Cisco Secure Network Analytics（旧 Stealthwatch）

2024 年 1 月

The bridge to possible

目次

Cisco Secure Network Analytics

このドキュメントでは、Cisco Secure Network Analytics（旧 Stealthwatch Enterprise）について説明します。Cisco Secure Cloud Analytics（旧 Stealthwatch Cloud）のデータシートはここから確認できます。

詳細情報については、https://cs.co/sna から確認できます。

ソリューションの概要

Cisco Secure Network Analytics は、企業全体のネットワークの可視化を実現し、脅威をリアルタイムで検出して対応します。このソリューションは、ネットワークアクティビティを継続的に分析して、通常のネットワーク動作のベースラインを作成します。次に、このベースラインを使用して、動作モデリングと機械学習アルゴリズムを含む非シグネチャベースの高度な分析、およびグローバル脅威インテリジェンスにより、異常を識別し、脅威をリアルタイムで検出して対応します。Secure Network Analytics は、コマンドアンドコントロール（C&C）攻撃、ランサムウェア、分散型サービス妨害（DDoS）攻撃、違法仮想通貨マイニング、未知のマルウェア、組織内に潜む脅威などの脅威を迅速かつ高い信頼度で検出できます。エージェントレス ソリューションにより、暗号化されている場合でも、ネットワークトラフィック全体にわたって包括的な脅威モニターリングを実現できます。

組織では、IT インフラストラクチャやセキュリティにすでに多くの投資を行っています。それでも、脅威はそれをすり抜ける方法を見出していきます。さらに、違反を検出するのに数か月または数年かかることがよくあります。この可視性の欠如は、増大するネットワークの複雑化そして脅威の進化と相関関係にあります。限られたリソースとまとまりのないツールしか持たないセキュリティチームができることには限りがあります。事実上すべての組織にファイアウォールなどのセキュリティソリューションがありますが、これらのツールが正しく機能し、管理および構成されているかどうかをどのように知るのでしょうか。これらのツールが必要な役割を果たしていることをどのように確認できるでしょうか。

シスコでは、この問題を逆の側面から考えてみることにしました。つまり、組織のセキュリティを確保するために、既存のネットワークへの投資を積極的に行ってみることにしたのです。ネットワークテレメトリは、組織に接続しているユーザーとその状況に関する有用なインサイトを提供する、貴重なデータソースです。すべてがネットワークに接続されるため、この可視性は本社から支店、データセンター、ローミングユーザー、スマートデバイスにまで及び、プライベートクラウドとパブリッククラウドにまで拡張されます。このデータの分析によって、既存の制御をバイパスする方法を見出した脅威を、その脅威が大きな影響を与える前に検出できるようになります。

このソリューションとなるのが Secure Network Analytics であり、ネットワークを活用してエンドツーエンドでのトラフィックの可視性をオンプレミスとプライベート/パブリッククラウドの両方で提供します。この可視性によって、すべてのホストを把握することができます。つまり、特定の時点で誰がどの情報にアクセスしているかを確認できるようになります。ここで重要なのは、特定のユーザーまたは「ホスト」の正常な動作を理解し、異常発生時にユーザーの動作を変更するように警告できるベースラインを確立することです。

Secure Network Analytics は、ハードウェアアプライアンスまたは仮想マシンとしてのオンプレミスの 2 つの異なる展開モデルを提供します。Secure Cloud Analytics（旧 Stealthwatch Cloud）は、Secure Network Analytics の Software-as-a-Service（SaaS）バージョンです。プライベートネットワークの監視に加えて、Secure Cloud Analytics を展開して、パブリッククラウドの脅威と構成の問題を検出することもできます。

主な使用例

リアルタイムの脅威の検出

簡単に言えば、Secure Network Analytics は、最も包括的でコンテキストが豊富なネットワークの可視性を提供します。実績のある、業界をリードするセキュリティ分析と組み合わせることで、最も幅広く忠実な行動ベースの脅威検出機能が実現され、以下が劇的に改善されます。

- 未知の脅威の検知：通信や悪意のあるドメインなど、従来のシグネチャベースのツールでは見逃される、疑わしい動作ベースのネットワークアクティビティを識別します。
- インサイダー脅威の検知：データホーディング、データの漏洩、疑わしい侵入拡大の動きに対して警告します。
- 暗号化されたマルウェアの検出：多層機械学習を活用し、暗号化された Web トラフィックを復号せずに可視性を拡張します。
- ポリシー違反：他のツールで設定されているセキュリティおよびコンプライアンスポリシーが実施されていることを確認します。
- インシデント対応とフォレンジック：脅威アクティビティ、フォレンジックのネットワーク監査証跡、および SecureX やその他の Cisco Secure ソリューションとの統合に関する完全な知識を使用して、迅速かつ効果的に対応します。

リモートワーカーの監視

Secure Network Analytics は、AnyConnect Network Visibility Module（NVM）からのエンドポイント レコード テレメトリ データを主要なテレメトリソースにしました。これにより、ユーザーは、単一の VPN セッションを使用して作業しているかどうか、スプリットトンネリングを使用してリモート作業エクスペリエンスを最適化しているか、または VPN から完全に切断されているかどうかに関係なく、エンドポイント固有の詳細なユーザーおよびデバイスコンテキストを幅広くキャプチャして、モバイル リモート ワーカー エンドポイント アクティビティの完全かつ継続的な可視性を、組織に効果的に提供できます。これにより、パッチを適用する必要のある脆弱性を備えた古いバージョンのオペレーティングシステムを実行している従業員、データホーディングやデータの漏洩に関与している従業員などの、以前は見えていなかったアクティビティを可視化することで、組織のセキュリティ体制が強化されます。

グループベースポリシーのレポーティング

ユーザーは、Cisco Secure Network Analytics と Cisco Identity Services Engine の統合を活用して、グループ通信を視覚化する新しい方法を提供するグループベースのポリシーレポートを生成することにより、グループベースのポリシー採用の取り組みを加速できます。グループベースのポリシーレポートを使用すると、ユーザーはグループ間のコミュニケーションを簡単に視覚化、分析、ドリルダウンできます。また、ポリシーの有効性を検証し、環境のニーズに基づいて適切なポリシーを採用し、関連するフローおよび関連付けられている IP への情報を通じてポリシー違反の調査を合理化できます。詳細については、At-a-Glance を参照してください。

暗号化トラフィック分析

暗号化トラフィックの急増により、脅威の状況も変化しています。暗号化はデータのプライバシーとセキュリティを向上させていますが、サイバー犯罪者がマルウェアを隠して検出を回避する手段にもなっています。現在、すべての Web トラフィックの約 95% が暗号化されており、攻撃の 70% 以上が暗号化を使用すると予想されています。一括復号、分析、および再暗号化を使用する従来の脅威検査は、パフォーマンスとリソース上の理由から、常に実用的または実行可能であるとは限りません。また、プライバシーとデータの整合性に対する侵害も行われています。シスコ

は、ネットワーク インフラストラクチャ市場での専門知識により、暗号化されたトラフィックを復号せずに分析する革新的なテクノロジーを導入しました。これにより、組織は 1) 暗号化されたトラフィックの脅威を検出し、2) 暗号化コンプライアンスを確保できます。詳細については、https://www.cisco.com/jp/go/eta にアクセスしてください。

主な利点

- **死角を排除する：**Secure Network Analytics は、センサーをどこにでも配置することなく、プライベートネットワーク全体とパブリッククラウドに包括的な可視性を提供できる唯一のセキュリティ分析ソリューションです。また、暗号化されたトラフィックのマルウェアを復号することなく検出する最初のソリューションでもあります。
- **ノイズではなくインシデントに焦点を当てる：**Secure Network Analytics は、動作モデリング、マルチレイヤ機械学習、グローバルな脅威インテリジェンスの機能を活用して、環境に影響を与える重大な脅威に関する誤検出やアラームを大幅に削減します。
- **実際の攻撃に対処する：**Secure Network Analytics は常にネットワークを監視して、高度な脅威をリアルタイムで検出します。ステルス攻撃の前には、通常、ポートスキャン、ping の繰り返し、偵察戦術などのアクティビティがあります。このソリューションは、これらの早期警告サインとアラームを認識して、攻撃を早期に阻止します。脅威が特定されると、ユーザーはフォレンジック調査を実施して、脅威の根源を特定し、他にどこに伝播した可能性があるかを判断することもできます。
- **投資を最大限に活用する：**エージェントレス ソリューションにより、既存のネットワーク インフラストラクチャによって生成された豊富なテレメトリを使用して、セキュリティ態勢を改善します。
- **ビジネスの成長に合わせてセキュリティを拡張する：**ビジネスニーズの変化によってこれ以上セキュリティを犠牲にする必要はありません。新しいブランチやデータセンターを追加する場合でも、ワークロードをクラウドに移動する場合でも、単にデバイスを追加する場合でも、Secure Network Analytics の展開では、ネットワークのニーズに合わせて拡張することで、簡単に対応できます。オンプレミスまたはクラウドにデプロイでき、SaaS ベースまたはライセンスベースのソリューションとして使用でき、ネットワークに追加された新しいデバイスを自動的に分類する自動役割分類機能を実現できます。
- **セキュリティエコシステムと SecureX を統合する：**このソリューションには、脅威の調査の強化および対応機能を提供する SecureX プラットフォームが組み込まれています。Secure Network Analytics は SecureX と統合して、可視性を統合し、脅威への対応を簡素化し、すべての脅威ベクトルとアクセスポイントの自動化を可能にします。

ソリューションのコンポーネント

Secure Network Analytics の中核となる必要なコンポーネントには、マネージャ、フローコレクタ、および Flow Rate License があります。さらに、フローセンサー、Cisco Telemetry Broker、データストアなどのオプションのコンポーネントを提供します。これらのコンポーネントは、柔軟で堅牢なアーキテクチャを提供するためにも利用できます。

システムに必要なコンポーネント

マネージャ

Secure Network Analytics マネージャは、最大 25 のフローコレクタ、Cisco Secure Network Access（旧 Cisco Identity Services Engine）、およびその他のソースからの分析を集約、整理、および表示します。包括的な分析用として、ネットワークトラフィック、ID 情報、カスタマイズされたサマリーレポート、および統合されたセキュリティとネットワーク インテリジェンスのグラフィカル表示を使用します。

マネージャのキャパシティによって、分析および表示できるテレメトリデータの量と、展開されるフローコレクタの数が決まります。マネージャは、ハードウェアアプライアンスまたは仮想マシンとして使用できます。表 1 に、マネージャの利点を示します。

表 1. マネージャの主な利点

利点	説明
リアルタイムの最新データ	数百あるネットワークセグメント間のトラフィックを同時にモニターするデータフローを提供して、疑わしいネットワークの動作を特定できます。この機能は、特にエンタープライズレベルで役立ちます。
セキュリティの脅威を検出して優先順位を付ける機能	セキュリティ上の脅威の速やかな検出と優先順位付け、ネットワークの不正使用と準最適なパフォーマンスの特定、全社でのイベント応答の管理を、単独のコントロールセンターからすべて行うことができます。
アプライアンスの管理	フローコレクタ、フローセンサー、UDP Director などの Cisco Network Analytics アプライアンスを設定、調整、および管理します。
複数のタイプのフローデータの使用	NetFlow、IPFIX、sFlow など、複数のタイプのフローデータを使用します。その結果、コスト効率に優れた、動作ベースのネットワーク保護が実現します。
拡張性	最大規模のネットワーク要求にも対応します。非常に高速な環境で優れたパフォーマンスを発揮し、IP に接続可能なネットワークのあらゆる部分をサイズに関係なく保護できます。
ネットワーク トランザクションの監査証跡	より効果的なフォレンジック調査のために、すべてのネットワーク トランザクションの完全な監査証跡を提供します。
リアルタイムでカスタマイズ可能なリレーショナルフローマップ	組織のトラフィックの現在の状態をグラフィカル表示します。管理者は、場所、機能、仮想環境などの任意の基準に基づいて、組織のネットワークの構造マップを簡単に表示できます。2 つのホストグループ間に接続が作成されるため、それらの間を移動するトラフィックを迅速に分析することができます。次に、問題となっているデータポイントを選択するだけで、特定の時点で起きている状況をさらに詳しく把握できます。
柔軟な配信オプション	あらゆる規模の組織に適したスケーラブルなデバイスである、物理アプライアンスを注文できます。 また、VMware または KVM ハイパーバイザ環境ではアプライアンスエディションと同じ機能を実行するように設計されたバーチャルエディションを注文することもできます。

マネージャの仕様書

- Secure Network Analytics マネージャ 2210：製品番号：ST-SMC2210-K9
- Secure Network Analytics マネージャ 2300：製品番号：ST-SMC2300-K9
- Secure Network Analytics マネージャ バーチャル エディション：製品番号：L-ST-SMC-VE-K9

フローコレクタ

フローコレクタは、ルータ、スイッチ、ファイアウォール、エンドポイント、その他のネットワーク インフラストラクチャ デバイスなどの既存のインフラストラクチャから、NetFlow、IPFIX（インターネット プロトコル フロー情報エクスポート）、NVM、SYSLOG などのエンタープライズ テレメトリ タイプを収集して保存します。フローコレクタは、プロキシデータソースからテレメトリを収集することもできます。これは、クラウドベースの機械学習エンジン（グローバル脅威アラート）で分析できます。

テレメトリデータが分析され、ネットワークアクティビティの全容が示されます。フォレンジック調査やコンプライアンスの取り組みを改善するために使用できる監査証跡を作成して、何ヵ月または何年ものデータを保存できます。ネットワークから収集できるテレメトリの量は、展開されたフローコレクタの合計容量によって決まります。複数のフローコレクタをインストールできます。フローコレクタは、ハードウェアアプライアンスまたは仮想マシンとして使用できます。表 2 に、フローコレクタの利点について示します。

表 2. フローコレクタの主な利点

利点	説明
脅威の検出	プロキシレコードを取得してフローレコードに関連付け、各フローのユーザーアプリケーションと URL 情報を提供して、コンテキスト認識を改善します。このプロセスにより、組織は脅威を正確に特定できるようになり、平均到達時間（MTTK）が短縮されます。
フロー トラフィック モニタリング	数百あるネットワークセグメント間のフロートラフィックを同時にモニターするため、疑わしいネットワークの動作を特定できます。この機能は、特にエンタープライズレベルで役立ちます。
データ保持期間の拡大	組織や代理店が大量のデータを長期間保持できるようにします。
拡張性	非常に高速な環境で優れたパフォーマンスを発揮し、IP に接続可能なネットワークのあらゆる部分をサイズに関係なく保護できます。
重複排除とスティッチング	重複排除を実行して、複数のルータを通過した可能性のあるフローが一度だけカウントされるようにします。次に、フロー情報をつなぎ合わせて、ネットワーク トランザクションを完全に可視化します。
配信方法の選択	あらゆる規模の組織に適したスケーラブルなデバイスである、アプライアンスエディションを注文できます。 また、VMware または KVM ハイパーバイザ環境ではアプライアンスエディションと同じ機能を実行するように設計されたバーチャルエディションを注文することもできます。このソリューションは、割り当てられたリソースに応じて動的に拡張されます。

フローコレクタの仕様書

- Secure Network Analytics フローコレクタ 4210：製品番号：ST-FC4210-K9
- Secure Network Analytics フローコレクタ 5210：製品番号：ST-FC5210-K9
- Secure Network Analytics フローコレクタ 4300：製品番号：ST-FC4300-K9
- Secure Network Analytics フローコレクタ バーチャル エディション：製品番号：L-ST-FC-VE-K9

データストア

データストアは、1 つ以上のフローコレクタの容量を超える高いデータ取り込み容量レベルまたは長期保存時間を必要とする環境向けのソリューションを提供します。データストアクラスタは、Secure Network Analytics マネージャとフローコレクタ間に追加できます。これらのより大規模で大規模なネットワークの場合、1 つ以上のフローコレクタがフローデータを取り込んで重複排除し、分析を実行してから、フローデータとその結果をデータストアに直接送信します。次に、このフローデータは 3 つ以上のデータノードアプライアンスで構成されるデータストアに均等に分散されます。データストアによってフローデータストレージを容易にし、すべてのネットワークテレメトリを、分散型モデルの複数のフローコレクタに分散させるのではなく一元化された場所に保持します。この新しい一元化モデルでは、分散型モデルに比べてストレージ容量やフローレートの取り込み容量が増大するだけでなく、復元力も向上します。

表 3. データストアの主な利点

利点	説明
データ取り込み容量の増加	Data Store を組み合わせて 300 万フロー/秒（FPS）超を監視できる単一のデータノードのクラスタを作成し、大量のフローを処理する組織の取り込み帯域幅に対する課題を軽減します。
エンタープライズクラスのデータ復元力	テレメトリデータはノード全体に冗長的に保存されるため、1 つのノードでの障害時にもシームレスにデータを利用でき、テレメトリデータの損失を防ぐことができます。2 つ以上のデータストアがある展開では、データノードの損失の最大 50% をサポートし、運用を継続できるようにします。* また、データストアは、ネットワークのアップグレードや計画外の停止時にも完全な運用を維持できるように、冗長集約スイッチをサポートしています。 *ハードウェアの構成やインストールによって異なります。
クエリとレポートの応答時間の大幅な改善	データストアによってクエリパフォーマンスとレポート応答時間が劇的に改善され、他の標準的な導入モデルよりも 10 倍以上高速化されています。また、API または Secure Network Analytics マネージャの Web UI を使用して、同時実行クエリの数を増やすことができます。これらのクエリの改善により、運用効率が大幅に向上します。データストアでは、レポートを実行してより迅速に回答を得ることができるため、担当者は脅威を今まで以上にすばやく特定してそれに対応し、トリアージ、調査、および修復のワークフローを迅速に進めることができます。
ストレージの拡張性	データストアは、データベースクラスタを追加する機能により、拡大を続けるネットワークを持つ組織に対してデータストレージの拡張性に関する柔軟性の強化を実現します。
長期データ保持	スケーラブルで長期的なテレメトリのストレージ機能により、フローコレクタを追加することなく、最大 1 ～ 2 年分のデータを長期間保持できます。これは、規制要件を満たし、サードパーティのストレージソリューションまたは追加のフローコレクタの購入と統合に関連するコストと複雑さを軽減するのに役立ちます。

データストアの仕様

- Cisco Secure Network Analytics Data Store 6200：製品番号：ST-DS6200-K9
- Cisco Secure Network Analytics Data Store 6300：製品番号：ST-DN6300-K9
- Cisco Secure Network Analytics Virtual Data Store：製品番号：L-ST-DS-VE-K9

詳細については、『Secure Network Analytics Data Store Solution Overview』を参照してください。

フローレートライセンス

Secure Network Analytics Manager で集約されたフローテレメトリを収集、管理、および分析するには、フローレートライセンスが必要です。フローレートライセンスは、収集される可能性のあるフローの量を定義し、1 秒あたりのフロー数（FPS）に基づいてライセンスされます。必要なレベルのフロー容量を実現するために、ライセンスを任意の組み合わせで並べ替えることができます。

- Cisco Secure Network Analytics フローレートライセンス 100 パック：製品番号：ST-FR-100-LIC
  - Secure Network Analytics XaaS サブスクリプションを通じて注文可能：製品番号：ST-SEC-SUB

システムのオプションコンポーネント

Flow Sensor

フローセンサーはオプションのコンポーネントです。NetFlow をネイティブに生成できないスイッチングおよびルーティング インフラストラクチャのセグメントにテレメトリを生成します。また、アプリケーション レイヤ データに対する可視性も提供します。Secure Network Analytics で収集されたすべてのテレメトリに加えて、フローセンサーではセキュリティ分析を強化するための追加のセキュリティコンテキストを提供します。また、Secure Network Analytics ソフトウェアリリース 7.1 以降、フローセンサーは、暗号化されたトラフィックを分析できるように、拡張された暗号化トラフィック分析テレメトリを生成することもできます。高度な動作モデリングであるクラウドベースのマルチレイヤ機械学習がこのデータセットに適用され、高度な脅威を検出し、これまで以上に迅速な調査を実施します。

フローセンサーは、ミラーリングポートまたはネットワークタップにインストールされ、観測されたトラフィックに基づいてテレメトリを生成します。ネットワークから生成されるテレメトリの量は、展開されたフローセンサーの容量によって決まります。複数のフローセンサーをインストールできます。フローセンサーは、仮想マシン環境をモニターするためにハードウェアアプライアンスまたは仮想アプライアンスとして使用できます。また、追加のセキュリティコンテキストを必要とするオーバーレイ モニタリング ソリューションが IT 組織の運用モデルにより適している環境でも機能します。

表 4. フローセンサーの主な利点

利点	説明
レイヤ 7 アプリケーションの可視性	アプリケーション情報を収集することで、レイヤ 7 アプリケーションの真の可視性を提供します。これには、RTT（ラウンドトリップ時間）、SRT（サーバー応答時間）、再送信などのデータ機能が含まれます。
パケットレベルのパフォーマンスおよび分析	アプリケーション情報を収集することで、レイヤ 7 アプリケーションの真の可視性を提供します。これには、RTT、SRT、再送信などのデータ機能が含まれます。

利点	説明
ネットワーク異常に関するアラート	Web トラフィックの URL 情報や TCP フラグの詳細など、フローセンサーの追加のテレメトリによって、セキュリティ担当者が迅速な対応を行い、損害を軽減できるようコンテキストに応じたインテリジェンスを使用してアラームを生成することができます。
コストの削減	問題またはインシデントの根本原因を数秒以内に特定して切り分けることで、運用効率を高め、コストを削減します。
配信方法の選択	あらゆる規模の組織に適したスケーラブルなデバイスである、アプライアンスエディションを注文できます。 また、VMware または KVM ハイパーバイザ環境ではアプライアンスエディションと同じ機能を実行するように設計されたバーチャルエディションを注文することもできます。

フローセンサーの仕様書

- Secure Network Analytics フローセンサー 1210：製品番号：ST-FS1210-K9
- Secure Network Analytics フローセンサー 3210：製品番号：ST-FS3210-K9
- Secure Network Analytics フローセンサー 4210：製品番号：ST-FS4210-K9
- Secure Network Analytics フローセンサー 4240：製品番号：ST-FS4240-K9
- Secure Network Analytics フローセンサー 1300：製品番号：ST-FS1300-K9
- Secure Network Analytics フローセンサー 3300：製品番号：ST-FS3300-K9
- Secure Network Analytics フローセンサー 4300：製品番号：ST-FS4300-K9
- Secure Network Analytics フロー センサー バーチャル エディション：製品番号：L-ST-FS-VE-K9

Cisco Telemetry Broker

Cisco Telemetry Broker は、さまざまなテレメトリソースからネットワークテレメトリを取り込み、それらのデータ形式を変換してから、そのテレメトリを 1 つまたは複数の宛先に転送することができます。たとえば、次のいずれかを取り込むことができます。

- NetFlow、syslog、IPFIX などのオンプレミス ネットワーク テレメトリ
- AWSVPC フローログや AzureNSG フローログなどのクラウドベースのテレメトリソース

また、そのテレメトリを次の宛先例のいずれか、またはすべてに転送できます。

- Cisco SNA、Cisco XDR
- Hadoop などの分析プラットフォーム
- Cisco DNA Center および Cisco Nexus Dashboard Insights などのネットワーク管理および自動化プラットフォーム
- セキュリティ情報とイベント管理（SIEM）プラットフォーム
- Cisco Security Analytics や Logging（オンプレミス）などのストレージ/スマートキャプチャ

Telemetry Broker は、NetFlow、Syslog、IPFIX などのオンプレミス ネットワーク テレメトリだけでなく、クラウドベースの AWS VPC フローログや Azure NSG フローログなどの他の非伝統的なテレメトリソースも取り込み、IPFIX レコードに、または Secure Network Analytics と互換性のあるその他のデータ形式に変換できます。これにより、非標準のソースからネットワークテレメトリを取り込み、分析する機能を通じて、Secure Network Analytics のデータ収集機能がさらに拡張されます。

表 5. Cisco Telemetry Broker の主な利点

利点	説明
データの仲介	テレメトリデータを送信元の場所から複数の宛先の消費者にルーティングおよび複製して、新しいテレメトリベースのツールの迅速なオンボーディングを容易にする機能。
データのフィルタリング	消費者に複製されているデータをフィルタリングして、消費者が表示および分析できるものをきめ細かく制御する機能。高価なツールにデータを送信する必要がなくなるため、ユーザーにとってはお金の節約にもなります。
データの変換	データプロトコルを、エクスポータから選択した消費者のプロトコルに変換する機能。これにより、Secure Network Analytics およびその他のツールは、互換性のない複数の以前のデータ形式を使用できるようになります。

Cisco Telemetry Broker の仕様

- Cisco Telemetry Broker アプライアンス：製品番号：ST-TB2300-K9
- Cisco Telemetry Broker 100GB/1 日ライセンス：製品番号：TB-ESS-100GB
- Cisco Telemetry Broker サブスクリプションを通じて注文可能：製品番号：TB-SEC-SUB

詳細については、Cisco Telemetry Broker データシートを参照してください。

追加のライセンス

追加された機能に使用できるその他のオプションのライセンスは次のとおりです。

Cisco Secure Network Analytics エンドポイントライセンス：エンドユーザーデバイスの可視性を拡張するためのライセンスアドオンとして利用できます。エンドポイントライセンスは、モバイル リモート ワーカー エンドポイント アクティビティの完全かつ継続的な可視性を提供することにより、組織がリモートワーカーを保護するのに役立ちます。（Cisco AnyConnect® Network Visibility Module（NVM）を別途購入する必要があります）。

- Cisco Secure Network Analytics エンドポイントライセンス：製品番号：ST-EP-LIC
- Secure Network Analytics XaaS サブスクリプションを通じて注文可能：製品番号：ST-SEC-SUB

詳細については、『Cisco Secure Network Analytics Endpoint License At-a-Glance』を参照してください。

Cisco Secure Network Analytics 脅威フィード：業界をリードする脅威インテリジェンスグループ、Cisco Talos® が提供するグローバルな脅威インテリジェンスフィードです。ボットネットやその他の高度な攻撃に対するさらなる予防策となります。ローカルネットワーク環境での疑わしいアクティビティを、既知の数千ものコマンドアンドコントロール サーバーおよびキャンペーンのデータと関連付けて、信頼性の高い検出と迅速な脅威対応を実現します。Cisco Talos は、1 日あたり 150 万件のマルウェアサンプルを検出し、200 億もの脅威をブロックしています。

展開内のフローコレクタごとに脅威フィードライセンスが必要です。以下は、各フローコレクタモデルの脅威フィードの製品 ID です。

- FC1K ライセンスの Cisco Secure Network Analytics 脅威フィード：製品番号：L-LC-TI-FC1K=
- FC2K ライセンスの Cisco Secure Network Analytics 脅威フィード：製品番号：L-LC-TI-FC2K=
- FC4K ライセンスの Cisco Secure Network Analytics 脅威フィード：製品番号：L-LC-TI-FC4K=
- FC5K ライセンスの Cisco Secure Network Analytics 脅威フィード：製品番号：L-LC-TI-FC5K=

詳細については、『Cisco Secure Network Threat Feed License At-a-Glance』を参照してください。

Security Analytics and Logging On-premises：Security Analytics and Logging（SAL）オンプレミスは、大規模なファイアウォールの展開にエンタープライズクラスの集中ログ管理とストレージを提供します。平均保持期間 30 日で、1 秒あたり 100,000 イベント（EPS）の持続レートでファイアウォールロギングをサポートできます。さらに、このサービスは API を介してこの広範なデータセットを Cisco Firewall Management Console（FMC）に接続し、FMC のデータストレージ容量を 300 倍（つまり 30,000%）効果的に強化します。

Security Analytics and Logging（SAL）オンプレミスは、Secure Networks Analytics リリースバージョン 7.3.1 以降にインストールできる、無料でダウンロード可能なアプリケーションを介して提供されます。サービスを実行するには、ユーザーはボリュームベースのライセンスを購入する必要があります。これは次のようにして利用できます。

- アラカルトライセンス：製品番号：SAL-OP-LT-1GB
- 親製品 ID を通じて注文可能：製品番号：SAL-SUB
- ファイアウォール サブスクリプションに添付されたバンドルライセンス：製品番号：SEC-LOG-OP
- 親製品 ID で注文可能：製品番号：FPR1150-NGFW-K9

SAL オンプレミスは、次の 2 つの展開アーキテクチャ（ハードウェアまたは仮想）のいずれかでホストできます。

- シングルノード：20,000 ファイアウォール eps をスケーリング、またはマルチノード：100,000 ファイアウォール eps をスケーリング
  - Cisco Secure Network Analytics Manager：製品番号：SMC-2210-K9 または SMC-2300-K9
  - Secure Network Analytics フローコレクタ 4210：製品番号：ST-FC4210-K9 または ST-FC4300-K9
  - Cisco Secure Network Analytics Data Store 6200：製品番号：ST-DS6200-K9 または ST-DN6300-K9
    詳細については、『Data Store Solution Overview』を参照してください。

詳細については、オーダーガイド、スタートアップガイドを参照するか、cisco.com/go/sal にアクセスしてください。

M6 ハードウェアアプライアンスの Field Replaceable Unit（FRU）

表 6 に、M6 ハードウェアの Field Replaceable Unit（FRU）として使用できる Cisco Secure Network Analytics のコンポーネントのスペアを示します。

表 6. M6 ハードウェア：Cisco Secure Network Analytics のスペアコンポーネント

製品番号	適用可能な製品	説明
UCS-HD600G10K12N=	FS3300 および FS4300	600GB 12G SAS 10K RPM SFF HDD
UCS-HD12TB10K12N=	SMC2300 および FC4300	1.2 TB 12 G SAS 10K RPM SFF HDD
UCS-HD18TB10K4KN=	DN6300	1.8 TB 12G SAS 10K RPM SFF HDD（4K）
UCSC-PSU1-1050W=	FS3300、FS4300、SMC2300、FC4300、DN6300	ラックサーバープラチナム用 Cisco UCS 1050W AC 電源

注文情報

Secure Network Analytics は、1 年、3 年、および 5 年間のサブスクリプションとして利用できます。

Secure Network Analytics SaaS および Secure Cloud Analytics では、1 か月、12 か月、24 か月、36 か月、および 60 か月のサブスクリプションを利用できます。1 か月および 12 か月の自動更新というオプションもあります。期間オプションを選択した後で、パブリック クラウド モニタリングおよびプライベート ネットワーク モニタリングのサービスを追加できます。

発注の際は、代理店に問い合わせてください。

表 7 に、M5 ハードウェアの Field Replaceable Unit（FRU）として使用できる Cisco Secure Network Analytics のコンポーネントのスペアを示します。

表 7. M5 ハードウェア：Cisco Secure Network Analytics 用のスペアコンポーネント

製品番号	適用可能な製品	説明
ST-M5-HDD-600GB=	FS1210、FS3210、FS4210、FS4240、UDP2210、FC5210-E	Cisco Stealthwatch 600 GB 12G SAS 10K RPM SFF HDD
ST-M5-HDD-1.2TB=	SMC2210、FC4210、FC5210-D、DS6200	Cisco Stealthwatch 1.2 TB 12G SAS 10K RPM SFF HDD
ST-M5-PWR-AC-770W=	FS1210、FS3210、FS4210、FS4240、SMC2210、FC4210、FC5210-E、FC5210-D、DS6200、UDP2210	Cisco Stealthwatch AC 電源 770 W
ST-M5-PWR-AC-1050=	FS1210、FS3210、FS4210、FS4240、SMC2210、FC4210、FC5210-E、FC5210-D、DS6200、UDP2210	Cisco Stealthwatch AC 電源 770 W

製品番号	適用可能な製品	説明
UCSC-RAILB-M4=	FS1210、FS3210、FS4210、FS4240、SMC2210、FC4210、FC5210-E、FC5210-D、DS6200、UDP2210	C220 および C240 M4、M5 ラック サーバー用ボール ベアリング レール キット

シスコの環境保全への取り組み

シスコの企業の社会的責任（CSR）レポートの「環境保全」セクションでは、製品、ソリューション、運用、拡張運用、サプライチェーンに対する、シスコの環境保全ポリシーとイニシアチブを掲載しています。

次の表に、環境保全に関する主要なトピック（CSR レポートの「環境保全」セクションに記載）への参照リンクを示します。

持続可能性に関するトピック	参照先
製品の材料に関する法律および規制に関する情報	材料
製品、バッテリ、パッケージを含む電子廃棄物法規制に関する情報	WEEE 適合性

シスコでは、パッケージデータを情報共有目的でのみ提供しています。これらの情報は最新の法規制を反映していない可能性があります。シスコは、情報が完全、正確、または最新のものであることを表明、保証、または確約しません。これらの情報は予告なしに変更されることがあります。

サービスおよびサポート

Secure Network Analytics には、いくつかのサービスプログラムが用意されています。シスコのサービスは、お客様のネットワーク投資を保護してネットワーク運用を最適化するだけでなく、ネットワーク インテリジェンスの強化や事業拡張に向けた新しいアプリケーションの導入準備という面でもサポートします。プロフェッショナルサービスの詳細については、テクニカルサポートのホームページを参照してください。

Cisco Capital

目的達成に役立つ柔軟な支払いソリューション

Cisco Capital® により、目標を達成するための適切なテクノロジーを簡単に取得し、ビジネス変革を実現し、競争力を維持できます。総所有コスト（TCO）の削減、資金の節約、成長の促進に役立ちます。100 ヵ国あまりの国々では、ハードウェア、ソフトウェア、サービス、およびサードパーティの補助機器を購入するのに、シスコの柔軟な支払いソリューションを利用して、簡単かつ計画的に支払うことができます。詳細はこちらをご覧ください。

詳細情報

Secure Network Analytics の詳細については、https://www.cisco.com/go/secure-network-analytics を参照するか、シスコのセキュリティアカウント担当者に問い合わせの上、無料の Secure Network Analytics 可視性アセスメントに参加して、組織が拡張されたネットワークで可視性を確保する方法について確認してください。

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

Printed in USA C78-739398-10 01/24