Umbrella パッケージ比較表

ライセンス	DNS Security Essentials	DNS Security Advantage	SIG Essentials	SIG Advantage
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高リスクのドメインをブロック	○	○	○	○
エンフォースメント API を使用し、Cisco SecureX、ダイレクトインテグレーション（Splunk、Anomaliなど）、およびカスタムリストからのドメインをブロック	○	○	○	○
DNSをバイパスするC2コールバックのdirect-to-IPトラフィックをブロック *1	—	○	○	○
セキュア ウェブ ゲートウェイ (SWG)				
プロキシを介した通信のインスペクション	—	セレクティブ プロキシ時	全てのウェブ通信	全てのウェブ通信
SSL (HTTPS) トラフィックの復号	—	セレクティブ プロキシ時	○	○
ウェブ フィルタリング	ドメイン、ドメイン カテゴリ	ドメイン、ドメイン カテゴリ	ドメイン、URL、URL カテゴリ	ドメイン、URL、URL カテゴリ
カスタム ブロック / 許可リスト	ドメイン	ドメイン	ドメイン、URL	ドメイン、URL
Cisco Talos などのフィードに基づく URL のブロック、AV Engine やマルウェア防御に基づくファイルのブロック	—	セレクティブ プロキシ時	○	○
疑わしいファイルに対するサンドボックス解析	—	—	500 サンプル/日	無制限
遡及的なセキュリティにより、後からファイルが悪意あるものと判定されたことを特定	—	—	○	○
リモート ブラウザ アイソレーション (RBI)				
疑わしいサイトに対する安全なアクセスの提供	—	—	Isolate Risky オプション	Isolate Risky オプション
ウェブ アプリケーションに対する安全なアクセスの提供	—	—	Isolate Web Apps オプション	Isolate Web Apps オプション
任意の宛先に対する安全なアクセスの提供	—	—	Isolate Any オプション	Isolate Any オプション
ファイアウォール				
特定のIP、ポート、プロトコルをブロックするレイヤ 3/ レイヤ 4 ポリシーの作成	—	—	○	○
アプリケーション レイヤ 7 のポリシーと侵入防止システム (IPS) を用いたアウトバウンド通信保護の強化	—	—	オプション	○
IPsec を利用した接続の終端	—	—	○	○
Data Loss Prevention (DLP)				
Web やクラウドアプリのトラフィックをインラインで検査し、機密データを検出	—	—	オプション	○
Cloud access security broker (CASB)				
App Discovery レポートによるシャドー IT の発見とブロック	ドメイン	ドメイン	URL	URL
より詳細な制御が可能なポリシー （ アップロード、添付ファイル、投稿をブロック ） の作成	—	—	○	○
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除去	—	—	2 つまでのアプリケーション	サポート済み全アプリケーション
Umbrella Investigate				
Investigateのウェブコンソールにアクセスし、インタラクティブな脅威情報を入手	—	○	○	○
Investigate のオンデマンドエンリッチメント API を使用し、ドメイン、URL、IP、ファイル情報を他のシステムに送信 （2,000リクエスト / 日） *2	—	○	○	○
SecureX と統合し、シスコ製品全体のアクティビティを集約	レポーティング / エンフォースメント API	全ての API	全ての API	全ての API
セキュア マルウェア アナリティクス (サンドボックス)				
インシデントレスポンスの迅速化 (悪意のあるドメイン、IP、ASN、ファイルの発見)	—	—	—	○
ユーザ属性				
ネットワーク（出口 IP）、内部サブネット *3、ネットワークデバイス （VLAN と SSIDを含む） *4、ローミングデバイス、Active Directoryグループ（特定のユーザーを含む） *5 ごとにポリシーを作成し、レポートを表示	○	○	○	○
SAML ベースのポリシー作成とレポーティング	—	—	○	○
マネジメント				
ブロックページのカスタマイズとバイパス オプション	○	○	○	○
マルチ テナント (Multi-Org)	○ (無償オプション)	○ (無償オプション)	○ (無償オプション)	○ (無償オプション)
レポーティグとログ				
リアルタイムのアクティビティ検索とレポーティング API を活用し重要なイベントを簡単に抽出	○	○	○	○
北米またはヨーロッパのログ ストレージ	○	○	○	○
お客様のAWSのS3バケットを使用して、必要な期間だけログをエクスポートして保持または、シスコが管理するS3バケットを利用して最大30日間のログを保持 *6	○	○	○	○
アクセスログ	ドメイン (30 日間 (詳細), 1 年間 (概要))		ドメイン， URL, ファイアウォール (30 日間 (詳細))	
サポート				
Enhanced (24x7 テクニカル サポート および オンボーディング支援)	必須	必須	必須	必須
Premium (Enhanced に加え、テクニカル アカウント マネージャ (TAM))	オプション	オプション	オプション	オプション

注釈事項

*1. エンドポイント エージェントが必要 (Umbrella roaming client, Chromebook client, or AnyConnect roaming module)
*2. MSSPs can purchase (and use):
Investigate Console (licensed per analyst)
Investigate Integration API (licensed per analyst)
MSSPs cannot purchase the Investigate API Tier 1, 2, or 3
End customers can purchase
Investigate Console (licensed per analyst)
Investigate Integration API (licensed per analyst)
Investigate API (Tier 1, 2, 3) (licensed per site)
3. 内部 IP アトリビューションには、ネットワークフットプリント（当社の仮想アプライアンス）、Meraki MX との統合、 Cisco ISR との統合、または Cisco ASA との統合が必要
4. Cisco Integrated Services Router（ISR）またはCisco Wireless LAN Controllerとのネットワーク機器の統合が必要
5. Active Directory (AD)のポリシーとアトリビューションには、Umbrella AD コネクタに加え、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
6. 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

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10:00-12:00, 13:00-17:00
0120-092-255

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

©2021 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems, およびCisco Systems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一定の国における商標登録または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(1502R) この資料の記載内容は2021年7月現在のものです。この資料に記載された仕様は予告なく変更する場合があります。

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
http://www.cisco.com/jp