Cisco Secure Workload リリースノート、リリース 3.7.1.22

初版：2022 年 12 月 21 日

はじめに

Cisco Secure Workload プラットフォーム（旧称 Cisco Tetration）は、ファイアウォールとセグメンテーション、コンプライアンスと脆弱性の追跡、動作ベースの異常検出、およびワークロードの分離を使用して、オンプレミスやマルチクラウド環境全体のすべてのワークロードにマイクロ境界を確立することにより、包括的なワークロードセキュリティを提供するように設計されています。このプラットフォームでは、高度な分析とアルゴリズムのアプローチを使用して、これらの機能を提供します。

このソリューションは、次の機能をサポートしています。

- 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
- ロールベースのアクセス制御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ラベルベースのポリシー定義
- ネイティブ オペレーティング システム ファイアウォール、および ADC（アプリケーション デリバリ コントローラ）や物理ファイアウォールまたは仮想ファイアウォールなどのインフラストラクチャ要素の分散制御による、一貫したポリシーの大規模な適用
- すべての通信のほぼリアルタイムのコンプライアンス モニタリングにより、ポリシー違反または潜在的な侵害を特定して警告
- ワークロード動作のベースライン化とプロアクティブな異常検出
- 動的な緩和と脅威ベースのワークロード分離を行う、一般的な脆弱性の検出

Cisco Secure Workload プラットフォーム内での分析とさまざまな使用事例をサポートするため、環境全体からの一貫したテレメトリ（フローデータ）が必要です。Cisco Secure Workload は、ソフトウェアエージェントやその他の方法を使用して豊富なテレメトリを収集し、データセンターのインフラストラクチャ内にある既存と新規の両方のインストールをサポートします。

このリリースでは、次のテレメトリソースがサポートされています。

- 仮想マシンおよびベアメタルサーバーにインストールされている Cisco Secure Workload エージェント
- コンテナホストのオペレーティングシステムで実行されているデーモンセット

- ミラーリングされたパケットから Cisco Secure Workload テレメトリを生成できる ERSPAN コネクタ
- アプリケーション デリバリ コントローラ（ADC）からのテレメトリの取り込み：F5 と Citrix
- Cisco Secure Workload テレメトリベースの NetFlow v9 または IPFIX レコードを生成できる Netflow コネクタ
- NetFlow セキュアイベントロギング（NSEL）テレメトリを収集するための ASA コネクタ
- VPC フローログ構成を使用して生成されたフローテレメトリデータ用の AWS コネクタ
- NSG フローログ構成を使用して生成されたフローテレメトリデータ用の Azure コネクタ

さらに、このリリースでは、以下との統合によるエンドポイントデバイスのポスチャ、コンテキスト、およびテレメトリの取り込みもサポートされています。

- ラップトップ、デスクトップ、スマートフォンなどのエンドポイントデバイスにインストールされた Cisco AnyConnect
- Cisco ISE（Identity Services Engine）

また、Cisco Secure Workload エージェントは、アプリケーション セグメンテーションのポリシー適用ポイントしても機能します。このアプローチを使用して、Cisco Secure Workload プラットフォームは、パブリック、プライベート、およびオンプレミスの展開全体で一貫性のあるマイクロセグメンテーションを実現します。エージェントはネイティブのオペレーティングシステム機能を使用するポリシーを適用し、データパスにエージェントを置く必要がなく、フェールセーフなオプションが提供されます。その他の製品マニュアルについては、「関連資料」の項を参照してください。

新機能および変更された機能に関する情報

この項では、このリリースの新機能と拡張機能、および既知の動作を示します。

互換性に関する情報

- OS のサポート終了に伴い、Windows 8.1 のエージェントパッケージは削除されました。

互換性の詳細については、Cisco.com の「プラットフォーム情報」を参照してください。

既知の動作

Cisco Secure Workload メジャーリリース 3.7.1.5 のリリースノートを参照してください。

特記事項

この項では、Cisco Secure Workload ソフトウェアに関する重要な注意事項をいくつか示します。

- Web ベースのユーザーインターフェイスにアクセスするには、Google Chrome ブラウザ バージョン90.0.0 以降を使用する必要があります。

- DNS を設定した後、Cisco Secure Workload クラスタの URL（https://<cluster.domain>）まで参照します。
- Cisco Secure Workload 仮想アプライアンス環境でコミッション/デコミッション機能を使用する場合は、次の使用上のガイドラインに従ってください。
  - この機能は TAC の支援を受けて使用することを意図しており、誤って使用すると回復不能な障害を引き起こす可能性があります。TACからの明示的な承認がない限り、2つの VM を同時にデコミッションしないでください。次の VM の組み合わせは、同時にデコミッションしないでください。
    - 複数のオーケストレータ
    - 複数のデータノード
    - 複数の namenode（namenode または secondaryNamenode）
    - 複数の resourceManager
    - 複数の happobat
    - 複数の mongodb（mongodb または mongoArbiter）
    - 一度に実行できるデコミッション/コミッションプロセスは1つだけです。異なるVMのデコミッション/コミッションを同時にオーバーラップしないでください。

（注） esx_commission スナップショット エンドポイントを使用する前に、必ず TAC にご連絡ください。

新しいソフトウェア機能、新しいハードウェア機能、および廃止された機能

新しいソフトウェア機能

このリリースでは、新しいソフトウェア機能はありません。

新しいハードウェア機能

このリリースでは新しいハードウェア機能はありません。

廃止された機能

このリリースには、廃止された機能はありません。

拡張機能

- ソフトウェアエージェントで x86_64 アーキテクチャの Oracle Linux 9 がサポートされるようになりました。

- ソフトウェアエージェントで x86_64 アーキテクチャの AlmaLinux 9 がサポートされるようになりました。
- ソフトウェアエージェントで x86_64 アーキテクチャの Rocky Linux 9 がサポートされるようになりました。
- ソフトウェアエージェントで MS Windows 10 Pro for Workstation と MS Windows 11 Pro for Workstation がサポートされるようになりました。
- インストーラ スクリプト ベースの Linux および AIX のインストール用に --golden_image フラグが追加されました。
- ソフトウェアエージェントのアンインストール操作で、すべてのインストールファイル、ランタイムファイル、およびログファイルとそのディレクトリがディスクから自動的に削除されるようになりました。
- *enforcer_config* ファイルを変更することで、適用モードが WFP の場合にポートスキャン防止フィルタをプログラムしないように Windows ホストのソフトウェアエージェントに指示できるようになりました。
- 新しい [セキュアコネクタ（Secure Connector）] ページで、Secure Connector の RPM を直接ダウンロードしたりトークンを生成したりできます。

動作における変更

このリリースでは動作の変更はありません。

検証済みスケーラビリティの制限値

次の表に、Cisco Secure Workload（39-RU）、Cisco Secure Workload M（8-RU）、および Cisco Secure Workload Cloud の拡張性の制限を示します。

表 *1 : Cisco Secure Workload*（*39-RU*）の拡張性の制限

設定可能なオプション	規模
ワークロードの数	最大 25000（VM またはベアメタル） すべてのセンサーが会話モードの場合、最大 50,000（2x）。
1 秒あたりのフロー機能	最大 200 万。

表 *2 : Cisco Secure Workload M（8-RU）* の拡張性の制限

設定可能なオプション	規模
ワークロードの数	最大 5,000（VM またはベアメタル） すべてのセンサーが会話モードの場合、最大 10,000（2x）。
1 秒あたりのフロー機能	最大 500,000。

表 *3 : Cisco Secure Workload Virtual（VMWare ESXi）* の拡張性の制限

設定可能なオプション	規模
ワークロードの数	最大 1,000（VM またはベアメタル）
1 秒あたりのフロー機能	最大 70,000。

（注） サポートされているスケールは、最初に制限に達したパラメータに基づいています。

解決済みのバグと未解決のバグ

このリリースで解決済みのバグと未解決のバグには、Cisco Bug Search Tool を使用してアクセスできます。この Web ベースのツールから、この製品やその他のシスコハードウェアおよびソフトウェア製品での問題と脆弱性に関する情報を保守するシスコ バグ トラッキング システムにアクセスできます。

（注） Cisco Bug Search Tool にログインしてこのツールを使用するには、Cisco.com アカウントが必要です。アカウントがない場合は、アカウントを登録できます。

Cisco Bug Search Tool の詳細については、Bug Search Tool（BST）ヘルプおよび FAQ を参照してください。

解決済みの問題

次の表に、このリリースで解決されたバグを示します。バグ ID をクリックして、シスコのバグ検索ツールにアクセスし、そのバグに関する詳細情報を表示します。

ID	見出し
CSCwc79283	RHEL ホストのエージェントがエージェントの再起動の異常で繰り返し表示される

ID	見出し
CSCwf78123	[Linux] iptables-legacy が存在する場合、新しいプラットフォームでポリシーの逸脱/修正が継続的に発生する。
CSCwc47484	[ソルトウェアエージェントリスト（Software Agents List）] ページにエージェントリストが正しく表示されない
CSCwc42706	適用を有効にするときに、影響を受けるワークロードのリストで内部エラーが発生する。
CSCvz98522	フェデレーションでコンプライアンス適用アラートを使用できない
CSCwd07794	タグを更新する POST API で変更ログにログエントリが生成されない
CSCwd85126	AIX LPAR で、エージェントには最終チェックイン時刻があるが、適用の登録は失敗した。
CSCwd00870	NetScaler サービスグループにスペースが含まれている場合、NetScaler 外部オーケストレータ REST API が失敗する
CSCwb21189	コンシューマとプロバイダーのポートが一致しない
CSCwd24158	CSW ルールと Openshift ルールの間に Iptables ルールの競合がある
CSCwc98940	vCenter 外部オーケストレータで、最後に行われた既知の正常な試行についてステータスとタイムスタンプを取得するスナップショットが必要
CSCwd65352	3.7 へのクラスタのアップグレード後に Windows エージェントの重複が報告される
CSCwb77220	ADM からすべての会話を表示またはダウンロードできない
CSCwc31985	ACI から受信した NetFlow データセットの復号化で EOF エラーが発生する
CSCwd60363	バックエンド WSS サービスへの接続の問題により、設定された制限を超える CPU がエージェントで消費される
CSCwc68679	フォレンジック機能を無効にしても、監査ログへのイベントの記録が停止しない
CSCwc72280	ユーザーが IP 仮想化を使用してネットワーク情報を取得している場合、Tetration UI でデータがレンダリングされない
CSCwd14928	パッケージ情報に基づくインベントリフィルタクエリで[インベントリフィルタ（Inventory Filter）] ページが表示される。
CSCwd00625	ホスト IP に関連付けられたラベルが、そのホストで報告される他のすべての IP に複製される

ID	見出し
CSCwc31977	NetFlow コネクタからの NetFlow パケットの復号化で一定のエラーが発生する。
CSCwd28349	Windows：ワークロードに IPV6 アドレスしかない場合、エージェントの登録が失敗する
CSCwd60335	3.7 の Linux/AIX エージェントで、使用可能な場合は FQDN でホスト名が報告される
CSCwb80743	ポリシー圧縮を使用する場合、UI ユーザー フィードバック メッセージが必要

未解決の問題

次の表にこのリリースで未解決の問題を示します。ID をクリックして、シスコのバグ検索ツールにアクセスし、そのバグに関する詳細情報を表示します。

ID	見出し
CSCwd67224	AIX 7.x で適用が有効になると、フラグメンテーションが原因でエージェントが CSW クラスタに接続できない
CSCwf78123	[Linux] iptables-legacy が存在する場合、新しいプラットフォームでポリシーの逸脱/修正が継続的に発生する。
CSCwd60340	リリース 3.6 からダウンロードしたエージェントインストーラ スクリプトでリリース 3.7 のセンサーがダウンロードされない
CSCwb39541	タイムアウトしている Investigate Traffic クエリのエラーメッセージを変更します。
CSCwb91717	保留状態のソフトウェアエージェントの SW ステータスのアップグレードチャートのデータがない。
CSCwb80213	vNIC がベアメタルサーバーでハングアップする（BM の eNIC バージョンをアップグレードする必要がある）
CSCwc63711	Azure セグメンテーションのアクセス許可がない
CSCwd93604	3.7 で Druid セグメントのロードキューが過負荷状態なる場合がある
CSCwb42177	ライブポリシーと適用ポリシーの分析：テーブルにカーソルを合わせると、範囲列とテキストが切り取られる

関連資料

ドキュメント	説明
Cisco Secure Workload Cluster Deployment Guide	Cisco Secure Workload（39-RU） プラットフォームと Cisco Secure Workload M（8-RU）のシングルおよびデュアルラックインストールの物理的な構成、設置場所の準備、およびケーブル配線について説明します。 Cisco Tetration（Cisco Secure Workload）M5 クラスタハードウェア導入ガイド
Cisco Secure Workload Virtual Deployment Guide	Cisco Secure Workload 仮想アプライアンス（旧称 Tetration-V）の展開について説明します。 Cisco Secure Workload Virtual (Tetration-V) Deployment Guide
Cisco Secure Workload プラットフォームのデータシート	Cisco Secure Workload プラットフォームのデータシート
Cisco Secure Workload のドキュメント	Cisco Secure Workload のドキュメント
最新の脅威データソース	Cisco Secure Workload

シスコへのお問い合わせ

上記のオンライン リソースでは問題を解決できない場合は、Cisco TAC にお問い合わせください。

- Cisco TAC の電子メール アドレス：tac@cisco.com
- Cisco TAC の電話番号（北米）：1.408.526.7209 または 1.800.553.2447
- Cisco TAC の連絡先（世界全域）：Cisco Worldwide Support の連絡先

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。