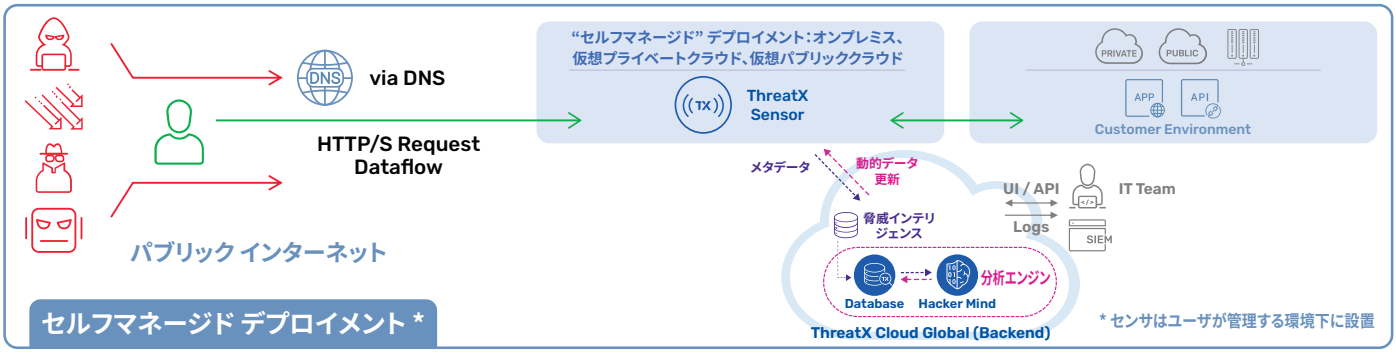
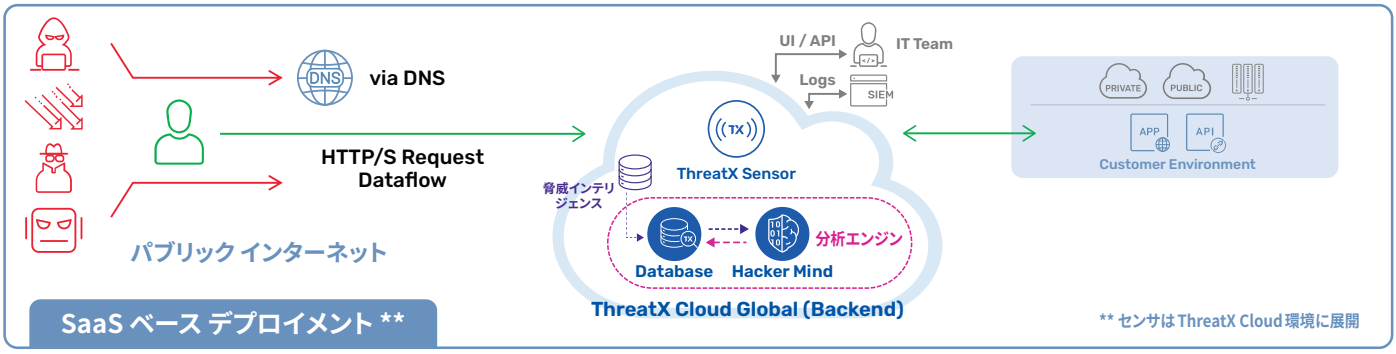
ThreatX by A10 Networks

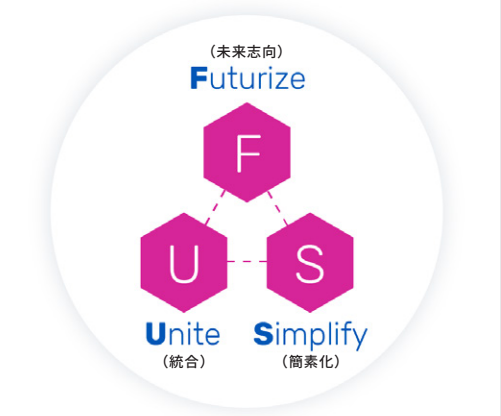
Web アプリケーション保護プラットフォーム（WAPP）
攻撃および攻撃者からアプリケーションエコシステムを
包括的に保護

真の標的であるアプリケーションを守る

A10 Networks の ThreatX は、従来の WAF を凌駕するソリューションです。アプリケーションを徹底的に保護します。WAF は主にアプリケーション層への攻撃を、API 保護は API 攻撃をそれぞれ防御しますが、これらのアプローチは全体像を見落としています。攻撃者は攻撃ベクタ（攻撃経路や攻撃手法）ではなく、現代ビジネスの生命線であるアプリケーションを標的にしているのです。ThreatX は統合的なアプローチを採用し、攻撃と攻撃者の両方からアプリケーションエコシステムを保護します。トランザクション / エンティティベースの追跡、攻撃ベクタ間の相関関係、過去の行動、その他の要素に基づいて継続的に進化する適応型リスクスコアリングにより、精度を向上させます。ThreatX 管理を支援する ThreatX SOC はこの保護をさらに強化するだけでなく、アプリケーションエコシステム全体の保護も管理します。SOC チームは平均して 1 日あたり 3,000 件以上のアラートに直面しています（Hacker News、2025 年）。真の脅威とノイズを人間が区別することはもはや現実的ではありません。 ThreatX ソリューションは、悪意のあるアクティビティを自動的にフィルタリングおよび検証し、自己検証を行った後、ThreatX SOC チームが人間の専門知識を適用してアラートリストをチェックするという三重のチェックを実施します。これにより、顧客は信頼性の高い実用的なアラートのみを受信することができ、アプリケーションセキュリティ運用が効率化されます。







アプリケーションエコシステムの保護を、未来志向で統合、簡素化する

ThreatX は、API、Web、ボット、DDoS 攻撃を網羅した保護機能を、Web アプリケーション保護プラットフォームとして統合します。

- **未来志向：**ThreatX は、高度な機械学習、行動学習、リスクベースプロファイリングを活用し、攻撃者への先手を打つことができます
- **統合：**サイロ化された防御ではなく、ThreatX は攻撃ベクトル全体のアクティビティを相関させ、その情報を統合的に活用して検出・緩和戦略を調整します
- **簡素化：**WAF を導入し、API 保護を追加し、さらにボットと DDoS 防御を重ねるのではなく、ThreatX は統合プラットフォームで保護を提供します

仕組み

- **アプリケーション統合保護 (WAPP):** 現在のアプリケーションセキュリティアプローチには、いくつかの問題があります。多くの場合、保護範囲は不完全で、複数のベストオブブリードツールに依存しています。その結果、追加料金によるコスト増加、専門知識要件による技術的負債の増加、そして過剰な誤検知によるセキュリティチームの負担増加などが生じ、期待した効果には届きません。SIEM を追加しても、アラートの手動分析が必要となるため、これらの問題は解決されません。統合アプローチがなければ、保護は個々のベクトルによって提供され、本来のターゲットであるアプリケーションは保護されません。Web アプリケーション保護プラットフォーム (Web Application Protection Platform：WAPP) アプローチは、攻撃と攻撃者の両方からアプリケーションエコシステムを統合的に保護します。WAPP は、統合された内部構築型の保護を提供することで、コストと複雑さを削減すると同時に、複数の防御ベクトルを単一の目標である「アプリケーション保護」に整合させることで精度を向上させます。

- **適応型リスクスコア：**ThreatX は、クロスベクトル相関、エンティティ / トランザクションベースの追跡、そして実戦で実証された機械学習によって生成される適応型リスクスコアを使用し、継続的に調整・精度向上を図ります。クロスベクトル相関の一例として、ボットのような行動の初期兆候はエンティティのリスクスコアを高め、L7 DDoS 攻撃や API 攻撃などの後続のアクションは、蓄積された行動コンテキストを用いてリスクスコアをより急速にエスカレートさせます。ThreatX は Hacker Mind を介して、悪意のあるトランザクション（飛んでくる雪玉）とその背後にあるエンティティ（雪玉を投げる攻撃者）の両方を継続的に追跡し、リスクをリアルタイムで更新します。Hacker Mind の適応型リスクスコアは、ポイントソリューションでは再現が難しい、統合アプリケーション保護の鍵となります。

- **ThreatX SOC チームは継続的な監視、チューニング、そして対応を可能にします。**お客様は、ポリシー管理、アラート調査、そしてリアルタイムでの対応を行う専門アナリストの恩恵を受けることができます。これにより、アプリケーションセキュリティ運用が大幅に効率化されます。例えば、React2Shell（CVE-2025-55182）の脆弱性が明らかになった際、ThreatX SOC チームは、公開されるかなり前から、根底にある攻撃行動を特定していました。そのため、広範囲にわたる悪用が発生する前に保護策を展開することができました。このプロアクティブな検出は、仮想パッチの適用にとどまらず、ゼロデイ脆弱性が実際の攻撃へとエスカレートする前に、お客様環境を保護します。

Hacker Mind

- 適応型リスクスコアを活用：
  - エンティティ / トランザクションベースのトラッキング
  - クロスベクタ相関
  - 実証済の機械学習アルゴリズム

WAPP

- Web アプリケーション保護プラットフォーム (Web Application Protection Platform: WAPP) は、統合型かつ内部構築型のアプローチを採用し、アプリケーションエコシステムを攻撃や攻撃者から保護します。

SOC

- ThreatX は、お客様のアプリケーションエコシステムを最大限に保護するために、プロアクティブかつ自動で継続的に微調整されます。生成されたアラートは ThreatX ソリューションによって二重チェックされます。フィルタリングされたアラートリストは、ThreatX SOC チームの担当者によってチェックされ、最終的なアラートリストがお客様に配信されます。

柔軟性

- ThreatX はお客様のアプリケーション環境にシームレスに統合されます。
  - セルフマネージド：センサは、お客様が管理するオンプレミス、仮想プライベートクラウド、仮想パブリッククラウドなどの環境に導入されます。
  - SaaS ベース：センサは ThreatX クラウドに導入されます。
- ThreatX の導入は、数時間から数日で可能です。

適応性

- カスタムポリシーやお客様のニーズにも対応し、実装可能です。

A10 Networks / A10 ネットワークス株式会社について

A10 Networks は、オンプレミス、ハイブリッドクラウド、エッジクラウド環境における、セキュリティ、インフラストラクチャの課題を解決するソリューションを提供しています。大手グローバル企業や通信、クラウド、Web サービス事業者まで 7000 社以上のお客様に導入いただいており、ビジネスに不可欠なアプリケーションやネットワークの安全性、可用性、効率性を高めています。A10 ネットワークスは 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社を置き、世界中のお客様にサービスを提供しています。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キ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：https://www.a10networks.co.jp/ • X（旧 Twitter）：https://twitter.com/a10networksjp • Facebook：https://www.facebook.com/A10networksjapan

About A10
A10Networks.co.jp

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

Part Number: A10-BR-20118-JA-03 Jan 2026