Progress Flowmon

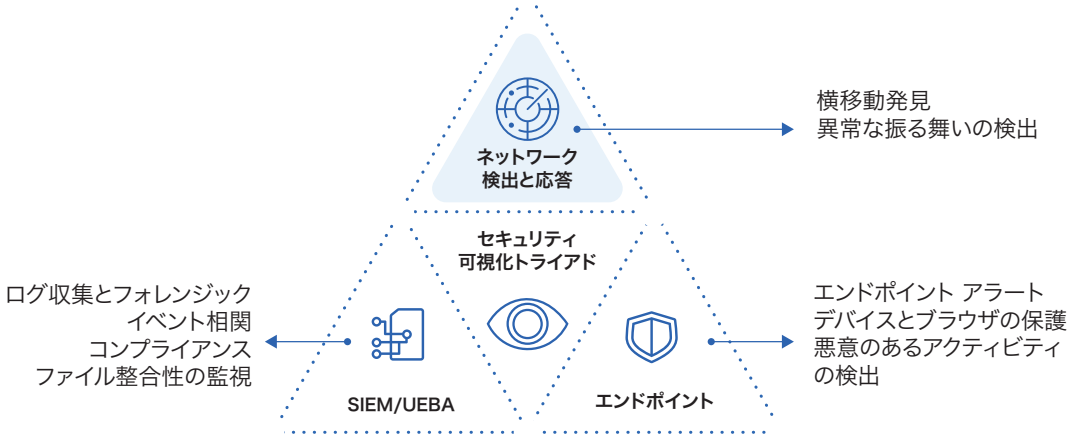
Cisco Secure Network Analytics (旧 Stealthwatch)と Progress Flowmon との比較

Ransomware/マルウェア/振る舞い検知

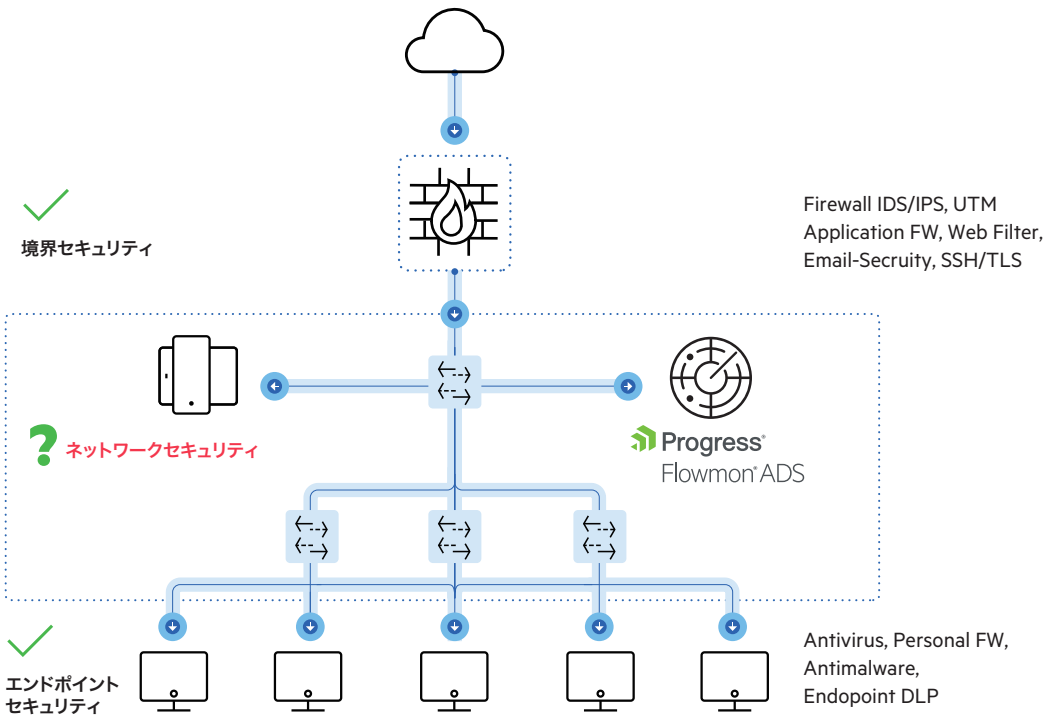
データシート

NDR – ネットワーク検出と応答 – について

NDR (Network Detection and Response、ネットワーク検出と応答) は、組織が悪意のあるアクターやネットワークトラフィック上の疑わしい振る舞いを監視し、ネットワークに対するサイバー脅威の検出に反応して対応できるようにする、サイバーセキュリティの成長分野です。



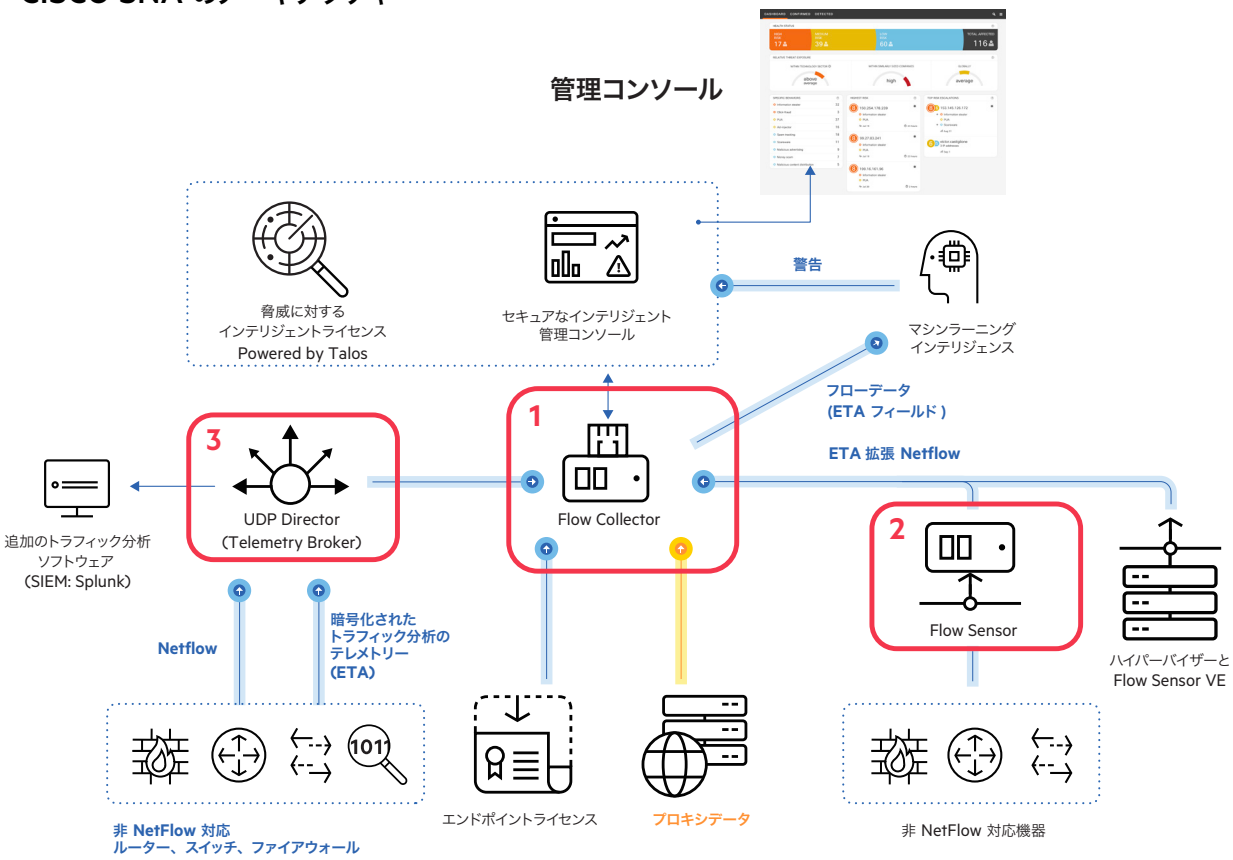
- ネットワークフローを使用してシグネチャに基づかない手法で疑わしいトラフィックを検出
- 継続的に分析、関係づけをして監視モデルを構築
- 企業ネットワークの南北方向トラフィックだけではなく、東西方向トラフィック (横移動) も監視



境界とエンドポイントセキュリティは対策が進んでいますが、ネットワークセキュリティは手薄で対策が必要です。

Cisco Secure Network Analytics (旧 Stealthwatch) とは

CISCO SNA のアーキテクチャ



1 **フローコレクター**

ネットワークデバイス (ファイアウォール、スイッチ、エンドポイントなど) からのすべての着信テレメトリーの収集集約と保存を担当するデバイス

2 **フローセンサー**

オプションで、SPAN または単に TAP されたデバイスによって取得されたトラフィックのコピーを使用し、拡張された NetFlow をコレクターに送信して、アプリケーション層のデータを提供

3 **UDP ディレクター (SPLUNK など)**

フローコレクターなどの複数の宛先や既存の SIEM ソリューション NetFlow、syslog、または SNMP データを送信する場合に使用されるオプションのコンポーネントである UDP ブローカーまたは UDP ディレクター

Cisco SNA と Flowmon との比較

Ransomware/マルウェア/振る舞い検知などを行う NDR システムには、上述の Cisco SNA や Progress® Flowmon® などがありますが、選択するにあたっては以下の6つのポイントを考慮することをお勧めします。

1. 機能

機能	Cisco SNA	Flowmon ADS
NDR	✓	✓
NPMD	✗	✓

Cisco SNA には、ネットワーク運用にとって重要な、詳細なドリルダウン分析機能が欠如しています。Cisco SNA は、NDR のマーケットガイドでは言及されていますが、Gartner の NPMD (Network Performance Monitoring and Diagnostics、ネットワークパフォーマンス監視と診断) レポート (2020 Market Guide for Network Performance Monitoring and Diagnostics, ID G00463582) からは除外されています。

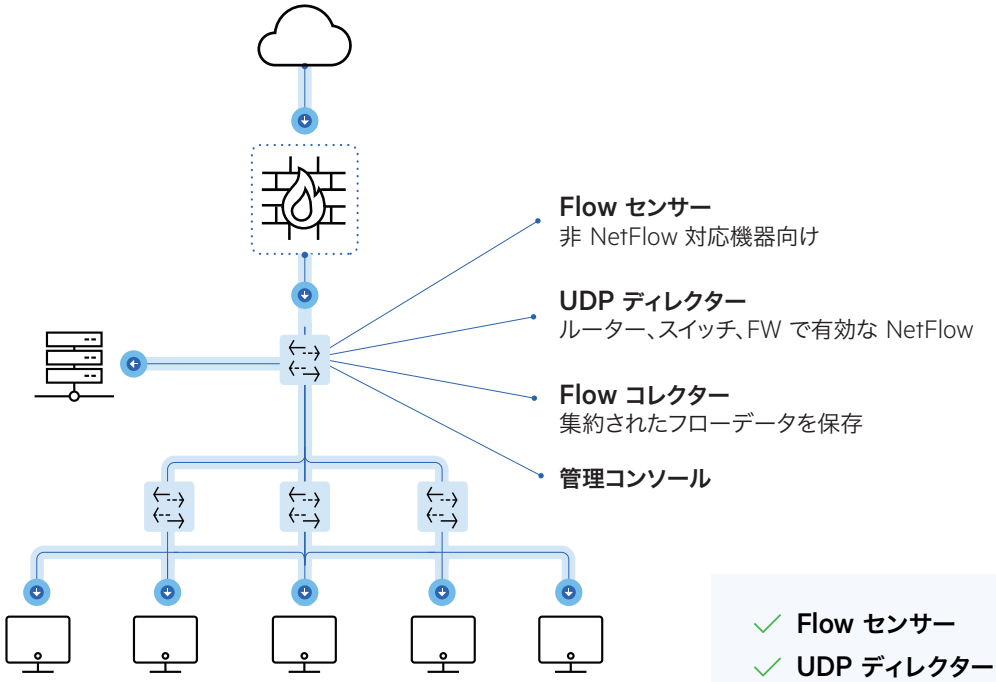
2. 保存するデータと容量

Cisco SNA は、集計データのみ、かつデータ保持は短期間になります。6TB の容量には、ストレージ用2台、コンピューティング用1台の3台のサーバーユニットが必要になります。

Flowmon の場合は、集計せずに完全なデータを保存でき、長期データ保持が可能です。最大24TB のサーバーユニットが1台だけ必要で、最大 192TB まで拡張可能です。

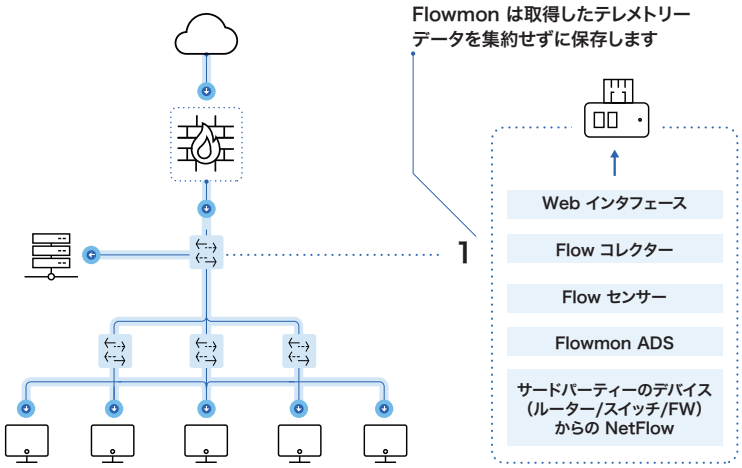
3. アーキテクチャ

Cisco SNA は、アーキテクチャが複雑で、コンポーネントを完全活用するためには少なくとも以下の4つのライセンスが必要で、コストも非常に高くなります。



- Flow センサー
- UDP ディレクター
- Flow コレクター
- 管理コンソール

一方、Flowmon の場合は、取得したテレメトリーデータを集約せずに保存するため、アーキテクチャがシンプルです。

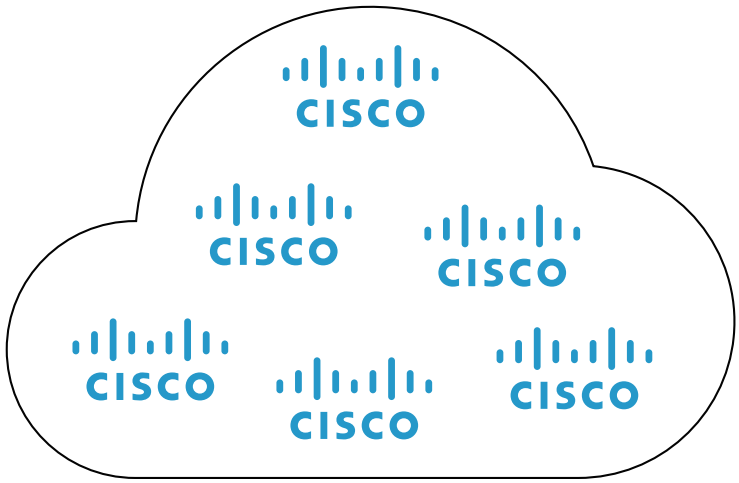


Flowmon Collector は、複数種類のソースからネットワークテレメトリーを受信することもできます。そのための追加ライセンス (UDP ディレクターなど) は必要ありません。Flowmon Collector は、Flowmon ADS (コレクター上で実行される異常検出システムモジュール) を備えた 1 つのアプライアンスであり、ネットワークを保護するための実用的なインテリジェンスを提供します。

4. ベンダーからの独立性

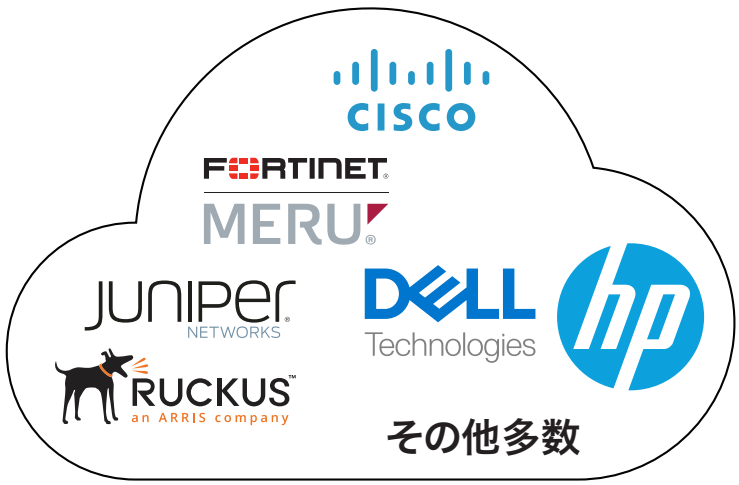
ベンダーロックインとは、製品、サービス、システムが特定のベンダーに依存しているため、他ベンダーの提供する製品、サービス、システムへの乗り換えが困難になる現象です。Cisco は大手ベンダーであり、すべてを Cisco 製品、サービス、システムで統一しようとするシングルベンダーロックイン・アプローチを採用しています。

Cisco 環境
- シングルベンダーロックイン



Flowmon の場合は、ベンダーにとらわれないアプローチを採用しており、どの環境でも同じように機能します。多くのお客様がベンダーからの独立性を非常に重要視しており、最終的に Flowmon が選択される大きな理由の1つになっています。

Progress Flowmon
- マルチベンダー環境



5. ハードウェアの耐用年数

IT 資産をできるだけ長く使用したいというのは、企業規模の大小にかかわらず普遍的な希望です。IT ハードウェアの原価償却期間は最大7年が認められており、国内の多くのお客様は7年間で減価償却を行いたいと考えられています。プログレスでは、国内のニーズを理解し、長期間安心してご使用いただけるよう耐用年数は標準7年に設定しています。

	CISCO	Progress Flowmon
耐用年数	標準5年	**標準7年**

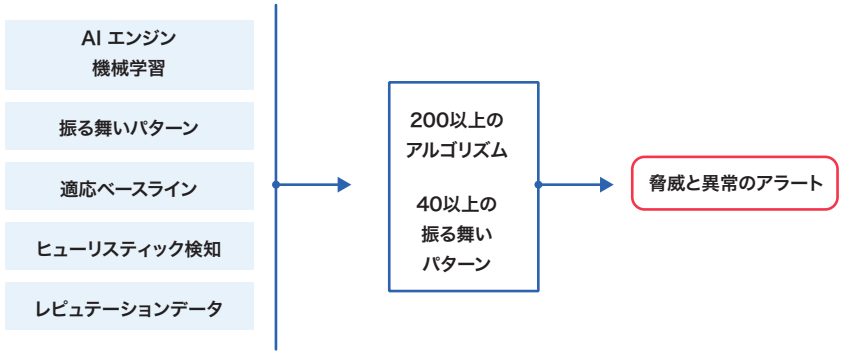
6. 機能と価格

2. に示したように、機能面だけでも Flowmon に優位性がありますが、価格の比較においても、次表のように Cisco SNA は Flowmon の約3倍のコストがかかります。

機能と価格比較	CISCO	Progress Flowmon
自動脅威検出	✓	✓
統合ダッシュボード	✓	✓
検出された異常を SIEM に送信	✓	✓
NPMD 機能	✗	✓
長期間保存容量	**4TB**	**12TB**
価格	**$672.380**	**$202.997**

Flowmon ADS の特長

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を作成します。



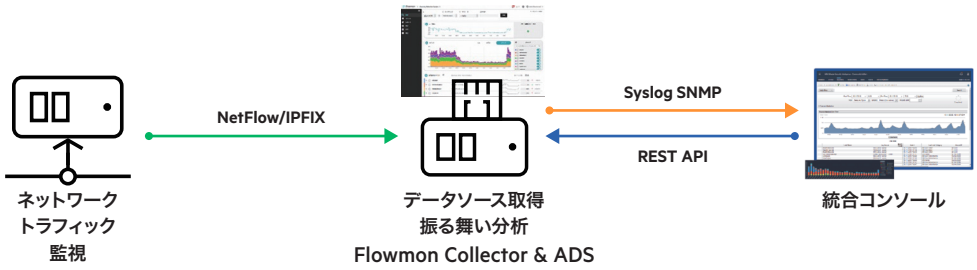
Flowmon Collector へのプラグインである Flowmon ADS には、次のような特長があります。

1. AI エンジンと機械学習によって関係のあるフローデータの相関関係を自動作成
2. 異なる観点からトラフィックを検査する 40 を超える振る舞い検出方法を提供。悪意ある振る舞いの特性とカテゴリに基づいて200以上の個別アルゴリズム
3. 脅威のない通常の状態をベースラインとして保存し、現状と比較して脅威を検出
4. 機械学習、ヒューリスティック、統計、ポリシー、シグネチャを使用して、広範囲に脅威を検出
5. レピュテーションデータを毎日更新し、IDS Suricata と統合し、振る舞いパターンをアルゴリズムに組み込む
6. NetFlow, sFlow, jFlow, IPFIX, NetStream などの標準プロトコルのほか、Gigamon などその他のベンダーのフローデータもサポート

シグネチャベース検出

- オープンソースの IDS Suricata は、ネットワークプローブで実行され、検出されたイベントを追加の洞察で強化
- Flowmon Collector は、ユーザーの入力を集約して前処理
- セキュリティオペレータに追加情報とコンテキストを提供

SIEM と Security Analytics の統合



- イベントの Syslog フィードは、ログ管理、SIEM、ビッグデータプラットフォーム、インシデント処理、および SOAR ツールに提供されます
- 応答ツールは、そのイベントソースと同じくらい重要です

重要なポイント：見えないものは管理も保護もできません

環境全体を可視化する単一のソース

パフォーマンスの低下をすぐに確認

可用性、使用状況、容量を監視

ボトルネックを明らかにし、エラーを分析し、検出を自動化

最後に

単一のソリューションで、すべてのプラットフォームを監視、検知することは不可能です。必要なソリューションを組み合わせて効果的に使用することを推奨します。また、データバックアップは1つのリスク回避策ですが、侵入者は Samba、NAS などの外部ストレージを頻繁に標的にしていますので、注意が必要です。まず、タイムリーに監視、検知をし、侵入者の手口を知ることが非常に重要です。

Flowmon ADS は、お客様の大切な資産を守ることができるソリューションです。

Progress