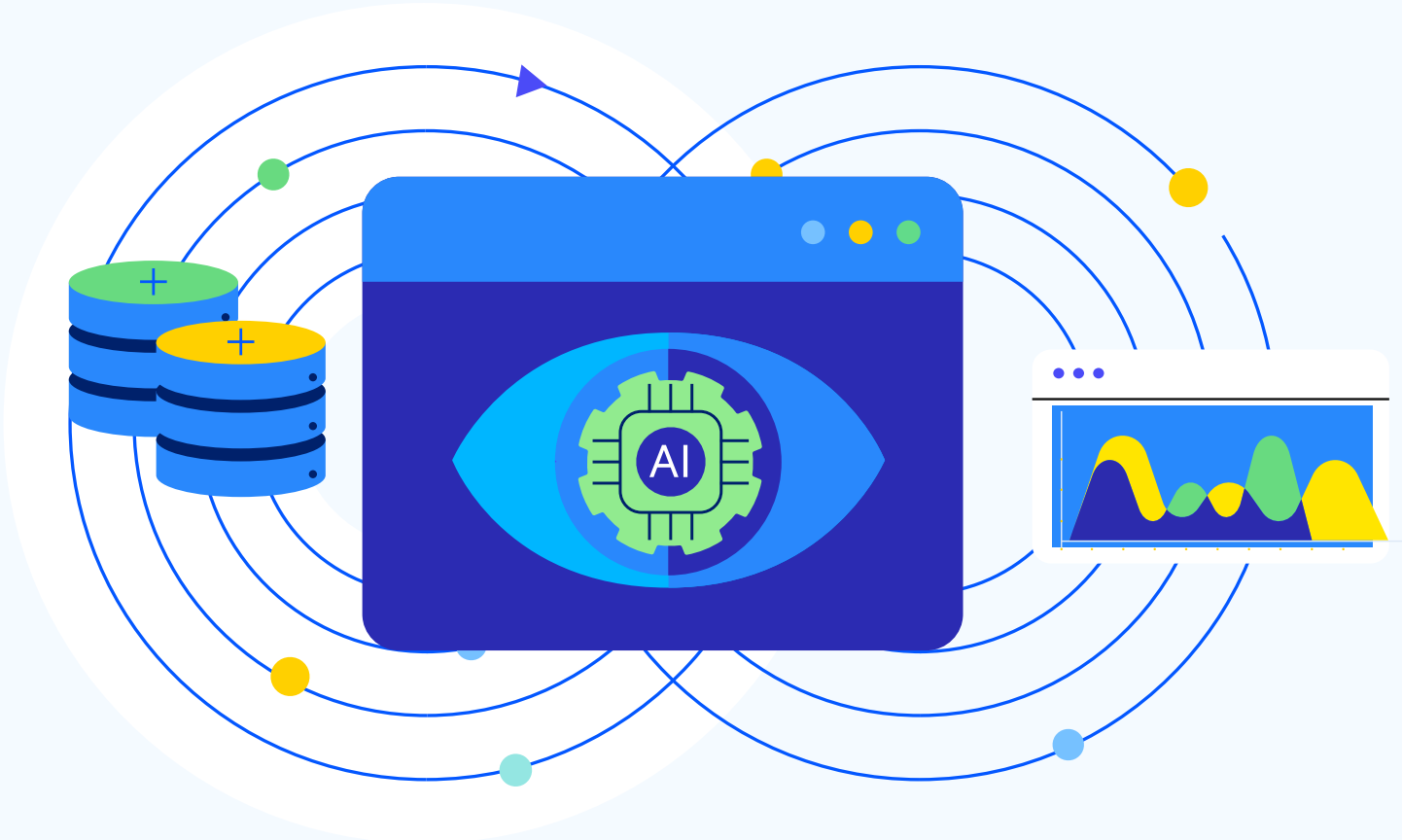
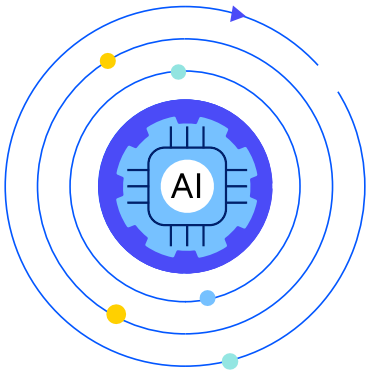
Progress Flowmon

Flowmon ADS

AI を実装した Flowmon 異常検出システム

データシート





強力に不正アクセスを検出

過去のエクスペリエンスを AI 分析で使用

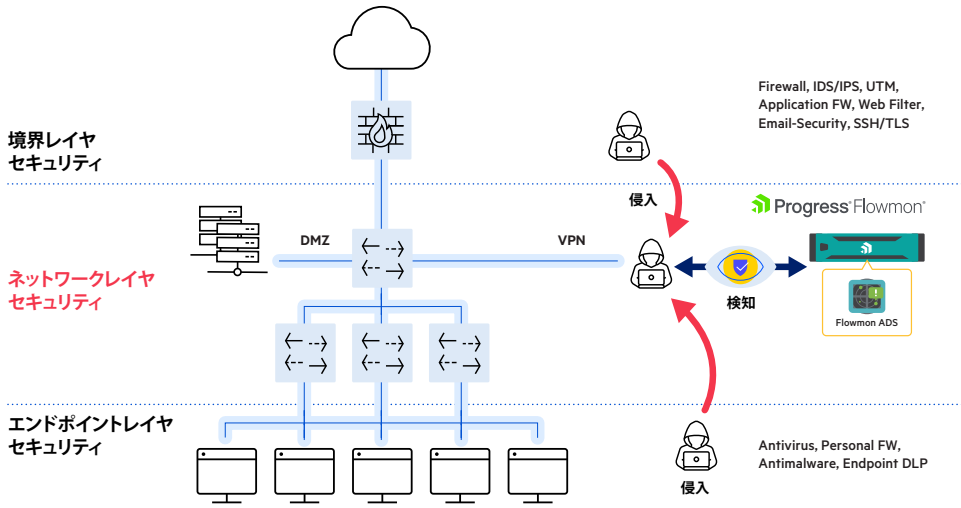
分析を自動化

スマートな優先順位付け

Flowmon ADS とは

Flowmon 異常検出システム（Anomaly Detection System, ADS）は、人工知能と機械学習を使用してネットワークトラフィック内の見つかりにくい異常を検知するセキュリティソリューションです。従来のセキュリティツールを補完し、侵害の様々な段階で脅威を検出できる多層保護システムです。ファイアウォール、IDS/IPS、ウイルス対策などの従来のシグネチャやルールベースの検出アプローチは、境界とエンドポイントの保護に重点を置いています。既知の悪意あるコードや振る舞いによる初期感染の検出には効果的ですが、境界やエンドポイントを超えて保護することはできません。インサイダー脅威や未知の脅威が発生する可能性がある広大な領域が残ったままとなります。

データ侵害やデータ窃盗には、このギャップがしばしば悪用されます。インサイダー脅威は、侵害の兆候を示すわずかな異常を検知しないと発見できません。Flowmon ADS は、AI 技術を駆使して検出機能の範囲を拡張・強化し、振る舞いベースの異常とインシデントの検出に追加のコンテキストを提供できます。次の図に示されるように、Flowmon ADS は、境界セキュリティとエンドポイントセキュリティの間のギャップを埋めるネットワークレイヤセキュリティとして、全体的なサイバーセキュリティ防御戦略を強化できます。



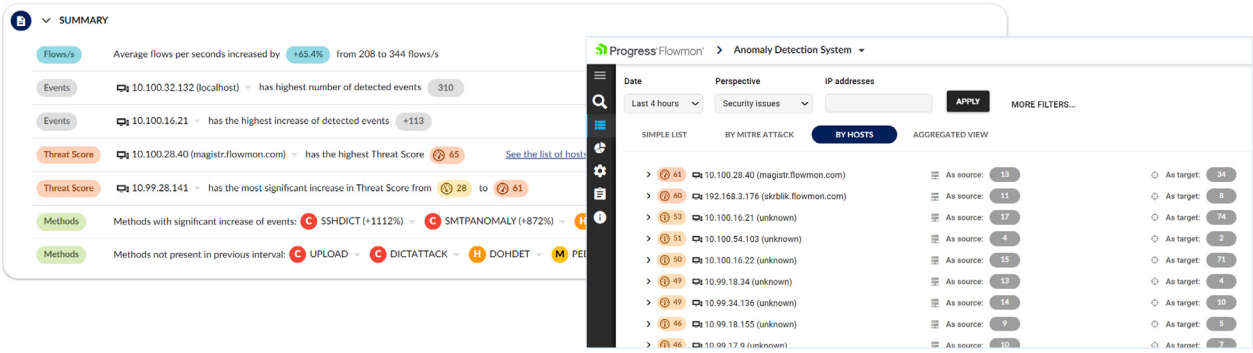
© 2025 Progress. All Rights Reserved.

AI によって強化された検知・分析・表示機能

Flowmon ADS に組み込まれている、AI によって強化された機能は、以下の通りです。

AI を活用したイベント概要とスコアリング

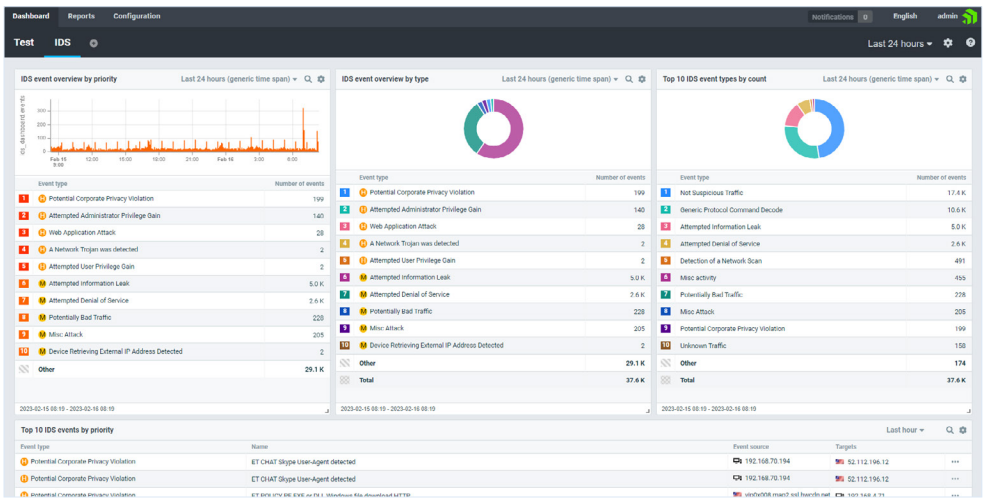
Flowmon ADS は、選択した時間間隔で最も重要な検知と注目すべきイベントに関する自動化されたサマリーを提供します。脅威スコアは、アナリストの作業に優先順位を付ける目的で、すべてのホスト（IP）に対して計算されます。



IDS イベントの視覚化と分析

Flowmon IDS プローブ（Suricata）によって生成されたイベントは、動作ベースの検出エンジンによって生成されたイベントと同じ方法で視覚化されます。これには、次のものが含まれます:

- 関連フローを含むイベントの詳細
- 中央ダッシュボードのウィジェット
- レポートの各チャプター



これらの機能はすべてFlowmon ADS に含まれ、中央ダッシュボードとレポートで利用できます。

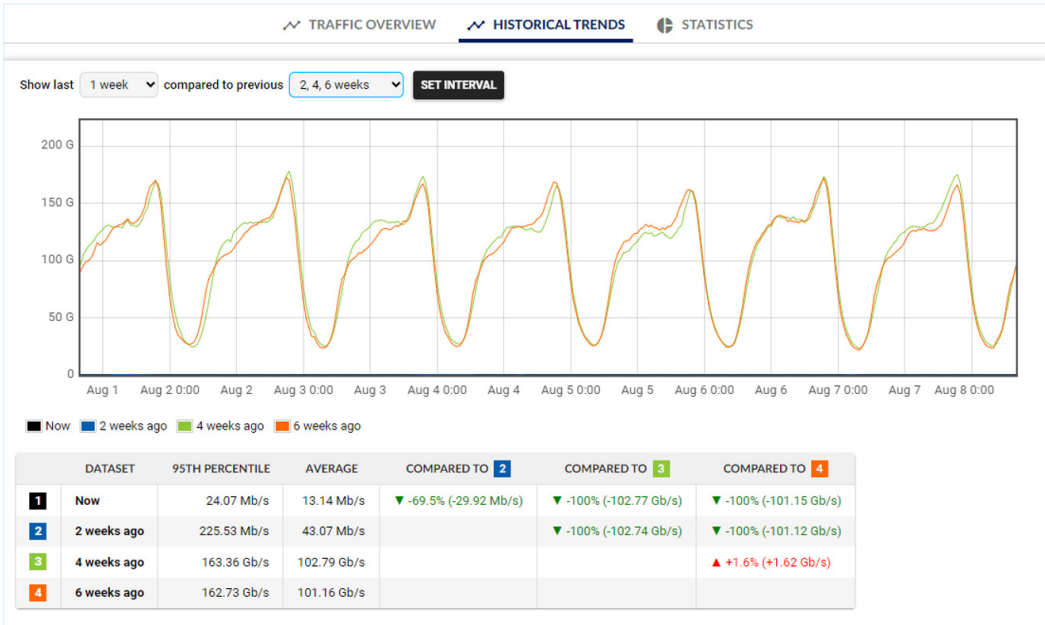
© 2025 Progress. All Rights Reserved.

AI を活用した分析と Flowmon ユーザーインタフェース

AI を活用した分析は、ユーザーインタフェース (UI) を通して表示されますが、リリース 12.2 で UI が大幅に向上しました。リリース 12.2の前後で比較すると、UI で費やす時間が52%削減されました。ユーザーが分析を表示するページに費やす時間が、12.2 リリース前は平均119分だったのに対し、リリース後には平均57分に半減しました。

過去からの傾向

現在のデータと履歴データの視覚的かつ計算された比較を表示します。レポートや分析用のダッシュボードウィジェットとしてプロファイルごとに利用できます。トラフィック量の傾向を理解するのに役立ちます。



© 2025 Progress. All Rights Reserved.

Flowmon IDS Probe のライセンスと可用性

IDS Probe (プローブ) は、ライセンスなしで、任意の Flowmon Probe (IP フロー統計を生成する NetFlow/IPFIX エクスポーター) または Flowmon Collector (高度レポート機能を備えたフローデータ収集、保存、分析のための NetFlow/IPFIX コレクター) にインストールできます。

シグネチャベースの検出

Flowmon IDS Probe (プローブ)

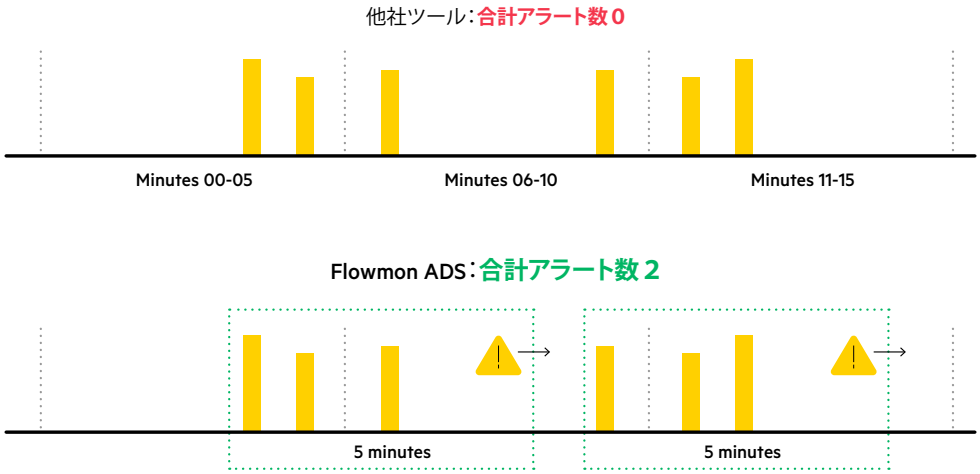
Flowmon IDS Probe (プローブ) は、異常検出システムのネイティブな動作ベースの検出機能を補完する、シグネチャベースの検出エンジンです。

- コミュニティ脅威検出ルール (ET Open Ruleset) と自動更新が組み込まれたオープンソースの Suricata IDS をベースにしています
- Suricata と互換性のある商用脅威検出ルール/シグネチャは、サードパーティーから購入して IDS プローブで使用できます
- Suricata はシグネチャベースの検出専用で、各ネットワークセッション (フロー) からの最初の N パケットを処理するように最適化されており、パフォーマンスに影響を与えることなく任意の Flowmon Probe モデルで使用できます
- 検出されたイベントは、異常検出システムと任意のログ管理または SIEM システムに syslog 経由で並行してエクスポートできます

Flowmon ADS のそのほかの重要な特徴

精度と状況の明確さを向上させる真のリアルタイムアラート

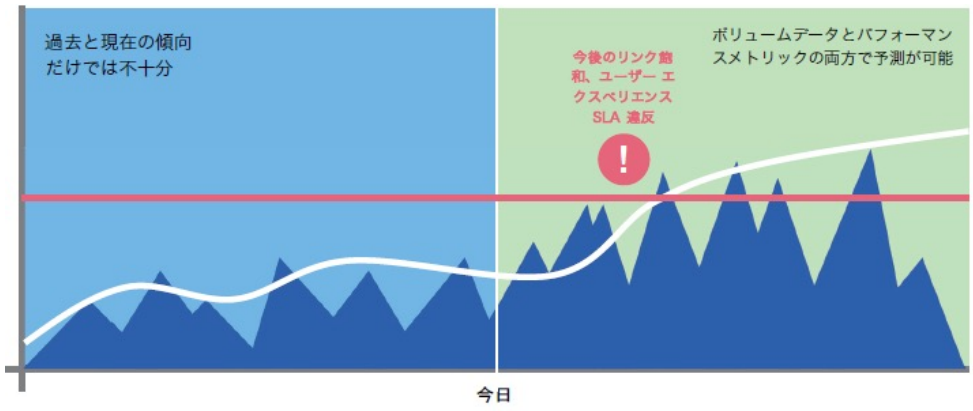
例えば、「開発サーバーに、5分以内に3つ以上の固有の接続があったらアラート送信する。」という指定をした場合、Flowmon ADS のアラートは、任意の5分間の間に開発サーバーに3つ以上の固有の接続があれば、メールでアラート通知します。他社ツールの場合、5分間ごとに区切って接続をカウントするので、次の5分間の初期に3つ目の接続があっても3つ目の接続と認識されず、アラート通知されません。



© 2025 Progress. All Rights Reserved.

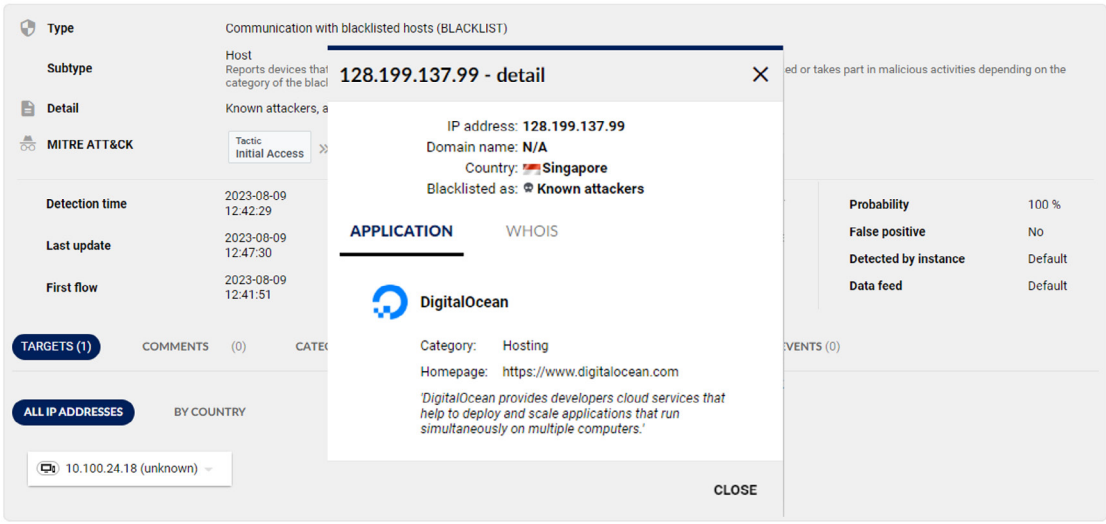
予測トレンド

過去と現在の傾向だけでは不十分です。Flowmon ADS は、ボリュームデータとパフォーマンスメトリックの両方で予測が可能であり、今後のリンク飽和や SLA 違反などの予測トレンドにより、インシデントが発生する前にプロアクティブに問題解決を図ることができます。



アプリケーションとプラットフォームの情報

Flowmon ADS は、IP アドレスを対応する SaaS アプリケーションおよびプラットフォームにマッピングするための追加のネットワークインテリジェンスを表示します。イベントの分析と調査のプロセスが合理化され、シンプルになります。

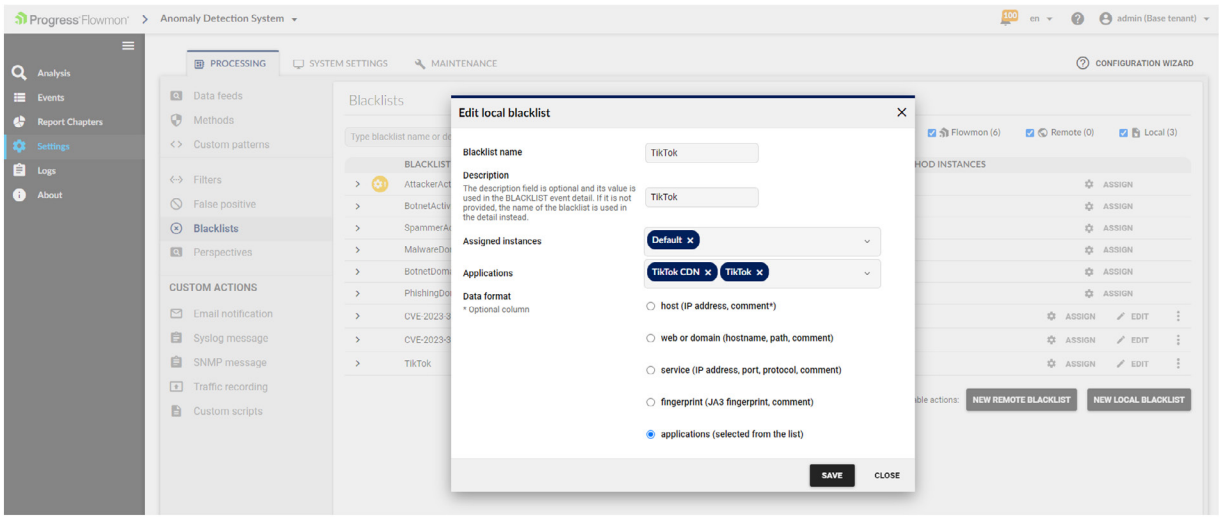


© 2025 Progress. All Rights Reserved.

シャドー IT と疑わしいサービスの検出

シャドー IT とは、企業内で情報システム部門などが関知せず、従業員や部門が独自に導入した IT 機器やシステムなどを指します。シャドー IT が起きやすいものには、私物のスマートフォンや PC のほか、チャットツールやフリーメール、クラウドストレージなどがあります。いずれもプライベートでもよく使われており、従業員が特に意識せず使ってしまいやすいものと言えるでしょう。シャドー IT には、企業側で適切に資産管理されていない IT 機器やシステムを使用することで、セキュリティの脆弱性につながるという問題があります。近年はリモートワークが一般化し、企業の管理が及ばない状況で業務を行う機会が増え、シャドー IT がより問題視されるようになっています。

Flowmon ADS を使うと、このようなシャドー IT や疑わしいサービスを検出することができます。



© 2025 Progress Software Corporation、そして/または その子会社もしくは関連会社。全著作権を所有。Rev 2025/01 1209125064510264JP

Progress と、ここで使用される特定の商品名は、Progress Software Corporation、そして/または 米国内もしくはその他の国の子会社あるいは関連会社の1つ、の商標、または登録商標です。その他記載の製品名や会社名は、それぞれの会社の商標もしくは登録商標で、その保有者に帰属します。

プログレス・ソフトウェア・ジャパン株式会社
〒106-0047 東京都港区南麻布 4-11-22 南麻布 T&F ビル
www.progress.com/jp/flowmon
sales_japan@progress.com

Progress