Cisco Secure Workload プラットフォーム

2024 年 4 月

目次

Cisco Secure Workload（旧称 Tetration）は、単一のコンソールから、あらゆる場所、あらゆるインフラストラクチャ、そしてあらゆるフォームファクタのワークロードに対して、ゼロトラストのマイクロセグメンテーションをシームレスに提供します。すべてのワークロードのやり取りを包括的に可視化し、強力な AI/ML を活用したポリシーライフサイクルの自動化を実現することで、攻撃対象領域を縮小し、ラテラルムーブメントを防止し、ワークロードの動作の異常を特定し、脅威を迅速に修復し、コンプライアンスを継続的に監視します。

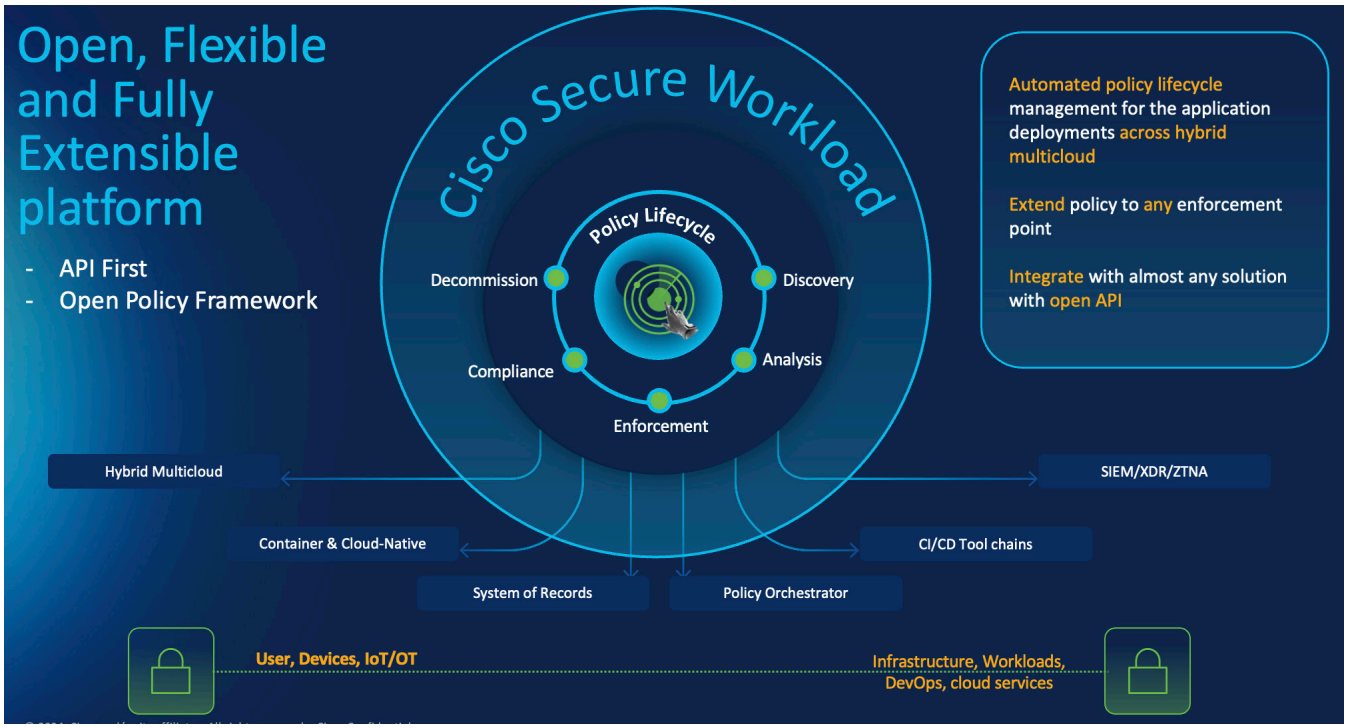
製品の概要

従来の IT には、インフラストラクチャを中心とする考え方がありました。最も重要なデータがデータセンターに格納されていたため、適正なトラフィックを受け入れ、悪意のある攻撃者を排除することが私たちの仕事でした。そしてシスコでは、ファイアウォールをツールとして選択していました。

今日の組織では、アプリケーションを中心とした考え方へとシフトしています。アプリケーションは、お客様との関わり方、業務の遂行方法、および収益を得る手段として不可欠なものになっています。しかし、こうしたアプリケーションにおいては、その絶え間ない増加と動的な性質により、IT プロフェッショナルにとって前例のないセキュリティ上の課題が浮き彫りになっています。

アプリケーションは、クラウドとクラウド ネイティブ テクノロジーの活用によって進化を遂げ、オンプレミスとクラウドの両方、または複数のクラウドに分散されています。重要なワークロードは一時的（エフェメラル）なものとなり、データセンター内に整然と保管され、境界ファイアウォールで保護される時代は終わりました。ある意味、もはやはっきりとした境界はないのです。このアプリケーション中心の世界に対応するには、すべてのワークロードを取り囲む「新しいファイアウォールまたはマイクロ境界」を使用してアプリケーションに対するセキュリティを強化するセキュリティソリューションが必要です。これにより、お客様の重要なアプリケーションとデータを保護できるようになります。

Cisco Secure Workload を使用すると、インフラストラクチャ全体にわたって一貫したワークロードレベルのマイクロ境界を作成し、ベアメタルサーバー、仮想マシン、またはコンテナのどこに導入されていてもアプリケーションを保護できます。



Cisco Secure Workload のユースケース トップ 5

Cisco Secure Workload によって、ゼロトラストのマイクロセグメンテーションを提供してアプリケーションを保護し、リスクを軽減し、コンプライアンスを遵守できます。以下は、Cisco Secure Workload のユースケースの上位 5 つです。

- SDN とマルチクラウドの導入：アプリケーションの通信パターンと依存関係の包括的な分析から自動的に生成されるマイクロセグメンテーション ポリシーにより、SDN とマルチクラウド環境の安全な導入を支援します。ロールベース アクセス コントロール（RBAC）による複数のユーザーグループの包括的な制御をもたらす、階層型ポリシーモデルを使用した動的な属性ベースのポリシー定義により、マルチクラウド環境のセキュリティ態勢を強化します。
- ラテラルムーブメントの抑制：高度で持続的な脅威は、ラテラルムーブメントを利用してワークロードにエクスプロイトを拡散するため、影響範囲が拡大します。セキュアワークロードのホワイトリスト ポリシー アプローチと変則的挙動を検出する機能により、ワークロードが悪意のあるラテラルムーブメントから保護され、影響範囲が縮小します。
- 攻撃対象領域の縮小：Cisco Secure Workload は、ネットワークトラフィックだけでなく、インストールされているパッケージや関連する脆弱性、ワークロード上のオープンポートや未使用のポートも可視化します。MITRE att@ck フレームワーク（TTP）に基づいて異常を検出するポリシーと、脆弱性スコアに基づいてポリシーを構成する機能が組み込まれているため、攻撃対象領域が大幅に減少します。
- コンプライアンス：Cisco Secure Workload での階層型のポリシーの継承により、InfoSec および企業全体のコンプライアンスポリシーの展開が簡素化されます。ほぼリアルタイムでポリシーコンプライアンスをモニタリングし、ポリシー違反または潜在的な侵害を特定して警告します。

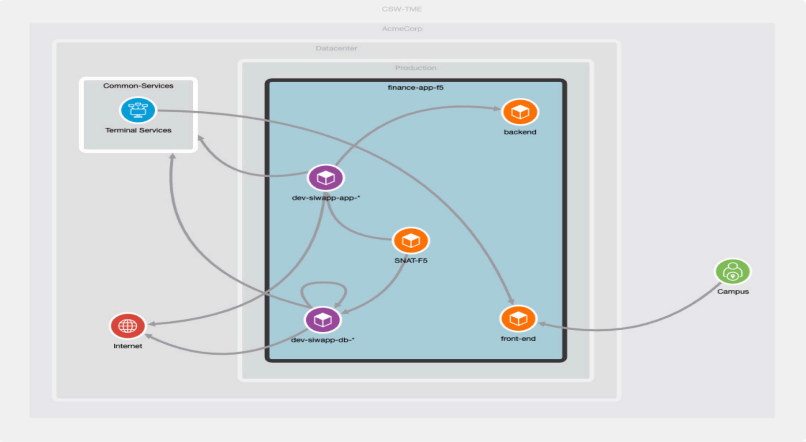
- セキュアな一時（エフェメラル）ワークロード：ワークロードのフォームファクタをよりダイナミックな短期コンテナに変更してスケールアップやスケールダウンの要件に適応し、クラウドネイティブとマイクロサービスアーキテクチャに移行することでワークロードをモダナイズします。こうしたエフェメラルワークロードをセキュリティで保護することは困難です。Cisco Secure Workload なら、あらゆるコンテナ環境で同じ水準の可視性と適用機能が実現します。

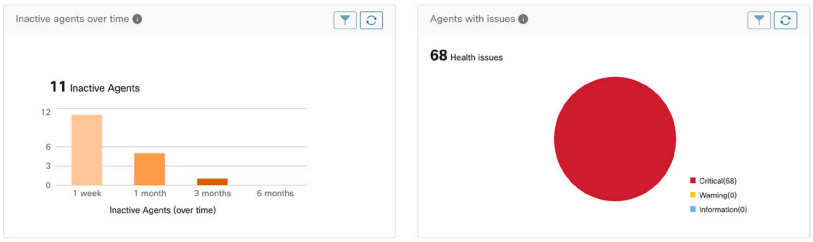
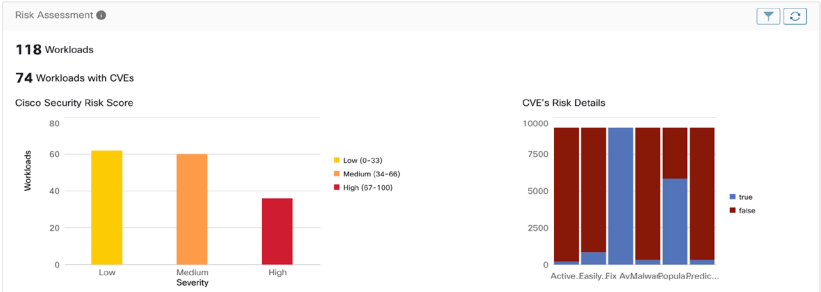
機能とメリット

表 1 に、Cisco Secure Workload の主な機能と利点を示します。

表 1. Cisco Secure Workload の主な機能と利点

機能	利点
可視性	• ワークロードのエージェントは、豊富なネットワークテレメトリを収集し、CSW テナントに送信します。このテレメトリはポートやプロトコルだけでなく、ネットワークパケットをより詳しく可視化します。 • ワークロードのエージェントは、徹底した可視性を提供するため、インストールされているパッケージ、未解決の脆弱性、未使用のオープンポート、プロセスツリーに関する情報も収集します。このため、ワークロードのセキュリティ態勢が向上します。 • エージェントレス環境の場合、ネットワークテレメトリは、NetFLow、ERSPAN、IP-FIX、ファイアウォール、ロードバランサなどの Ingest アプライアンスとコネクタを介して収集されます。パブリッククラウド環境では、ネットワークフローログ（vpc フローログ）が使用されます。DPU ハードウェアが利用可能な場合には、代わりに DPU ベースのテレメトリ統合を使用できます。 • Cisco Secure Workload は、さまざまな統合を使用してフローのコンテキストを取り込みます。既存のラベルまたはタグとユーザー情報が検出され、ISE、ServiceNow、Identity、Cloud Connector などの Edge アプライアンスとコネクタを通じて使用されます。Cloud Connector の場合、すべてのインベントリ、サービス、およびタグが REST API を介して検出されます。 • Cisco Secure Workload は、K8s クラスタおよび Openshift クラスタ内のコンテナ間トラフィックに関する徹底したインサイトと可視性を提供します。 • 企業ネットワークとインフラストラクチャは、階層化された範囲ツリーで可視化されます。それぞれの範囲は、同様のラベルを持つワークロードの集まりです。これにより、企業ネットワークの設計が可視化されます。
ゼロトラスト マイクロセグメンテーション ポリシーのライフサイクル	• **絶対ポリシー**：InfoSec の企業全体のポリシーがルート範囲レベルで定義されます。絶対ポリシーは、階層内のすべての子範囲に継承されます。また絶対ポリシーは、他のすべての低レベルのポリシーを上書きします。

機能	利点
	• **ポリシー検出**：Cisco Secure Workload は AI/ML テクノロジーを活用してワークロードの動作を分析して基準値を設定し、それをクラスタに分類し、マイクロセグメンテーション ポリシーを推奨します。 • **ポリシー分析**：検出されたポリシーを分析して、予期しないエスケープフローや拒否されたフローがないかを確認します。簡易分析を実行して、特定のフローを確認することもできます。 • **ポリシーの適用**：分析済みのポリシーは、ファイアウォール、クラウドネイティブツール、ロードバランサなどのさまざまなポリシー適用ポイントで、ホスト上のエージェントによって、またはエージェントレスに適用されます。 • **ポリシーの廃止**：ヒットカウント、使用パターン、最後に使用された情報などのポリシーインサイトにより、ポリシーの使用や廃止が推奨されるポリシーに関する詳しい情報がわかります。 • **高度なポリシー**：このタイプのポリシーには、FQDN、脆弱性スコア、プロセス、ユーザー、グループベースのポリシーが含まれます。一般に、これらは静的ポリシーであり、アプリケーション範囲レベルで設定されます。アプリケーション セグメンテーションのための、時間のかかるリソースリストの手動作成を排除。 
適用	• エージェントベースの適用では、OS レベルのフィルタ処理機能を利用してポリシー規則を設定します。Windows は Windows フィルタリング プラットフォームを、Linux は IP フィルタを使用します。 • エージェントレスな適用では、他の適用ポイントを使用します。たとえば、クラウドワークロードの場合は、クラウド ネイティブ セキュリティ グループ、ファイアウォール、NSG を使用します。オンプレミス ワークロードの場合は、Cisco ファイアウォール統合を使用し、適用には F5、NetScaler との統合が使用されます。 • サーバーの最新の DPU テクノロジーも活用され、物理ホストで実行されているすべての仮想ワークロードにポリシーを適用します。

機能	利点
脆弱性ダッシュボード	• Cisco Secure Workload エージェントは、ワークロードのすべてのパッケージ情報と、関連する脆弱性を収集します。 • CVE に関するインテリジェンスは、6 つのパラメータに基づいて、シスコの脆弱性管理のセキュアワークロードと統合されます。 • ダッシュボードには、環境に存在する脆弱性の概要が表示され、ワークロード、パッケージ、CVE によるフィルタ処理機能もあります。 
レポートダッシュボード	新しいレポートダッシュボードには、ペルソナベースの 3 つのレポートセクションがあります。 • **概要（Overview）**：このセクションには、セグメンテーション、ワークロード、トラフィック、ライセンスの使用状況の概要が表示されます。 • **オペレーション（Operation）**：このセクションには、エージェントの概要とバージョン、エージェントの問題と非アクティブなエージェント、上位のコンシューマとプロバイダー、クラスタとテレメトリの概要などの詳細が表示されます。  • **コンプライアンス（Compliance）**：このセクションの中心はセキュリティベースのレポートであり、CVE リスクスコア、MITRE フレームワークアラートの概要を含むワークロードのリスク評価が表示されます。 

導入モデルと規模

Cisco Secure Workload にはオンプレミスオプションと Software as a Service（SaaS）オプションの両方があり、お客様はそれぞれのビジネスニーズを満たすモデルを選択できます。

オンプレミスへの導入では、お客様はハードウェアベースのアプライアンスモデル（小型モデルまたは大型モデル）を選択できます。プラットフォームの選択は、環境内のワークロードの数や目的のフローテレメトリの忠実度レベルなど、拡張性に関する考慮事項によって異なります。

すべてのワークロードで会話のみのフローテレメトリ用に構成されている場合、各プラットフォームは、詳細なフローテレメトリが有効になっているデフォルトのプラットフォームの規模の 2 倍まで垂直方向に拡張できます。さらに、Cisco Secure Workload は、フェデレーション機能を使用して、地理的に分散した非常に大規模なエンタープライズ環境の要求を満たすために水平方向に拡張できます。

Cisco Secure Workload では、ディザスタリカバリ（DR）機能も提供しています。継続的なバックアップと復元の機能により、大規模な障害や災害が発生したときにデータと運用をスタンバイクラスタに復元できます。

Cisco Secure Workload SaaS オプション

Cisco Secure Workload SaaS オプションを使用すると、プラットフォームをオンプレミスで展開して維持しなくても、ワークロード保護機能のメリットを得ることができます。このオプションでは、Cisco Secure Workload ソフトウェアがクラウドで実行され、シスコによって管理および運用されます。お客様は必要なソフトウェア サブスクリプション ライセンスを購入して、ワークロードにソフトウェア エージェントを導入する必要があります。Cisco Secure Workload SaaS に、Cisco Security Cloud Control（SCC）からアクセスできるようになりました。SCC はプロビジョニング、ユーザーアクセス、およびロール管理など、複数のシスコ製品の管理を統合します。

この導入オプションは拡張性に優れているため、SaaS のみの環境のお客様や SaaS を初めて使用するお客様に適しています。小規模から開始し、需要の増大に応じて拡張できます。SaaS オプションのその他の利点は次のとおりです。

- TCO（総所有コスト）を大幅に削減。
- より短期間で価値を実現。

表 2 に、検証済みのサポート可能な SaaS オプションの規模を示します。

表 2. Cisco Secure Workload SaaS の規模

プラットフォームの特性	仕様
テナントごとにラベル付けできる IP アドレスの最大数（CMDB のみ）	6,000 / 100 ライセンス（SaaS のみ）
テナントごとにラベル付けできるサブネットの最大数（CMDB のみ）	120 / 100 ライセンス（SaaS のみ）
1 秒あたりの処理可能フローイベント数	1 秒あたり 5000 フロー / 100 ライセンス

Cisco Secure Workload-M（小型モデル）オプション

表 3 に、検証済みのサポート可能な規模を示します。

表 3. Cisco Secure Workload-M プラットフォームの規模

プラットフォームの特性	仕様
テレメトリデータを分析できる同時ワークロード数（仮想マシン、ベアメタル、またはコンテナホスト）	詳細モードで最大 10,000 のワークロード。 会話モードで最大 20,000 のワークロード。
1 秒あたりの処理可能フローイベント数	1 秒あたり最大 500,000 フロー
テナント数	7
テナントあたりの子範囲の数	1000
テナント全体の子範囲の総数	7000
テナントあたりのワークスペースの数	1000
テナント間のワークスペースの総数	5000
テナントあたりのインベントリフィルタの数	1000
テナント全体のインベントリフィルタの総数	7000
子範囲あたりのロール数	6
すべてのルート範囲でラベル付けできる IP アドレスの最大数	500,000
すべてのルート範囲でラベル付けできるサブネットの最大数	50,000

表 4 には、Cisco Secure Workload-M プラットフォームの電力および冷却要件を示します。

表 4. Cisco Secure Workload-M の電力および冷却の仕様

プラットフォーム要件	Cisco Secure Workload M5 アプライアンス	Cisco Secure Workload M6 アプライアンス
最大電力	5.5 kW	6 kW
最大冷却要件	13,500 BTU/時	14,171 BTU/時
ラック仕様	Cisco R42612 ラックデータシート [英語]	

Cisco Secure Workload（大型モデル）プラットフォームオプション

表 5 に、検証済みのサポート可能な規模を示します。

表 5. Cisco Secure Workload 大型プラットフォームの規模

プラットフォームの特性	仕様
テレメトリデータを分析できる同時ワークロード数（仮想マシン、ベアメタル、またはコンテナホスト）	詳細モードで最大 37,500 のワークロード。 会話モードで最大 75,000 のワークロード。
1 秒あたりの処理可能フローイベント数	1 秒あたり最大 200 万フロー
テナント数	35
テナントあたりの子範囲の数	5000
テナント全体の子範囲の総数	35000
テナントあたりのワークスペースの数	3500
テナント間のワークスペースの総数	20000
テナントあたりのインベントリフィルタの数	5000
テナント全体のインベントリフィルタの総数	35000
子範囲あたりのロール数	6

プラットフォームの特性	仕様
すべてのルート範囲でラベル付けできる IP アドレスの最大数	1,500,000
すべてのルート範囲でラベル付けできるサブネットの最大数	200,000

表 6 には、Cisco Secure Workload プラットフォームの電力および冷却要件を示します。

表 6. 大型モデルの電力および冷却の仕様

プラットフォーム要件	Cisco Secure Workload M5 アプライアンス	Cisco Secure Workload M6 アプライアンス
ピーク電力シングルラックオプション*	22.5 kW	31.8 kW
最大冷却要件シングルラックオプション*	50,000 BTU/時	72117 BTU/時
総重量シングルラックオプション	800 kg（1,800 ポンド）	800 kg（1,800 ポンド）
配電ユニット（PDU）と電源シングルラックオプション	三相 PDU X 4（定格電流と定格電圧は地域によって異なる）	三相 PDU X 4（定格電流と定格電圧は地域によって異なる）
ピーク電力デュアルラックオプション	1 ラックあたり 11.25 kW（合計 22.5 kW）	15.9 kW
最大冷却要件デュアルラックオプション	1 ラックあたり 25,000 BTU/時	1 ラックあたり 36,059 BTU/時
デュアルラックオプションの総重量	1 ラックあたり 400 kg（900 ポンド）	1 ラックあたり 400 kg（900 ポンド）
PDU と電源デュアルラックオプション	1 ラックあたり単相 PDU X 4（定格電流と定格電圧は地域によって異なる）	1 ラックあたり単相 PDU X 4（定格電流と定格電圧は地域によって異なる）
ラック仕様	Cisco R42612 ラックデータシート [英語]	

データのバックアップと復元

データのバックアップおよび復元機能の主な使用例には、停止中にクラスタを同じサイトまたは別のサイトの別のクラスタに復元することがあります。

表 7. データのバックアップと復元の完全バックアップモードとリーンモードの比較

プラットフォームの特性	完全バックアップモード	リーンモード
サポートされているプラットフォーム	• Cisco Secure Workload（大型モデル）プラットフォームオプション。 • Cisco Secure Workload-M（小型モデル）。	完全バックアップモードと同様。
サポートされるストレージタイプ	• バックアップと復元は、コピーされたデータの大部分が不変でフラットであり、特にオブジェクトストアに適しているため、S3V4 API と互換性のある S3 インターフェイスを備えた顧客管理オブジェクトストアからサポートされます。 • DBR は、クラスタのすぐ隣にある物理データストア、またはクラウド内の AWS S3 などのクラウドストレージ、または IP アドレスで到達できる任意の場所で動作します。	完全バックアップモードと同様。
バックアップされたデータ	すべてのバックアップは、すべてのデータストアにわたるポイントインタイム同期バックアップになります。以下のデータがオブジェクトとしてパッケージされ、バックアップされます。完全バックアップでは、チェックポイント内のすべてのオブジェクトがコピーされます。オブジェクトが変更されていない場合でもコピーされます。	設定データ以外をバックアップから除外するために、[リーンデータモード（Lean Data Mode）] を有効にできます。 次を除くすべてのデータがバックアップされます。 • フローデータベース。 • 自動ポリシー検出に必要なデータ。 • 適用ポリシー。 • ファイルハッシュ、データリークモデルなどのフォレンジックに役立つデータ。 • 攻撃対象領域の分析に関連するデータ。 • CVE データベース。

プラットフォームの特性	完全バックアップモード	リーンモード
ストレージ制限。	200 TB のストレージを推奨します。	フローはバックアップされないため、1 TB で十分です。

ライセンス要件

データのバックアップと復元を有効にするには、プライマリ（アクティブクラスタ）にアクティベーションキー形式のソフトウェア利用資格が必要です。アクティベーションキーは、クラスタ識別情報とともに ciscosecureworkload-licensing-support@cisco.com に電子メールを送信することで取得できます。

ソフトウェアライセンス

Cisco Secure Workload ソフトウェアは、使用されているエージェントまたはセンサーの種類に応じた等価ワークロードまたはデバイス（エンドポイント）の数に基づいてライセンスされます。テレメトリデータは、対応する他のセンサーまたはコレクタによってサポートされているエージェントを任意の組み合わせで使用して収集できます。ポリシーの適用は、インフラストラクチャの適用機能を備えたエージェントによって有効になり、Cisco Secure Firewall 統合、アプリケーション配信コントローラ（ADC）、およびパブリック クラウド インフラストラクチャのセキュリティグループを介して提供されるか、ストリーミングされる Kafka ポリシーを介してオーケストレーションされます。ワークロードは仮想マシン、ベアメタルサーバー、またはコンテナホストとして定義され、サーバーとデスクトップのオペレーティングシステムを含みます。

Secure Workload には、次の 2 つの主要な種類のライセンスがあります（SaaS およびオンプレミス導入オプションを含む）。

- **Secure Workload 保護ライセンス**：このライセンスは、テレメトリデータ収集、アプリケーションインサイト、フォレンジック、ソフトウェア脆弱性検出、ポリシーの推奨事項、ポリシーシミュレーション、ポリシー適用、コンプライアンスの追跡などのワークロード保護機能を提供します。
- **Secure Workload エンドポイントライセンス**：このライセンスは、エンドポイント（ラップトップ、デスクトップ、スマートフォンなど）にインストールされた Cisco AnyConnect クライアントから、NVM モジュールを使用して包括的なテレメトリデータの収集を行います。エンドポイントからアクセスされた、ユーザー、デバイス、グループ、プロセス ID、プロセス階層、OS、およびドメイン名に関する情報が提供されます。さらに、このライセンスは、pxGrid の統合を通じて Cisco ISE で管理されるエンドポイントデバイスにユーザーデバイスからの豊富なコンテキストを提供します。プラットフォームの機能を使用してポリシーの収集、分析、定義を行い、エンドポイントデバイスのアクティビティに対する可視性を提供する場合は、エンドポイント可視性ライセンスを購入する必要があります。このライセンスは、ワークロード保護ライセンスとは別に購入できます。このライセンスには、AnyConnect NVM または Cisco ISE を有効にするために必要なその他のライセンスは含まれていません（それらのライセンスは、別途購入する必要があります）。

複数の Cisco Secure Workload クラスタを導入している場合は、それらのクラスタ間でソフトウェアライセンスをプールすることもできます。

Cisco Secure Workload SaaS ライセンスを保有している場合、オンプレミス ライセンス オプションにライセンスを移植することはできません（その逆も同様です）。

ライセンス期間

Secure Workload SaaS の導入

SaaS サブスクリプションには、Cisco Secure Workload as a Service のオファー説明書 [英語] およびシスコの一般利用規約 [英語]（エンドユーザーライセンス契約など）（以下「本契約」）が適用されます。

オンプレミスの導入オプション

オンプレミスライセンスおよびサブスクリプションには、Cisco Secure Workload のオファー説明書 [英語]、およびシスコの一般利用規約 [英語] またはお客様とシスコとの間で締結された同様の規約（エンドユーザーライセンス契約など）（以下「本契約」）が適用されます。

サポートと互換性

Cisco Secure Workload のオペレーティングシステムのサポートと互換性の詳細については、互換性マトリクス [英語] のプラットフォームのサポート情報を参照してください。

発注情報

表 8 に、Cisco Secure Workload SaaS の導入オプションで使用されるサブスクリプション ソフトウェアのバンドルの製品番号を示します。

表 8. Cisco Secure Workload SaaS オプションのソフトウェアバンドル。

バンドルの製品番号	バンドルに含まれる製品番号	説明
C1-TAAS-SW-K9		SaaS オプション用のソフトウェア サブスクリプション ライセンスを含む Cisco Secure Workload バンドルの製品番号。
	C1-TAAS-WP-FND-K9	Cisco Secure Workload 保護サブスクリプション ライセンスのバンドルの製品番号。最小数量は 100 で、その後は 1 ずつ増加します。
	C1-TAAS-ENDPT-K9	エンドポイント向け Cisco Secure Workload エンドポイント可視性ソフトウェア サブスクリプション ライセンス。1,000 から 999,999 までの数を選択してください。たとえば、数量が 5,000 の場合、Cisco AnyConnect または Cisco ISE を介して追跡される 5,000 台のエンドポイントデバイスまで対応するライセンス価格になります。

また、ソフトウェア サブスクリプション ライセンスの製品番号に関する以下の追加情報も念頭に置いてください。

- サブスクリプション期間は 1 年、3 年、5 年から選択できます。
- サブスクリプション価格にはソフトウェアサポートが含まれます。
- 年次請求、月次請求、四半期請求オプション、または期間全体の前払いを選択できます。
- サブスクリプションを変更することで、ワークロード インスタンス ライセンスを追加できます。

- このソフトウェア サブスクリプション ライセンスは、Cisco Secure Workload SaaS の導入でのみ使用できます。

表 9 に、Cisco Secure Workload-M プラットフォームオプションのハードウェアおよびソフトウェアバンドルの製品番号を示します。

表 9. Cisco Secure Workload-M オプションのハードウェアおよびサブスクリプション ソフトウェア バンドル。

バンドルの製品番号	バンドルに含まれる製品番号	説明
C1-TETRATION-M		ハードウェアおよびソフトウェア サブスクリプション ライセンスを含む Cisco Secure Workload バンドルの製品番号。
	TA-CL-8U-M5-K9	Cisco Secure Workload Gen2 8RU クラスタ。
	TA-CL-8U-M6-K9	Cisco Secure Workload Gen3 8RU クラスタ。
	C1-TA-SW-K9	Cisco Secure Workload ソフトウェア サブスクリプション ライセンスのバンドルの製品番号。詳細については、表 9 を参照してください。

表 10 に、Cisco Secure Workload プラットフォームオプションのハードウェアおよびソフトウェアバンドルの製品番号を示します。

表 10. Cisco Secure Workload オプションのハードウェアおよびサブスクリプション ソフトウェア バンドル。

バンドルの製品番号	バンドルに含まれる製品番号	説明
C1-TETRATION		ハードウェアおよびソフトウェア サブスクリプション ライセンスを含む Cisco Secure Workload バンドルの製品番号。
	TA-CL-39U-M5-K9	Cisco Secure Workload Gen2 39RU クラスタ。
	TA-CL-39U-M6-K9	Cisco Secure Workload Gen3 39RU クラスタ。
	C1-TA-SW-K9	Cisco Secure Workload ソフトウェア サブスクリプション ライセンスのバンドルの製品番号。詳細については、表 9 を参照してください。

表 11 に、Cisco Secure Workload ソフトウェア サブスクリプション ライセンスのソフトウェアバンドルの製品番号を示します。

表 11. Cisco Secure Workload のオンプレミスの導入オプションに使用されるサブスクリプション ソフトウェア ライセンス。

バンドルの製品番号	バンドルに含まれる製品番号	説明
C1-TA-SW-K9		Cisco Secure Workload ソフトウェア サブスクリプション ライセンスのバンドルの製品番号
	C1-TA-CWP-K9	ワークロード保護のための Cisco Secure Workload オンプレミス サブスクリプション ライセンス。最小数量は 100 で、その後は 1 ずつ増加します。このライセンスは、以前の基本機能と適用機能を組み合わせたものです。たとえば、数量 500 は、最大 500 のワークロードまで対応するライセンスとなります。

バンドルの製品番号	バンドルに含まれる製品番号	説明
	C1-TA-ENDPT-K9	Cisco Secure Workload エンドポイント可視性ソフトウェア サブスクリプション ライセンスは、1 エンドポイント単位で発注します。最小発注数量は 1,000 です。たとえば、数量が 1,505 の場合、Cisco AnyConnect または Cisco ISE を介して追跡される 1,505 台のエンドポイントデバイスに対応するライセンス価格になります。

また、ソフトウェア サブスクリプション ライセンスの製品番号に関する以下の追加情報も念頭に置いてください。

- サブスクリプション期間は 1 年、3 年、5 年から選択できます。
- サブスクリプション価格にはソフトウェアサポートが含まれます。
- サブスクリプション階層は、入力された数量に基づいて自動的に選択されます。
- 年額課金オプションまたは期間全体の前払いを選択できます。
- サブスクリプションを変更することで、ワークロード インスタンス ライセンスを追加できます。
- このソフトウェア サブスクリプション ライセンスは、両方の形式の Cisco Secure Workload ハードウェア クラスタで使用できます。

Cisco Secure Workload エンドポイントソフトウェアのライセンスには、AnyConnect または AnyConnect NVM ライセンスが含まれていません。これらのライセンスは別途取得する必要があります。

シスコの専門知識を活用した導入の促進

シスコでは、組織が Cisco Secure Workload プラットフォームを最大限に活用できるように、アドバイザリ、実装、および最適化から継続的なソリューションサポートまで、プロフェッショナルサービスとサポートサービスを提供しています。シスコサービスのエキスパートが、お客様の実稼働データセンター環境にこのプラットフォームを統合し、お客様のビジネス目標に適した使用例を定義します。また、機械学習を調整し、ポリシーとコンプライアンスを検証して、アプリケーションと運用のパフォーマンスを向上させます。Cisco Secure Workload 向けシスコ ソリューション サポートでは、ハードウェア、ソフトウェア、ソリューションレベルのサポートを提供します。Cisco Secure Workload 向けに用意された、カスタムのサービスと固定価格で固定範囲のサービスをお選びいただけます。これらのサービスによって、短時間で価値を生み出し、環境への包括的な導入を行い、ポリシーやアプリケーション パフォーマンスを最適化し、ソリューションの幅広いサポートを得ることができます。

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。

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

Cisco Secure Workload プラットフォームの詳細については、https://www.cisco.com/go/Secureworkload を参照するか、最寄りのシスコ代理店にお問い合わせください。