Cisco Umbrella パッケージ比較

Cisco Umbrella は、お客様のネットワーク、ブランチオフィス、ローミングユーザーからクラウドアプリケーションへのアクセスを制御し、安全なインターネットアクセスを確立します。ばらばらのセキュリティツールとは異なり、Umbrella は、セキュア Web ゲートウェイ、クラウド アクセス セキュリティ ブローカ、DNS レイヤセキュリティ、クラウド型ファイアウォール、データ損失防止機能、マルウェア防御サンドボックス分析機能、リモートブラウザ分離機能を、単一のクラウドサービスに統合しています。インターネットへのセキュアなインターフェイスとして機能し、詳細なインスペクション機能と制御機能を備え、コンプライアンスに対応して、効果的に脅威を防御します。世界最大クラスの脅威インテリジェンスチームである Cisco Talos と連携し、調査力と対応力を向上させるために、脅威情報を公開しています。これらすべてをクラウドで提供することで、ユーザーがどこにいても可視化してポリシーを適用し、保護できます。

	DNS Essentials	DNS Advantage	SIG Essentials	SIG Advantage
	企業全体の DNS レイヤで、遅延を増やすことなく脅威を数分でブロック	DNS 保護に加えて、Web セキュリティと脅威に関するインサイトによって、調査時間を短縮	高度なセキュリティ機能を備え、業界でトップクラスの効果的なセキュリティで管理をシンプル化	IPS、DLP などを備えたレイヤ 7 ファイアウォールなどの高度なセキュリティ機能により、最高レベルの保護と制御を実現
ライセンス	対象ユーザー数単位	対象ユーザー数単位	対象ユーザー数単位	対象ユーザー数単位
セキュリティ/制御				
DNS レイヤセキュリティ				
マルウェア、フィッシング、ボットネットなどのリスクの高いドメインをブロック	●	●	●	●
Cisco SecureX からドメインをブロック、直接統合 (Splunk、Anomali など) 、Enforcement API を利用したカスタムリスト	●	●	●	●
セキュア Web ゲートウェイ (SWG)				
プロキシを利用して Web トラフィックを検査		危険なドメインに関連するトラフィックを検査 (選択的プロキシを利用)	すべての Web トラフィック	すべての Web トラフィック
SSL (HTTPS) トラフィックの復号と検査		選択的プロキシを利用	●	●
Web フィルタリングの有効化	ドメインまたはドメインカテゴリ別	ドメインまたはドメインカテゴリ別	ドメイン、URL、またはカテゴリ別	ドメイン、URL、またはカテゴリ別
カスタムブロックリスト/許可リストを作成	ドメインが対象	ドメインが対象	URL が対象	URL が対象
Cisco Talos やその他のフィードに基づいて URL をブロック、AV エンジンやマルウェア防御機能に基づいてファイルをブロック		選択的プロキシを利用	●	●
不審なファイルに対してマルウェア分析 (サンドボックス) を適用			500 サンプル/日	サンプル数無制限
レトロスペクティブ セキュリティを利用して、悪意のあるファイルに変わったファイルを特定			●	●

	DNS Essentials	DNS Advantage	SIG Essentials	SIG Advantage
セキュリティ/制御				
リモートブラウザ分離 (RBI)				
リスクの高いサイトを分離して安全なアクセスを実現			リスクの高いサイトを分離するオプションのアドオン	リスクの高いサイトを分離するオプションのアドオン
リスクの高い Web アプリを分離して安全なアクセスを実現			Web アプリを分離するオプションのアドオン	Web アプリを分離するオプションのアドオン
任意の Web サイトを分離して安全なアクセスを実現			任意の Web サイトを分離するオプションのアドオン	任意の Web サイトを分離するオプションのアドオン
ファイアウォール				
レイヤ 3/レイヤ 4 ポリシーを作成して、特定の IP、ポート、プロトコルをブロック			●	●
侵入防御システム (IPS) とレイヤ 7 アプリケーションポリシーを利用して、アウトバウンドトラフィックの保護を強化			オプションのアドオン	●
IPsec トンネル終端対応			●	●
データ損失防止 (DLP)				
Web アプリおよびクラウドアプリのトラフィックに対して、機密データに関するインラインインスペクションを実施			オプションのアドオン	●
クラウド アクセス セキュリティ ブローカ (CASB)				
アプリケーション検出レポートに基づいてシャドー IT を検出しブロック	ドメイン別	ドメイン別	URL 別	URL 別
特定のアプリケーションに対するきめ細かいポリシーの作成と適用 (アップロードや添付ファイル、投稿のブロックなど)			●	●
クラウドベースのファイルストレージアプリからマルウェアをスキャンして削除			2 つのアプリケーション	サポート対象のすべてのアプリケーション

	DNS Essentials	DNS Advantage	SIG Essentials	SIG Advantage
セキュリティ/制御				
Umbrella Investigate				
Investigate の Web コンソールにアクセスし、脅威インテリジェンスをインタラクティブに利用		●	●	●
Investigate のオンデマンド Enrichment API を利用して、ドメイン、URL、IP、ファイルに関する情報を他のシステムに提供 (2,000 リクエスト/日) [1]		●	●	●
SecureX と統合して、シスコ製品全体のアクティビティを集約	Reporting および Enforcement API	すべての API	すべての API	すべての API
Secure Malware Analytics				
悪意あるドメイン、IP、ASN、ファイルを検出し、インシデント対応を迅速化				●
トラフィック転送				
以下を目的とした外部 DNS トラフィックの転送 • シスコ製品 (SD-WAN、Meraki、ISR、WLAN) およびサードパーティ製品 (Cradlepoint、Aerohive など) の統合によるネットワーク内での保護 • Umbrella ローミングクライアントまたは Cisco Security Connector iOS アプリを利用したネットワーク外での保護	●	●	●	●
Umbrella モジュールを導入してトラフィックを転送するための Cisco AnyConnect クライアント (ライセンス含む)	●	●	●	●
IPsec トンネル、Cisco Secure VPN (AnyConnect) 、プロキシチェーン、PAC ファイルを利用してアウトバウンド ネットワーク トラフィックを送信	●	●	●	●

	DNS Essentials	DNS Advantage	SIG Essentials	SIG Advantage
セキュリティ/制御				
ユーザーアトリビューション				
ネットワーク（出力 IP）、内部サブネット[2]、ネットワークデバイス（VLAN および SSID 含む）[3]、ローミングデバイス、Active Directory グループ（特定のユーザー含む）[4]ごとにポリシーを作成し、レポートを確認	●	●	●	●
ポリシーを作成し、SAML を使用してレポートを表示			●	●
管理				
カスタマイズ可能なブロックページとバイパスオプション	●	●	●	●
Multi-Org Console を使用して、分散した組織を一元管理	●	●	●	●
シスコの Management API を利用して、子組織の ID を作成、読み取り、更新、削除	●	●	●	●
レポートおよびログ				
リアルタイムのアクティビティ検索および Reporting API を活用して、重要なイベントを簡単に抽出	●	●	●	●
ログ保管先を北米またはヨーロッパから選択	●	●	●	●
お客様が管理する AWS S3 バケットを使用して必要な期間だけログを保持およびエクスポート可能、またはシスコが管理する S3 バケットを使用してログ保持期間を延長可能[5]	●	●	●	●
アクセスログ	ドメイン対象（詳細：30 日、サマリー：1 年）	ドメイン対象（詳細：30 日、サマリー：1 年）	ドメイン、URL、ファイアウォール対象（詳細：30 日）	ドメイン、URL、ファイアウォール対象（詳細：30 日）

	DNS Essentials	DNS Advantage	SIG Essentials	SIG Advantage
セキュリティ/制御				
サポート				
Enhanced - 24 時間 365 日のテクニカルサポート + オンボーディングサポート	必須	必須	必須	必須
Premium - 24 時間 365 日のテクニカルサポート + オンボーディングサポート + テクニカル アカウント マネージャ (TAM)	オプションのアドオン	オプションのアドオン	オプションのアドオン	オプションのアドオン

1. MSSP は以下を購入 (および利用) できます。
   Investigate Console (アナリストごとのライセンス)
   Investigate Integration API (アナリストごとのライセンス)
   MSSP は Investigate API Tier 1、2、3 を購入できません。
   エンドカスタマーは以下を購入できます。
   Investigate Console (アナリストごとのライセンス)
   Investigate Integration API (アナリストごとのライセンス)
   Investigate API (Tier 1、2、3。サイトごとのライセンス)
2. 内部 IP によるアトリビューションには、ネットワークフットプリント (シスコの仮想アプライアンス。Professional パッケージでは利用不可) または、Meraki MR、Cisco ISR、Cisco ASA のいずれかとの統合が必要。
3. Cisco Integrated Services Router (ISR; サービス統合型ルータ) またはシスコ ワイヤレス LAN コントローラとネットワークデバイスの統合が必要。
4. Active Directory (AD) のポリシーとアトリビューションには、Umbrella AD コネクタとネットワークフットプリント (Umbrella 仮想アプライアンス) またはエンドポイント フットプリント (Umbrella ローミングクライアントまたは AnyConnect ローミングモジュール) が必要
5. シスコが管理する S3 バケットを使用する場合、Amazon アカウントは不要