Cisco Secure Cloud Analytics データシート

2022 年 12 月

目次

Cisco Secure Cloud Analytics データシート

このドキュメントでは、Cisco Secure Cloud Analytics（旧 Stealthwatch Cloud Public Cloud Monitoring）の製品概要と注文情報について説明します。

製品の詳細については、https://www.cisco.com/c/ja_jp/products/security/stealthwatch-cloud/index.html を参照してください。

パブリッククラウド、オンプレミス、およびハイブリッド環境を保護するために必要な可視化と継続的な脅威検出を実現します。

製品の概要

組織がより多くの IT リソースをパブリッククラウドに移行し、ビジネスサービスを分散させ、従業員がどこからでも接続できるようになると、潜在的な攻撃者が気付かれることなく、組織の環境に侵入できる可能性が高くなります。セキュリティ組織は、セキュリティスイートの他のツールと連携して、ネットワークとサービスのさまざまな場所に可視性を拡張し、日常の環境のノイズに潜む潜在的な攻撃者を特定するソリューションを必要としています。Cisco Secure Cloud Analytics は、Amazon Web Services（AWS）、Microsoft Azure、Google Cloud Platform などすべての主要なクラウド環境で組織を保護するために必要な可視性と脅威検出機能を、既存のオンプレミスネットワークと、それぞれのサービスに接続している従業員に提供します。

Secure Cloud Analytics は、包括的な可視性と低ノイズで高精度のアラートを、エージェントを使用せずに提供します。Secure Cloud Analytics は、クラウドベースの Software-as-a-Service（SaaS）で提供されるソリューションです。ランサムウェアやその他のマルウェア、データ漏洩、ネットワークの脆弱性、システム、イベントと構成のリスクを検出し、侵害を示すロールの変更を検出し、エンドポイント検出およびクラウド セキュリティソリューションを補完する異常と動作の検出機能を提供します。これらのソリューションでは、各アセットからの可視性を拡張することにより個々のワークロードとコンピュータが保護されるため、全体像がより理解され、脅威がより迅速に捕捉されて応答時間が短縮されます。

Cisco Secure Cloud Analytics には、統合と応答を可能にするために、最も包括的で統合されたセキュリティ プラットフォームである Cisco SecureX が付属しており、可視性の統合、脅威への対応の簡素化、あらゆる脅威媒体とアクセスポイントでの自動化を実現します。

機能とメリット

機能	利点
ネットワークおよびクラウド分析	デバイスレベルのネットワークトラフィックと通信パターンの完全に自動化されたリアルタイム分析を提供し、パブリッククラウドおよびプライベートネットワークで動作するすべてのデバイスとリソースを可視化します。
忠実度の高いセキュリティアラートによる平均検出時間の短縮	実用的なインテリジェンスを提供し、誤検出を減らして、スマートなセキュリティアクションを実現し、平均検出時間と脅威への応答時間を短縮します。
組み込み SecureX プラットフォーム	業界で最も包括的かつ統合的なセキュリティ プラットフォームで、可視性の統合、脅威への対応の簡素化、および自動化を実現します。
MITRE にマッピングされた調査結果	Cisco Secure Cloud Analytics のアラートの大部分は、MITRE Tactics and Techniques にマッピングされており、調査結果を理解して対応するための業界標準の方法を提供します。
Software as a Service（SaaS）	組織が大規模にセキュリティを導入する際に必要とされる使いやすさ、導入の容易さ、および柔軟性が強化されます。
エンティティモデリング	ネットワーク上のすべてのデバイスおよびエンティティの動作モデルを提供します。このモデルは、動作の突然の変化や、脅威を示す悪意のあるアクティビティを自動的に識別するために使用されます。
自動ロール分類	動作に基づいて、各ネットワークデバイスとクラウドリソースのロールを自動的に識別します。
エージェントレスの展開	ネットワークおよび Amazon Web Services（AWS）、Microsoft Azure、および Google Cloud Platform（GCP）クラウドインスタンスからのテレメトリのネイティブソースおよびログを使用します。特殊なハードウェアまたはソフトウェアエージェントは必要ありません。
広範な可視性による応答までの平均時間の短縮	ネットワークとパブリッククラウド全体のデバイスの影響範囲を理解し、Cisco Secure Cloud Analytics、またはエンドポイント セキュリティ ソリューションやファイアウォールなどの他のツールで検出された可能性のあるアクティブなインシデントをすばやく理解して修正する方法を提供します。

ネットワークの可視性は不可欠

今日の企業は、プライベートネットワーク上のデバイスの数が増加し、より多くのワークロードがパブリッククラウドに移行するにつれて、セキュリティの「盲点」に対処しています。一方、セキュリティ担当者には、対応不能になるほどセキュリティアラートが殺到しています。また、エンドポイント、ネットワーク、クラウドセキュリティなど、一連の保護を提供するさまざまなセキュリティ対策に焦点を当てる必要があります。異常、行動、IOC 検出はすべて、単一の方法では成功が保証されない状況で、攻撃者を補足するためのさまざまなレベルの可視性を提供します。多くの攻撃では、攻撃者は目的を達成するためにネットワークと対話する必要があります。これらの検出アプローチとカバレッジ領域を組み合わせることで、攻撃者の熟練度に関係なく、組織に侵入したときに攻撃者を検出するためのより堅牢なソリューションを実現できます。

Cisco Secure Cloud Analytics は、ネットワークとパブリッククラウド全体で異常、行動脅威、IOC 検出を提供し、他のセキュリティ製品では確認できない領域を可視化し、ポイント セキュリティ ソリューションでは確認できない攻撃者を特定するのに役立ちます。Cisco Secure Cloud Analytics は、パブリッククラウドやプライベートネットワークのテレメトリのソースとログを使用し、動作をモデル化して脅威のアクティビティを特定することでこれを実現します。

可視性と分析

このテレメトリは Secure Cloud Analytics で処理され、プライベートネットワーク、ブランチ、パブリッククラウドなどの最新のネットワークによってアクティブなすべてのエンティティに対する可視性が提供されます。Secure Cloud Analytics は、エンティティモデリングを使用してさまざまな脅威アクティビティを高い精度で検出できます。信頼度の高いセキュリティアラートがよりスマートなセキュリティ判断をサポートし、誤報の数を減らして調査に費やす時間を短縮します。

柔軟性と使いやすさ

Secure Cloud Analytics は Software as a Service（SaaS）として提供されるため、試用、購入、利用が容易です。専用ハードウェアを購入する必要がなく、ソフトウェアエージェントの導入や特別な専門知識も不要です。

ソリューションがデータの受信を開始した時点からは、追加の設定やデバイスの分類は必要ありません。すべての分析が自動化されているため、運用に必要な管理およびセキュリティに関する専門知識はほとんど必要ありません。

高度な脅威検出のためのエンティティモデリング

テレメトリが収集されると、Secure Cloud Analytics は、ネットワーク上またはモニター対象のパブリッククラウド内にあるすべてのアクティブエンティティのモデル（一種のシミュレーション）を作成します。このモデリングを使用することで、侵害の初期段階や隠された兆候を迅速に特定できます。更新するシグニチャリストや展開するソフトウェアエージェントはありません。

各モデルは、エンティティ動作の次の 5 つの主要な項目で構成されます。

- **予測：**過去のアクティビティに基づいてエンティティの動作を予測し、これらの予測に対して観測された動作を評価します。
- **グループ：**類似するエンティティと比較することで、エンティティの動作の一貫性を評価します。
- **ロール：**エンティティの動作に基づいてロールを決定し、そのロールと一致しないアクティビティを検出します。

- **ルール：**エンティティが組織のポリシーに違反した場合（プロトコルとポートの使用、デバイスとリソースのプロファイル特性、ブロックリストに記載された通信など）に検出します。
- **一貫性：**データ伝送とアクセスの両方の特性において、デバイスが過去の動作から大きく逸脱したタイミングを認識します。

エンティティモデリングを利用すると、潜在的な脅威に関連するさまざまな動作を検出できます。たとえば、Secure Cloud Analytics ではパブリッククラウドリソースを自動分類します。このリソースの動作では、類似するエンティティの動作との比較が経時的に行われます。これらの通信パターンによって「通常の」動作のベースラインが構築され、このベースラインから逸脱するトラフィックがある場合に、ユーザーは電子メールや他のシスコアプリを介してカスタムアラートを受信できます。また、Cisco SecureX プラットフォームまたは他のサードパーティ ソリューションを介して脅威を修復することも可能です。Secure Cloud Analytics は、すべての主要なパブリック クラウド プロバイダーのロールを識別できます。ほぼリアルタイムで新しい動作をすべて検出し、疑わしいトラフィックの詳細とともにアラートを生成します。

DNS の不正使用、地理的に異常なリモートアクセス、永続的なリモート制御接続、および潜在的なデータベースのデータ漏洩は、Secure Cloud Analytics によるアラートの例です。さらに、上位の IP、最も使用されているポート、トラフィックの統計情報を含むアクティブなサブネットなどのネットワークレポートを使用できます。

Cisco Secure Cloud Analytics を使用すると、ネットワークとクラウド全体にわたる広範な可視性と、強力な行動分析を活用することにより、未知、高度、または見逃された脅威をより簡単かつ迅速に特定するのに役立つだけでなく、この同じ可視性により、エンドポイントセキュリティなどの別のセキュリティソリューションで脅威が検出されたときに迅速に対応できます。

提供内容

Secure Cloud Analytics

ソリューションは、ソフトウェアエージェントを使用する代わりに、仮想プライベートクラウド（VPC）のフローログやオンプレミスの IPFIX などテレメトリのネイティブソースに依存して展開できます。Secure Cloud Analytics は、組織のリソースおよび機能によって生成されるすべての IP トラフィックをモデル化します。VPC 内または VPC 間にあるか、外部 IP アドレス宛てであるかは問いません。また、ネットワーク上の攻撃者の動作を検出し、組織のクラウド環境に深く侵入するために、Cloud Trail、Cloud Watch、Config、Inspector、Identity and Access Management（IAM）、Lambda など多くの追加のクラウド サービス プロバイダー API と統合されます。

注文情報

Secure Cloud Analytics 製品 ID：ST-CL-SUB

ライセンスはサブスクリプションベースで、期間は 1 か月、12 か月、24 か月、36 か月、および 60 か月の中から選択できます。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 モニタリングやプライベート 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、シスコの代理店にお問い合わせください。

セキュリティ向け Cisco Software Support

セキュリティ向け Cisco Software Support の基本的なオンライン サポート オプションは、Secure Cloud Analytics サブスクリプションで利用できます。基本的なオンラインサポートでは、購入したソフトウェア サブスクリプションの全期間にわたって次の基本的なサポートを提供します。

オンラインツールによるサポートへのアクセス。電話によるサポートは提供されていません。

シスコは送信されたケースに対し、翌営業日の標準業務時間内までに応答します。

Secure Cloud Analytics のサブスクリプションを注文すると、基本的なオンラインサポートがそのサブスクリプションの一部として組み込まれます。これは個別に注文できるサービスではありません。したがって、Secure Cloud Analytics のサブスクリプションが更新されると、基本的なオンラインサポートも同じ期間で更新されます。SaaS サブスクリプションでこのサポートを受けるにあたって、製品の追加購入や追加料金は不要です。

Cisco Software Support の詳細については、サービスの説明を参照してください。

環境を今すぐ保護

リスクのない 60 日間の無料トライアルで、今すぐ Secure Cloud Analytics をお試しください。詳細については、https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html を参照するか、お近くのシスコアカウント担当者にお問い合わせください。

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。

シスコ コンタクトセンター

自社導入をご検討されているお客様へのお問い合わせ窓口です。
製品に関して ｜ サービスに関して ｜ 各種キャンペーンに関して ｜ お見積依頼 ｜ 一般的なご質問

お問い合わせ先
お電話での問い合わせ
平日 9:00 - 17:00
0120-092-255

お問い合わせウェブフォーム
cisco.com/jp/go/vdc_callback

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
cisco.com/jp

0209-2023-000-X