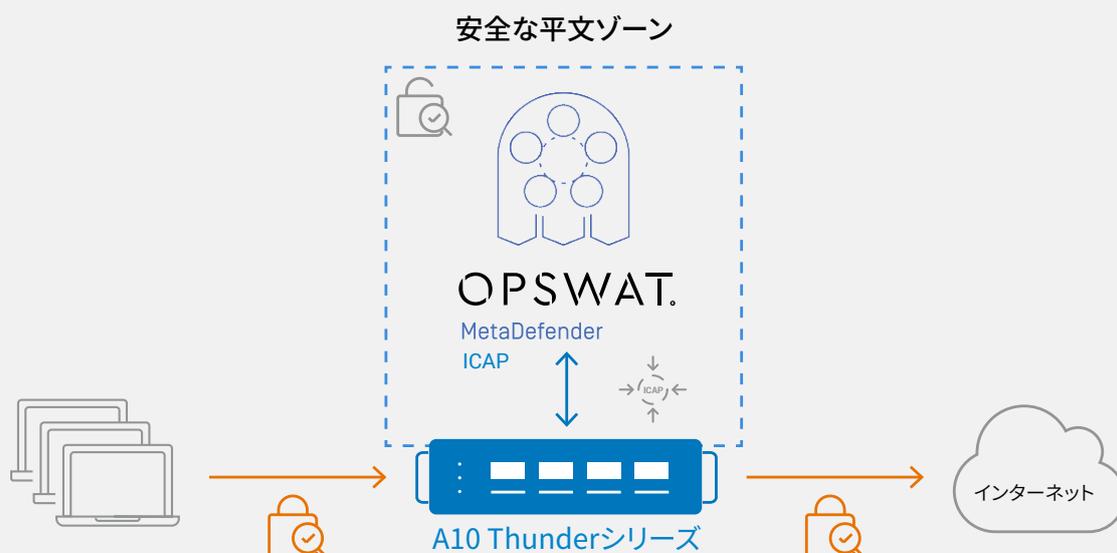


図1: A10 SSLインサイトとOPSWAT MetaDefender ICAPサーバーとの連携構成

MetaDefender ICAP サーバーは、CDRを使用して高度なマルチスキャンとデータサニタイズを実行し、隠れたマルウェアがネットワークに配信されないようにします。送信トラフィックの場合、MetaDefenderは、不正なデータ抽出を監視し、機密資産がネットワーク内で安全に保たれるようにします。

機能と特徴

A10のSSLインサイトによるハイパフォーマンスなSSL可視化機能とOPSWATのMetaDefender ICAPサーバーを連携させることにより、次のようなことが可能になります：

- 暗号化されたトラフィックを含むネットワークアクティビティを完全に可視化し、攻撃と侵入を発見し、安全でセキュアなユーザー体験を提供
- 複数のポート・プロトコルのトラフィックを復号することにより、全てのタイプのネットワークセキュリティデバイスをサポート
- 高度な脅威検出とデータ損失防止により、完全なネットワークセキュリティを実現
- 30種類を超えるマルウェア対策エンジンを活用したマルチスキャンにより、ほぼ100%の脅威検出精度を実現
- CDRを使用して、マルウェア、トロイの木馬、ウイルスの詳細なスキャンを実行
- プライバシー基準への準拠
- 構築や運用、管理をシンプル化
- 詳細なアプリケーションの可視性を含むネットワークトラフィックに関するリアルタイムで実用的な情報の入手
- 運用コストを削減し投資効果を向上

高度な脅威やデータ損失から 機密資産を保護

A10のSSLインサイトによるハイパフォーマンスなSSL可視化機能により、OPSWAT MetaDefenderの高度な脅威防御機能がさらに強化され、暗号化されたトラフィックであっても、最大のパフォーマンスを維持しながら、受信・送信トラフィック内の脅威を高精度に検知・ブロックすることができるようになります。このソリューションの展開と管理の容易さ、およびこのソリューションが提供する詳細な可視性と制御機能は、ネットワークセキュリティ全体の強化に役立ち、損害の大きいデータ侵害やTCOのリスクを軽減します

A10 Networks / A10 ネットワークス株式会社について

A10 Networks (NYSE: ATEN) はセキュアアプリケーションサービスにおけるリーディングカンパニーとして、高性能なアプリケーションネットワークングソリューション群を提供しています。お客様のデータセンターにおいて、アプリケーションとネットワークを高速化し可用性と安全性を確保しています。A10 Networksは2004年に設立されました。米国カリフォルニア州サンノゼに本拠地を置き、世界各国の拠点からお客様をサポートしています。

A10 ネットワークス株式会社はA10 Networksの日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワークングソリューションをご提供することを使命としています。

詳しくはホームページをご覧ください。

URL : <http://www.a10networks.co.jp/>

Facebook : <http://www.facebook.com/A10networksjapan>

OPSWATについて

OPSWATは、2002年から企業にセキュリティソリューションを提供しているグローバルサイバーセキュリティ企業です。OPSWATは、世界中の1,000を超える組織に信頼されている企業であり、組織で利用されるデータやデバイスからセキュリティリスクを排除する最も効果的なソリューションを提供することで、企業の損害を防いでいます。

URL : www.opswat.com

LEARN MORE

ABOUT A10 NETWORKS

お問い合わせ:

a10networks.co.jp/contact

A10ネットワークス株式会社

www.a10networks.co.jp

©2019 A10 Networks, Inc. All rights reserved. A10 Networks、A10 Networks ロゴ、ACOS、A10 Harmony は米国およびその他の各国における A10 Networks, Inc. の商標または登録商標です。その他の商標はそれぞれの所有者の資産です。A10 Networks は本書の誤りに関して責任を負いません。A10 Networks は、予告なく本書を変更、修正、譲渡、および改訂する権利を留保します。製品の仕様や機能は、変更する場合がございますので、ご注意ください。

商標について詳しくはホームページをご覧ください。 www.a10networks.com/a10-trademarks

Part Number: A10-SB-19199-JA-01 NOV 2019