Cisco Secure Access

クラウドベースの俊敏なセキュリティでハイブリッドワーカーを保護

2024 年 2 月

© 2024 Cisco and/or its affiliates. All rights reserved.

目次

© 2024 Cisco and/or its affiliates. All rights reserved.

クラウドベースの俊敏なセキュリティでハイブリッドワーカーを保護

ハイブリッドワークとセキュリティサービスエッジ

新しいハイブリッドワークの時代に伴ってセキュリティへのアプローチを見直す必要がある中、あらゆる組織のハイブリッドワーク戦略において重要な成功の鍵を握っているのが、SSE（セキュリティサービスエッジ）です。SSE は、複数のセキュリティ機能をクラウドに集約し、あらゆる場所で働く従業員、請負業者、パートナーを保護するとともに、重要なリソースも保護します。セッションが、プライベートデータセンター、SaaS ロケーション、ピアツーピア、IaaS またはインターネットサイトのどこでアプリケーションを実行しても、SSE は「セキュリティの仲介者」として機能し、悪意のあるさまざまなアクティビティを特定して阻止します。エンドユーザーは、オフィス、自宅、外出先など、どこで仕事をしても、安全で透過的なユーザー体験が確保されます。SSE ソリューションは、優れたユーザーエクスペリエンスの提供、IT の複雑さの軽減、およびセキュリティの有効性の向上という 3 つの主要な要件に対応する必要があります。

製品の概要

Cisco Secure Access は、ゼロトラストに基づく統合型のクラウドセキュリティ SSE ソリューションであり、場所を問わずシームレスで透過的かつ安全なアクセスを提供します。シスコの受賞歴のある Umbrella セキュア インターネット アクセス ソリューションは、より多くの機能を網羅する Secure Access という名称で拡張され、より多くの SSE 関連機能をカバーするようになりました。すべてのコア SSE コンポーネント（SWG、CASB、ZTNA、FWaaS）に加えて、拡張された一連の機能（マルチモード DLP、DNS セキュリティ、RBI、サンドボックス分析、DEM インサイト、Talos 脅威インテリジェンスおよび AI 使用の安全対策）が 1 つのライセンスと管理プラットフォームに含まれるようになりました。これらの機能をすべて 1 つのクラウド型プラットフォームで活用することで、組織はさまざまなセキュリティ上の課題を解決できるようになります。また、ユーザーは、プロトコルやポート、カスタマイズのレベルに関係なく、必要なすべてのリソースとアプリに安全かつシームレスにアクセスできるようになります。

Cisco Secure Access は、他の相乗的なコンポーネントとの相互運用性を容易にする共通の管理制御、データ構造、およびポリシー管理を備えた設計となっています。たとえば、SAML ベースのサービス（AD、Azure AD、Okta、Ping など）を含む広範なアイデンティティ プロバイダー（IDP）が、アイデンティティの確認とコンテキストを提供します。このソリューションは、SD-WAN、XDR、デジタル エクスペリエンス モニタリングなどのその他のシスコ製品のみならず、サードパーティのテクノロジーともうまく連携して、お客様の成果を高めていきます。

さらに、Cisco Secure Access では最新のサイバーセキュリティを適用すると同時に、リスクを根本的に軽減し、複雑な IT 運用を大幅に簡素化することで、エンドユーザーが実行するタスクを最小限に抑えます。

ユーザーにとっての改良点

Cisco Secure Access は、ユーザーエクスペリエンスを劇的に改善して摩擦を取り除き、必要なセキュリティ手順が回避されないようにして生産性を向上させます。このソリューションでは、ユーザーの接続方法を簡素化する統合クライアントを利用します。これにより、ユーザーが認証を行い、目的のアプリケーションに直接接続できるようになります。このような「すべてにアクセス」可能な機能により、最小権限の概念、事前設定済みのセキュリティポリシー、および管理者が制御する適応可能な手段を使用してユーザーが自動的に接続されます。

© 2024 Cisco and/or its affiliates. All rights reserved.

セッションが特定の非標準アプリに ZTNA や VPNaaS を使用するかどうかにかかわらず、ユーザーは追加の手順を実行する必要はありません。また、面倒な検証作業を何度も繰り返すこともありません。これにより、ユーザーの手間が最小化され、異なるリソースに対してどのような方法でアクセスする必要があるか、別のクライアントを起動する必要があるか、異なるサインオンプロセスの規定があるかといった懸念がなくなります。すべてのアプリケーションへ一元的にアクセスできることで、ユーザーの接続プロセスが大幅に簡素化され、ユーザーとデバイスのポスチャ検証などのセキュリティが確保されて生産性が向上します。

IT をより簡単に

今日の IT チームは、大量のセキュリティツールを統合することに苦労し、さまざまな管理コンソールやポリシーエンジンを必要とし、エンドユーザーのデバイスごとに複数のソフトウェアエージェントを展開して管理する必要に迫られています。こうした課題は、各セキュリティのポイント製品から発生するさまざまなレポート、アラート、およびインシデントによってさらに増幅していきます。

Cisco Secure Access は、単一のクラウド管理コンソール、統合クライアント、一元化されたポリシー作成プロセス、および集約されたレポート作成機能によってセキュリティチームと IT チームの運用を簡素化および自動化します。これで、IT チームは個別の製品を多数展開することなく 1 つのツールを管理するだけで済みます。その結果、効率が大幅に向上し、コストの削減およびビジネスの俊敏性の強化をサポートする柔軟な IT 環境が実現します。IT チームは、脅威をより迅速に検出してブロックし、調査を効率よく実施して修復タスクを最小限に抑えながら、手動の集計タスクを減らしてエンドユーザー アクティビティの可視性を向上させることができるようになります。これにより、さまざまな場所から複数の接続先（インターネット、SaaS アプリ、プライベートアプリ）に接続するユーザーまたはグループのきめ細かいコンテキスト認識制御（管理対象デバイスと管理対象外デバイスを含む）が可能になります。

すべてのユーザーにより安全な環境を

Cisco Secure Access は、エンドユーザーとオンプレミスリソースの両方に対して業界をリードするセキュリティの有効性を提供します。多層防御の構造的なアプローチが提供する拡張機能により、さまざまなサイバーセキュリティの脅威から保護します。エンドユーザーは、感染したファイル、悪質な Web サイト、フィッシングやランサムウェアといったスキームなどのリスクから保護されます。IT チームやセキュリティチームは、攻撃対象領域を減らし、最小権限の制御を実施できるほか、ポスチャ検証を有効にして、分散環境でのセキュリティギャップをなくすことができます。

セキュリティチームは、許可されていないシャドー IT の動作や未承認アプリケーションの使用を可視化し、それらのアクティビティをブロックできます。内部リソースをクローキングし、ハッカーから隠すことで、IT チームはセキュリティを強化できます。こうした機能はすべて、Cisco Talos 脅威インテリジェンスの比類のないテレメトリ、広範な調査、高度な AI に支えられ、脅威を特定して阻止し、修復を迅速化しています。リスクを軽減することで、組織は事業継続性を維持し、侵害によるレピュテーションや財務への影響を回避します。

© 2024 Cisco and/or its affiliates. All rights reserved.

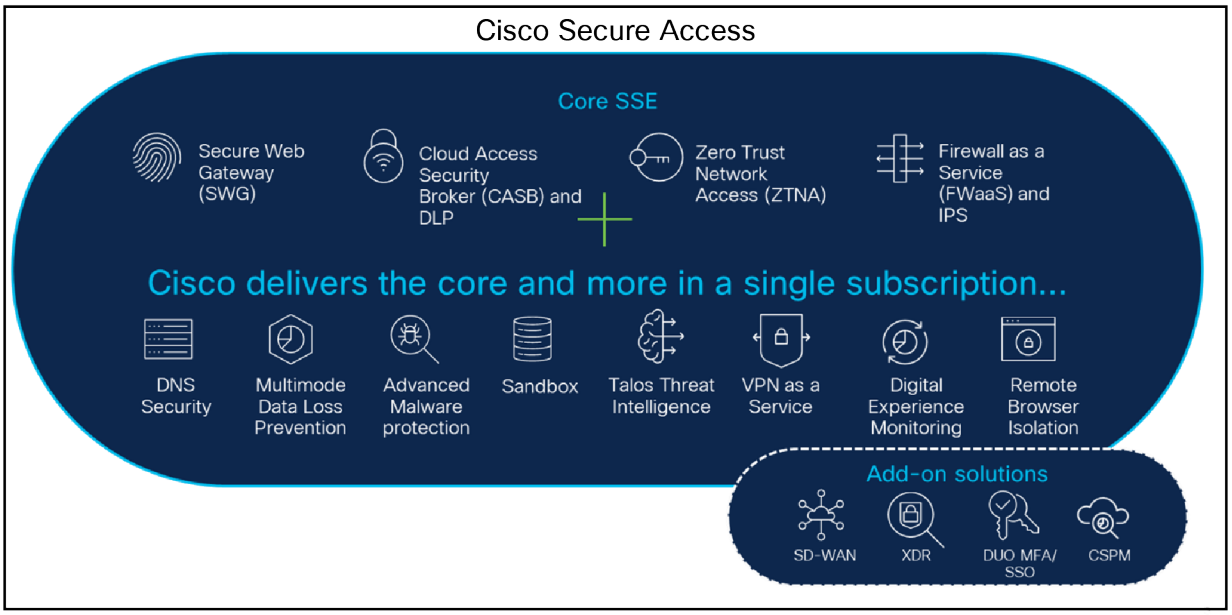

図 1.
コアのセキュリティサービスエッジ（SSE）を超えてビジネスのつながりと保護を強化

機能と利点

表 1. 機能と利点

機能	利点
ゼロトラスト ネットワーク アクセス（ZTNA）	オンプレミスのデータセンターまたはクラウド/IaaS 環境にあるプライベート アプリケーションに対して、きめ細かいアプリ固有のアクセスを提供します。 そのアイデンティティ認識型プロキシ設計では、定義されたアクセス制御ポリシーに基づいて、最小権限の原則とコンテキストに基づくインサイトを活用し、デフォルトでアクセスを細かく拒否します。また、明示的に許可された場合は、場所を問わずアプリケーションへのユーザーアクセスを仲介します。 • 2 つのアクセス方法：クライアントベースおよびクライアントレス ブラウザベースのアクセス。ユーザー、アプリケーションベースのきめ細かいアクセスポリシー、SAML 認証、アイデンティティ プロバイダー（IdP）、およびコンテキストに応じたアクセス制御。 • クライアントベースのアクセスでは、統合された Cisco Secure Client を活用します。 • デバイスのポスチャチェックが実行されると、セッションごとにセキュアなアクセスが確立されます。 • セキュアな暗号化トンネルを介してユーザーを認証し、ユーザーにはアクセス許可を持つアプリケーションとサービスのみが表示されます。 • アプリケーションプロキシは、アプリケーションをインターネットに公開することなく、透過的でセキュアなリモートアクセスを提供します。プライベートアプリに関するネットワークの詳細は、それらのアプリにアクセスするクライアントには表示されません。これにより、攻撃者がクライアントデバイスを侵害した場合でも、攻撃者は IP の偵察による学習ができなくなります。 • 水平移動する攻撃者を阻止します。 • ロケーションおよびデバイス固有のアクセス制御ポリシーを実装し、侵害された可能性のあるデバイスはそのサービスに接続できないようにします。 • 管理者は、請負業者と従業員に対し、アクセスが必要なリソースのみにアクセス権限を割り当てます。水平移動はできません。 • 管理者は、エンドポイントの OS のタイプとバージョン、ブラウザのタイプとバージョン、およびアクセス制御で使用される地理位置情報のポスチャプロファイルを設定できます。 • アクセスが拒否された原因を説明する際に役立つ情報をユーザーに提供し、修復手順を提案します。

© 2024 Cisco and/or its affiliates. All rights reserved.

機能	利点
	• 管理者は、ダッシュボードを使用して、特定のユーザーとデバイスの組み合わせの ZTNA アクセスを取り消すことができます。 • 管理者は、特定のアプリケーションの最大認証間隔を設定することで、特定のアプリケーションに追加のユーザー認証を適用できます。
VPNaaS	すべてのプライベートアプリが ZTNA の対象ではありません。VPNaaS クラウドベースオプションが含まれ、セキュアなリモートアクセスと Web 以外のインターネットトラフィックに対するセキュアなインターネットアクセスを実現します。 • 次のような機能が搭載されています。ユースケースのサポート（スプリットトンネリングとトンネルの完全サポート、ピアツーピアの通信、信頼ネットワーク検出、BYO 証明書、スプリット DNS、ダイナミックスプリット DNS）、複数の認証方法（SAML、証明書、Radius）、ユーザーの使いやすさ（常時 VPN 接続、ログオン前に開始）、IT 運用の簡素化（ローカル IP プール、複数の VPN プロファイル）。 • リモートユーザーが Cisco Secure Client でセキュリティ アクセス ファブリックを介してプライベート アプリケーションにアクセスできるようにします。 • お客様の IdP で SAML 認証を行うことで、ID ベースのアクセス制御を利用できます。 • エンドポイントのポスチャも評価されます。これにより、プライベートリソースに対するきめ細かいアクセス制御が可能になります。 • アプリケーションごとのきめ細かいアクセス制御をサポートします。 • ヘッドエンドまたはトンネルタイプを選択する必要がなく、接続が簡素化されます。 • ユーザーが PC にログインしてパスワードのリセットを実行するときに、VPN トンネルを起動し、オンプレミスの Active Directory に対してシームレスに認証できるようにするために使用される管理トンネルをサポートします。 • 管理トンネルは、デスクトップ管理チームがユーザー VPN ログインなしで PC にソフトウェアアップデートをダウンロードするために使用できます。 • Identity Services Engine（ISE）との統合および RADIUS 認証のサポート。
セキュア Web ゲートウェイ（フルプロキシ）	ポート 80/443 上のすべての Web トラフィックをログに記録して検査し、透過性、制御、および保護を強化します。IPsec トンネル、PAC ファイル、プロキシチェーンを使用してトラフィックを転送し、完全な可視性、URL およびアプリケーションレベルの制御、高度な脅威からの保護を実現します。 • ポリシーやコンプライアンス規制に違反する接続先をブロックするための、カテゴリまたは特定の URL によるコンテンツフィルタリング。 • ダウンロードしたすべてのファイルをスキャンして、マルウェアやその他の脅威を検出します。 • Cisco Secure Malware Analytics を使用したサンドボックス分析により、不明なファイルが分析されます（Cisco Secure Malware Analytics の専用セクションを参照）。 • ファイルタイプごとのブロッキング（例：.exe ファイルのダウンロードのブロック）。 • TLS 通信全体または一部を復号することで、隠蔽された攻撃や対処に時間がかかる感染から保護します。 • 一部のアプリで特定のユーザーアクティビティをブロックするためのきめ細かなアプリ制御（例：Dropbox へのファイルアップロード、Gmail へのファイル添付、Facebook での投稿/共有）。 • 完全な URL アドレス、ネットワーク アイデンティティ、許可またはブロックされたアクション、外部 IP アドレスが含まれた詳細なレポート。 • カスタマイズ可能な制御とトラフィックパスオプションを備えたインターネットベースの SaaS アプリのマルチモード保護。
クラウド アクセス セキュリティ ブローカ（CASB）	生成系 AI アプリケーションを含む使用中のクラウドアプリケーションを検出して報告することで、シャドー IT を特定します。クラウドの利用を適切に管理してリスクを軽減できるようになり、攻撃的、非生産的、高リスク、あるいは不適切なクラウドアプリケーションの使用をブロックできます。ユーザーまたはグループのアクティビティを検出、記録、および制御するマルチモード機能を備えています。 • クラウド内またはアウトバウンド Web トラフィック内の機密企業データが不正なユーザーに漏洩するのをブロックするデータ損失防止（DLP）。（別の「DLP」セクションを参照）。 • ベンダーカテゴリ、アプリケーション名、検出された各アプリケーションのアクティビティ量に関するレポート。 • Web レピュテーションスコア、財務状態、関連するコンプライアンス認定といったアプリの詳細やリスク情報。

© 2024 Cisco and/or its affiliates. All rights reserved.

機能	利点
	• クラウドベースのファイル ストレージ アプリケーションからマルウェアを検出して排除する、クラウドマルウェア検出。 • 特定のクラウドアプリケーションをブロックまたは許可する機能。 • すべてのユーザーまたは特定のグループ/個人がアクセスできる SaaS アプリケーションのインスタンスを制御するためのテナント制限。 • 70 以上の生成 AI アプリケーションの使用状況または使用試行を検出して制御。使用をブロックするか、これらのアプリケーションの使用方法を制御するポリシーを作成して適用します。
データ漏洩防止（DLP）	マルチモードのデータ損失防止。機密データをインラインで分析し、組織外部へ流出する機密データを可視化および制御します。また、API ベースの DLP 機能により、クラウドに保存されているデータのアウトオブバンド分析を提供します。より効率的な管理と規制順守のための統合されたポリシーとレポート機能が含まれています。 • PII、PHI、PCI、およびその他の規制を順守するための 600 以上の組み込み識別子に加えて、HIPAA、PCI、GDPR、および PII の組み込みデータ分類。 • しきい値と近接性を備えたカスタマイズ可能な組み込みのコンテンツ分類機能により、誤検出を調整および低減。 • カスタムフレーズ（プロジェクトコード名など）を追加できるユーザー定義のディクショナリ。 • 機密データの使用状況の検出と報告、および不正使用の特定に役立つドリルダウンレポート。 • AI アプリケーションに DLP ポリシーを割り当てて、ChatGPT などの公開されている AI サービスをより安全に使用できるようにする機能。危険なコンテンツを検出してブロックすることで、IP 損失や IP 汚染から保護します。 • クラウドアプリおよび Web トラフィックのコンテンツの検査とデータポリシーの適用。 • API ベースの機能は、Microsoft 365（SharePoint および OneDrive）、Google Drive、Webex、Box、および Dropbox をサポートします。 • ChatGPT の場合、不正ユーザーへの漏洩を防ぐために、独自のソースコードのアップロードをブロックします。 • ChatGPT から生成されたコンテンツのダウンロードをブロックして、ユーザーが ChatGPT でソースコードを生成し、ダウンロードして組織のコードリポジトリにコミットするのを防ぎます。
サービスとしてのファイアウォール（FWaaS）	すべてのポートとプロトコルでリクエストがあって送信されたインターネットに向かう非 Web トラフィックを可視化し、制御します。モバイルアプリ、ピアツーピアファイル共有、コラボレーション（Webex や ZOOM など）、O365、非 Web トラフィックまたは非 DNS トラフィックが含まれます。 • Security Access の単一の統合ダッシュボードによる展開、管理、レポート。 • カスタマイズ可能なポリシー（IP、ポート、プロトコル、アプリケーション、および IPS ポリシー）。 • レイヤ 3/4 ファイアウォールですべてのアクティビティを記録し、IP、ポート、プロトコルの各ルールを使用して不適切なトラフィックをブロックします。 • スケーラブルなクラウド コンピューティング リソースにより、アプライアンスのキャパシティに関する問題を解消します。 • レイヤ 7 アプリケーションの可視性と制御により、増大する 2,800 超の非 Web アプリケーションを識別し、ブロックするか許可するかを選択します。 • 検査を実施する前にトラフィックを復号します。
侵入防御システム（IPS）	IPS は、ネットワークトラフィックのフローを調査し、SNORT 3 テクノロジーとシグニチャベースの検出による侵入防御のレイヤを追加して脆弱性エクスプロイトを防止します。 • 統合ダッシュボードを使用して、トラフィックを検査するためのポリシーを作成します。さらに、自動アクションを実行し、危険なパケットがネットワークに到達する前に補足して排除します。 • インターネットトラフィックとプライベートトラフィックの両方に IPS による保護を提供します。 • トラフィックの宛先に応じて、さまざまなカスタムプロファイルに対応するアクセスポリシーとオプションを設定します。 • 40,000 を超え、なお拡大を続ける Cisco Talos の膨大なシグニチャを使用します。 • シグニチャは、事前定義されたテンプレートで利用できます。 • 脆弱性の悪用を検出し、ブロックします。

© 2024 Cisco and/or its affiliates. All rights reserved.

機能	利点
Cisco Secure Malware Analytics	高度なサンドボックス分析と脅威インテリジェンスを組み合わせて 1 つの統合ソリューションを提供し、マルウェアから組織を保護します。Cisco Secure Malware Analytics コンソールへのフルアクセスを提供し、Glovebox での悪意のあるファイルの実行、ファイル実行アクションの追跡、およびファイルで生成されたネットワークアクティビティのキャプチャを Investigate と組み合わせると、セキュリティアナリストはさらに踏み込んで悪意のあるドメイン、IP、ファイルのアクションにマッピングされた ASN を検出し、攻撃者のインフラストラクチャ、戦術、およびテクニックの最も包括的なビューを取得できます。 • 隠蔽された攻撃方法を検出し、悪意のあるファイルについて報告する機能。 • セキュリティデータを強化するために XDR と一般的に使用される SIEM を統合する API。 • ファイルの性質が変更された場合（当初は良好だったが、後に悪意があると見なされた場合など）のレトロスペクティブな通知。
リモートブラウザ分離（RBI）	RBI は、ブラウザベースの脅威からユーザーと組織を保護します。これは、インターネットの脅威から保護するために、ユーザーによるブラウジングアクティビティの実行を遠隔にあるクラウドベースの仮想化ブラウザインスタンスに移行したものです。Web サイトコードは個別に実行され、安全なビジュアルストリームのみがユーザーに配信されます。RBI は、エンドユーザーに対して完全に透過的な機能です。まだ検出されていないマルウェアについても心配する必要はありません。 • ユーザーデバイスとブラウザベースの脅威との間にある Web トラフィックの隔離。 • ゼロデイ脅威からの保護。 • さまざまなリスクプロファイルの詳細な制御。 • 既存のブラウザ設定を変更せずに迅速に展開。 • オンデマンドの拡張性で追加のユーザーを簡単に保護。 • 既知の危険なインターネットサイトにアクセスする必要がある従業員を保護します。ブロッキングによって生産性が低下することはなく、ユーザーの安全性が維持されます。
DNS レイヤセキュリティ	DNS レイヤでフィルタリングを適用し、接続が確立される前に悪意のある不適切な宛先への要求をブロックします。脅威がネットワークやエンドポイントに到達する前に、ポートまたはプロトコル上の脅威をブロックします。 • すべてのネットワークデバイス、オフィスの場所、およびローミングユーザーのインターネットアクセスを保護します。 • セキュリティ脅威や Web コンテンツの種類、および実行されたアクションごとに DNS アクティビティに関する詳細なレポートを提供します。 • すべてのアクティビティのログを保持します。 • 数千におよぶ場所やユーザーへの展開を加速して、 • 迅速な保護を提供します。
Talos 脅威インテリジェンス	Talos は、最先端のセキュリティ研究を行う世界最大規模のリーディングプロバイダーであり、毎日数千億もの DNS 要求やその他のテレメトリデータを分析しています。この大規模なデータベースに対して AI、統計モデル、および機械学習モデルを継続的に実行し、サイバー脅威に関するインサイトを提供してインシデント対応率を向上させます。 • 攻撃に使用される前に、悪意のあるドメイン、IP、マルウェア、および URL を検出します。 • インシデント調査の優先順位付けを行います。 • インシデント調査を迅速に行い、対応します。 • 攻撃者のインフラストラクチャを特定してマッピングすることにより、将来の攻撃の発生源を予測します。
クラウドマルウェアの検出	クラウドベースのファイル ストレージ アプリケーションからマルウェアを検出して削除します。悪意のあるファイルをエンドポイントに到達する前に検出して修復することにより、セキュリティ保護を強化します。 • セキュリティ管理者の有効性と効率の向上 -- 有効化されると、クラウドベースのサービス内にあるすべてのファイルがハッシュ化され、マルウェアのスキャンを行うために自動的に送信されます。マルウェアを含むファイルにはフラグが付けられるため、セキュリティ管理者は検疫や削除などの修復処理を実行できます。 • Box、Dropbox、Webex、Microsoft 365、Google Drive をサポートします。

© 2024 Cisco and/or its affiliates. All rights reserved.

機能	利点
単一の管理およびレポートコンソール	インテントベースのルールなどの統合されたセキュリティポリシーの作成、およびインターネット、パブリック SaaS アプリ、プライベートアプリへのアクセス管理。広範なロギングや、エンタープライズ SOC へのログのエクスポート機能などを提供します。 • あらゆるユーザーのあらゆるアプリに対するポリシーを一元的に定義。セキュリティポリシーの構築プロセスを簡素化し、組織全体でポリシー定義の一貫性を促進します。 • 統合されたソース（ユーザー、デバイス）と統合されたリソース（アプリケーション、接続先）により、アタッチポイントやアクセスするアプリに関係なく、セキュリティポリシーがユーザーに対応するようになります。 • 進行中のポリシー管理アクティビティを削減します。 • 集約されたレポート作成機能により、可視化と検出までの時間が改善されます。 • SOC/セキュリティアナリストの調査プロセス全体を簡素化します。
AI Assistant*	Secure Access AI Assistant は、英語の会話フレーズを特定のセキュリティポリシーに自動的に変換します。 • セキュリティ管理者は、時間を節約し、業務効率を向上させ、複雑さを軽減できます。 • 複数のユーザーがいる管理者グループは、より一貫性のある効果的なポリシーセットを作成できます。 • 大規模なポリシーセットを作成する必要がある場合は、コスト削減とリソース節約を拡大できます。
リソースコネクタ	リソースコネクタによって、プライベート アプリケーションへの安全な接続を設定するための管理タスクを簡素化します。これらの軽量コネクタは、オンプレミスのデータセンターにあるかクラウドにあるかに関係なく、Cisco Secure Access とプライベートアプリケーション間の接続を管理します。現在、リソースコネクタは AWS および VMWare 環境のみをサポートしています。 • デバイスおよびファイアウォールルールの変更に関するネットワークチームへの依存を軽減します。 • ダイナミックルーティングの設定やサブネットの重複といったルーティングの複雑さを解消します。 • 合併などのシナリオでは、重複する IP でネットワークが異なる状況が多く見られます。トンネルを使用すると複雑になるため、アプリケーションコネクタによってこの複雑な状況を解消します。 • プライベートアプリの場所（IP アドレス）を非表示にし、セキュリティアクセス内のゼロトラストポリシーを介した接続のみを許可することで、プライベートアプリを保護します。 • リソースとネットワークを分離することで、ラテラルムーブメントを防止します。
エクスペリエンスに関するインサイト：デジタル エクスペリエンス モニタリング（DEM）	ユーザーがリソースにアクセスするときに、エンドポイント、アプリケーション、およびネットワーク接続の正常性とパフォーマンスをモニターします。ユーザーのエンドツーエンドのエクスペリエンスの詳細を自動的にマイニングすることでユーザーの生産性を最適化し、障害対応を簡素化し、インシデントの解決時間を短縮し、IT/セキュリティスタッフが問題を迅速に解決できるようにします。 主なインサイトの例： • エンドポイントのパフォーマンス：CPU レベル、メモリ使用率、および Wi-Fi 信号強度。 • ネットワークパフォーマンス：エンドポイントからSecure Accessでのラストマイルのパスの可視化とパフォーマンス。 • Outlook、Slack、Salesforce、SharePoint など、最も一般的に使用されている（上位 20）SaaS アプリケーション。 • ユーザー固有のセキュリティイベント。 • Webex、Zoom、Microsoft Teams などのさまざまなアプリケーションのコラボレーション アプリケーションのパフォーマンスとユーザー体験のスコア。 • 管理者が効率的に問題をトラブルシューティングできるように、スループット、遅延、改善策の提案などのメトリクスを使用して、セグメントごとに問題を解決します。 • ネットワーク接続パケット損失を分離します。

© 2024 Cisco and/or its affiliates. All rights reserved.

機能	利点
モバイルデバイスの ZTA サポート*	Apple iOS デバイスからの非常に効率的なゼロトラストアクセス（ZTA）をサポートします。Apple とシスコは、パフォーマンスとセキュリティの利点を備えた独自の ZTA プロセスを共同で作成しました。 • Secure Access は、効率的な登録、設定、および障害対応を提供します。 • iOS デバイスで完全なクライアントを導入および管理する必要がなく、展開が簡素化されます。 • iOS オペレーティングシステム内の組み込み機能を活用します。 • QUIC および MASQUE プロトコルを使用してトランジットを高速化し、VPP アクセラレーションを使用してスループットを向上させます。 • 高速で安全なアクセスを実現するために、単一レイヤの暗号化を備えた Apple の iCloud プライベートリレーを活用します。 • デスクトップと同じモバイル ZTA 登録エクスペリエンス。 • 管理者は、接続されている iOS デバイスの詳細を表示できます。 Samsung Galaxy デバイスで ZTA 機能をサポートします。 • Secure Access は、ZTA 登録、設定、障害対応、トラフィックステアリングを提供します。 • QUIC および MASQUE プロトコルを使用してトランジットを高速化し、VPP アクセラレーションを使用してスループットを向上させます。 • デスクトップと同じモバイル ZTA 登録エクスペリエンス。 • 障害対応においては、ユーザーはクライアントから使用可能なログをエクスポートし、ヘルプデスクと対話するときにこれらのログを使用できます。
インターネット/SaaS アプリケーションにアクセスする Catalyst SD-WAN ブランチユーザー	Catalyst SD-WAN と Secure Access の統合と自動化により、Cisco Secure Access を介してブランチユーザーから Web および SaaS アプリケーションへのトラフィックステアリングが可能になります。 • Secure Access のマルチレイヤ セキュリティ ソリューションによる脅威からの保護の強化 • ユーザーがローミング場所とオンプレミスの場所の間を移動するときのエクスペリエンスの一貫性が向上します。 • Secure Access の一元化されたポリシー管理、容易な拡張/縮小性、およびキャパシティの制約からの解放により、IT/セキュリティ運用を簡素化します。
Identity Services Engine（ISE）統合	これは ISE と Secure Access の統合の最初のインスタンス化であり、詳細なアイデンティティベースの情報を提供し、ユーザーが何を、いつ、どのように行っているかをより詳細に可視化できます。この統合により、VPNaaS トラフィックのポリシー制御と適用が強化され、次のことが可能になります。 • 適切なユーザーまたはデバイスに対して、適切なポリシーを適切なタイミングでより正確に適用できます。 • AI 分析を提供してデバイスポスチャ/アイデンティティの異常を検出し、正しいポリシーを自動的に適用します。 • ISE を使用した認証要求の RADIUS のサポート • シスコは今後、製品や機能全体で共通のアイデンティティを実現することを目指しています。これは、ユーザーが仕事をする場所、接続方法（有線またはワイヤレス）、アクセスするリソースに関係なく適用されます。

*まもなく一般提供を開始

© 2024 Cisco and/or its affiliates. All rights reserved.

パッケージオプション

Cisco Secure Access は Cisco Umbrella SIG を進化させたものであり、単一のサブスクリプションで提供されるシスコの最も広範な SSE ソリューションです。すべてのユーザーに対してより高いレベルのセキュリティを実現する一方で、IT とエンドユーザーの両方の生産性を向上させます。Cisco Secure Access は、お客様が組織のニーズに合わせて適切なレベルの保護と対象範囲を簡単に選択できるようにパッケージで提供されます。現在、Cisco Secure Access Essentials と Cisco Secure Access Advantage の 2 つのパッケージがあります。

表 2. コア製品パッケージ

カテゴリ	機能	Cisco Secure Access Essentials	Cisco Secure Access Advantage
Secure Access	Secure Internet Access（SIA） • SD-WAN DIA の統合 • Secure Client（ライセンス込み） ◦ ローミングセキュリティ（DNS、Web、および Firewall-as-a-Service）	✔	✔
	Secure Private Access（SPA） • Secure Client（ライセンス込み） ◦ ZTNA クライアント ◦ VPN-as-a-Service • ZTNA クライアントレス	✔	✔
基本的なセキュリティ	DNS の保護	✔	✔
	Web アプリおよびプライベートアプリのレイヤ 3 およびレイヤ 4 制御向け Firewall-as-a-Service	✔	✔
	セキュア Web ゲートウェイ（プロキシ Web トラフィック、URL フィルタリング、コンテンツフィルタリング、高度なアプリ制御）	✔	✔
	CASB - クラウドアプリの検出、リスクスコアリング、ブロッキング、クラウドマルウェアの検出、テナント制御	✔	✔
	リモートブラウザ分離（リスクの高いトラフィック専用のライセンス*）	✔	✔
	Cisco Secure Malware Analytics（サンドボックス）	限定的	限定的

© 2024 Cisco and/or its affiliates. All rights reserved.

カテゴリ	機能	Cisco Secure Access Essentials	Cisco Secure Access Advantage
デジタル エクスペリエンス モニタリング	Experience Insights	✔	✔
高度なセキュリティ	レイヤ 7 Firewall-as-a-Service		✔
	IPS による保護		✔
	生成 AI/ChatGPT 制御を含む Web アプリケーションのデータ損失防止（DLP）		✔
	リモートブラウザ分離（すべて**）		✔
ソフトウェア サポート	24 時間 365 日、電子メールと電話による Cisco Software Support-Enhanced のサポート（オプションで Software Support-Premium にアップグレード可能）	✔	✔

*高リスク：未分類の Web サイトやセキュリティ分野を隔離します（損害が発生する可能性があるものも含む）。

**すべて：コンテンツ分野やセキュリティ分野、接続先リスト、アプリケーション、未分類など、選択した宛先をすべて隔離します。

Cisco Secure Access：ソフトウェア サポート サービス

Cisco Secure Access 製品の購入には、Software Support-Enhanced 用の個別の SKU と、Software Support-Premium へのアップグレードオプションが必要です。

Cisco Software Support Enhanced

- テクニカルサポート（Cisco Cloud Security Support への 24 時間 365 日のアクセス：電話/オンライン）。
- ソフトウェアアップデート。
- ソフトウェアの専門知識を持つ主要な連絡窓口。
- 技術的なオンボーディングと導入支援。

Cisco Software Support Premium（オプションのアップグレード）

Enhanced レベルの機能に加えて、以下が含まれます。

- Enhanced サポートよりも優先的にケースを処理。
- セキュリティソフトウェアの導入と継続的な管理・最適化を成功させるために、インシデント管理、プロアクティブなコンサルティングや提案を行う専門家をアサイン。
- サポートケース分析。

セキュリティソフトウェアに関するシスコのサポートサービスの詳細については、こちらをクリックしてご確認ください。

© 2024 Cisco and/or its affiliates. All rights reserved.

詳細情報

詳細については、Cisco Secure Access をご覧ください。

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。

Cisco および Cisco ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、www.cisco.com/jp/go/trademarks をご覧ください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」または「partner」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。(1110R)

Printed in USA 02/24

© 2024 Cisco and/or its affiliates. All rights reserved.