Cisco Secure Workload リリース 3.8.1.1 の新機能

First Published: 2023-05-19

Last Modified: 2023-07-27

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

機能名	説明
使いやすさ	
初めてのユーザーの導入準備エクスペリエンスの向上	オンボーディングエクスペリエンスは、オンボーディングからインストーラスクリプトまたはインストーライメージ方式を使用したソフトウェアエージェントのインストールまで、エンドツーエンドで強化されます。
移行の自動化	テナントからテナントへの構成の移行が完全に自動化され、仮想アプライアンスとコネクタがセットアップされるようになりました。
Secure Connector	[セキュアコネクタ（Secure Connector）] ページが拡張され、トンネルインターフェイスの回線プロトコルがダウンしたとき、またはイベントログとともに起動したときにメトリックが表示されるようになりました。これにより、ユーザーはトンネルの安定性をより詳細に確認できます。
エージェントの移行の自動化	リホーム機能を使用して、ソフトウェアエージェントをオンプレミスから SaaS に、または SaaS からオンプレミスに移動できるようになりました。
ポリシーの使用状況のレポートとコンプライアンス	ポリシーヒットカウントをインジケータとして使用して、次のことができるようになりました。 • 時間範囲内の未使用のポリシーを検索します。 • 最初と最後のカウントを含む、時間範囲内の特定のポリシーのヒットカウントを返します。

機能名	説明
ラベル管理：ラベルとIPのマッピング	ラベルの使用状況ごとに、ラベルとキー、ラベルとフィルタ、およびフィルタとワークスペースに加えて、ラベルとIPのマッピングを追加できるようになりました。
フロー送信元タイプ別のトラフィックフィルタリングとポリシー分析	センサータイプを使用して、フローの送信元およびフロー検索でフィルタリングできるようになりました。
ADM エクスポート	新しい ADM 機能により、ポリシーのグラフィカルビューの高解像度画像をダウンロードできるようになりました。
Day 2 オペレーション	
スマートライセンス	シスコ製品全体のソフトウェアライセンスを管理する統合ライセンス管理システムである Cisco Smart Licensing は、Cisco Secure Workload クラスタの登録、ライセンスの使用状況のレポート、および Cisco Secure Workload オンプレミスクラスタのコンプライアンスの追跡に使用できるようになりました。
アラートの拡張機能	外部オーケストレータの構成中に、アラートの重大度とアラートのしきい値を構成できるようになりました。 また、外部オーケストレータが機能を停止したときに生成されたアラート、またはコネクタからの接続障害が原因で生成されたアラートを Cisco Secure Workload でそれぞれ表示することもできます。 外部オーケストレータでアラートを有効にして表示する方法の詳細については、『Cisco Secure Workload ユーザーガイド』の「外部オーケストレータ」セクションを参照してください。
テストアラートの生成	レビューまたはテストの目的で、[テストアラートの生成（Generate Test Alerts）] ボタンを使用して、パブリッシャとの接続を確認します。 アラートの構成中、サンプルアラートを構成して、アラートタイプとリンクされたパブリッシャに基づいてアラートを送信することもできます。 テストアラートを生成する方法の詳細については、『Cisco Secure Workload ユーザーガイド』の「Generate a Test Alert on the Alert」セクションを参照してください。
レポート機能	エグゼクティブ、ネットワーク管理者、およびセキュリティアナリスト向けに設計されたレポートダッシュボードが導入されました。このダッシュボードには、重要なワークフローステータス、トラブルシューティング機能、およびレポート作成機能が視覚的に表示されます。
MITRE ATT&CK フレームワーク UI の強化	レポートダッシュボードには、MITRE ATT&CK レイアウトに一致するセキュリティサマリーの新しいカードレイアウトが含まれています。その表示には、戦術とその数が含まれます。

機能名	説明
ホストエージェントでの拡張テレメトリバッファリング	ソフトウェアエージェントがホストで拡張ネットワークテレメトリバッファリングを提供するようになりました。この機能は、[フローディスククォータ（Flow Disk Quota）] を使用するか、エージェント設定プロファイルの [フロー時間枠（Flow Time Window）] を介して構成できます。
ソフトウェアエージェント（Windows）を無効にしてアンインストールするパスワードの保護	Windows のソフトウェアエージェントを、サービスの停止/無効化およびアンインストールから保護できるようになりました。この機能は、[エージェント設定プロファイル（Agent Config Profile）] ページのサービス保護設定を使用してオンにすることができます。
Cisco Secure Workload クラスタに報告されるエージェントのアンインストール	エージェントをアンインストールすると、その情報がクラスタに送信され、その情報で [ソフトウェアエージェント（Software Agent）] ページが更新されます。 [ソフトウェアエージェント（Software Agent）] ページの UI からエージェントを手動で削除することもできます。また、ユーザーは、エージェント設定プロファイルからクリーンアップ期間をオンにして、エージェントの自動クリーンアップまたは削除を有効にすることもできます。 詳細については、『Cisco Secure Workload ユーザーガイド』の「Removing Software Agents」にある Linux、Windows、AIX エージェントの「Remove a Deep Visibility or Enforcement」セクションを参照してください。
統合	
Cisco Secure Firewall Management Center 統合の拡張機能	ネットワーク管理者は、ワークロードに関連付けられた特定のルールセットを、対応する Cisco Secure Firewall Management Center および Cisco Secure Firewall Threat Defense ドメインにプッシュできるようになりました。
Cisco Secure Firewall Management Center を使用したワークロードの仮想パッチ適用	ネットワーク管理者は、CVE 情報を Cisco Secure Workload から Cisco Secure Firewall Management Center にプッシュして、ファイアウォールの脅威からの保護機能を強化できるようになりました。これにより、ワークロードを既知の脆弱性から保護し、ファイアウォールで IPS シグニチャを使用した補完コントロールとして仮想パッチ適用を提供できます。
ISE コネクタでの AD/LDAP 設定に対するユーザー権限	ISE および AnyConnect NVM コネクタの導入準備のために、標準のドメインユーザーアカウントを使用してコネクタに LDAP を設定できるようになりました。 詳細については、『Cisco Secure Workload ユーザーガイド』の 「LDAP Configuration」セクションを参照してください。

機能名	説明
ISE と ISE-PIC の統合	Cisco Secure Workload の ISE コネクタは、pxGRID を使用して ISE-PIC に接続し、ISE を通じて報告されたエンドポイントから ISE グループ名と ISE グループタイプを含むメタデータを取得するようになりました。
ISE 統合：ISE PxGrid から取り込まれたエンドポイントとその属性を選択/フィルタ処理する機能	ISE を通じて報告されたエンドポイントのコンテキスト情報をすべて取り込みたくない場合は、ISE コネクタの設定中に ISE 属性を無視できるようになりました。 ISE コネクタを設定するときに、複数の IPv4 または IPv6 サブネットを入力して ISE エンドポイントをフィルタ処理できるようになりました。
NetFlow ソースのリストを報告する NetFlow コネクタ	NetFlow コネクタに NetFlow を送信する NetFlow 送信元のリストを収集してクラスタに報告できます。
フォレンジック、脆弱性、アラートに関する AIX/UNIX の機能拡張	より詳細なフォレンジックモニタリングおよびポリシー適用のため、ネットワークの可視性、オペレーティングシステムのプロセスレベルの可視性を管理する Tetration エンジンが 1 つだけになりました。AIX、Linux、および Solaris 上のソフトウェアエージェントは、csw-agent サービスでのみ表されます。
製品の進化	
Windows のネイティブ OS API を介してパケットをキャプチャする	Windows エージェントは、ndiscap.sys（Microsoft 組み込み）ドライバと Windows を使用した eventstTracing（ETW）フレームワークを使用してネットワークフローをキャプチャするようになりました。既存の Cisco Secure Workload にバンドルされている Npcap バージョンは、ホストで使用できなくなりました。
Solaris 11.4 x86_64 でネットワークの可視性をサポート	Solaris 11.4 ではネットワークの可視性がサポートされています。
コンテナ	
Kubernetes コントロール プレーン トラフィック用の事前作成済みポリシーテンプレート	Kubernetes 環境（eks、aks、gke、openshift）でポリシーテンプレートを使用できるため、Kubernetes クラスタでのポリシーの検出と実装が簡単になり、アプリケーション要件に合わせてポリシーをカスタマイズおよび追加できます。
パブリッククラウドの K8s サービスオブジェクトタイプのロードバランサに対応	AKS および EKS クラスタの Kubernetes サービスオブジェクトタイプのロードバランサをサポートします。

機能名	説明
Kubernetes またはコンテナ化されたワークロードに対する ADM の有効性	ポリシー検出の Kubernetes サポートの新しいトピックが追加され、ポリシー検出で Kubernetes 設定のポッドとサービスに関する情報を使用して、ポッドとサービス両方のクラスタを作成します。 外部オーケストレータページから [ポリシー検出のクラスタリングに使用（Use for policy discovery clustering）] が削除されました。
Kubernetes - Windows ワーカーノードのサポート	ソフトウェアエージェントは、AKS 上の Kubernetes Windows ワーカーノードと、Windows ワーカーノードを使用する標準の Kubernetes クラスタで、ホストとポッドのネットワークテレメトリをキャプチャしてレポートするようになりました。 （注） GKE または EKS には適用されません。
クラウド ネイティブ ワークロード	
クラウドとオンプレミスのエージェントレス ワークロードを UI で区別する	フローから学習した通常の IP と、EC2 などのエージェントレス クラウド インスタンスを UI で区別します。
スケーリング	
SaaS および 39 RU アプライアンスの拡張性の強化（75k）	• SaaS のシングルテナントは、最大 75K のワークロードをサポートできます（会話モード）。 • 39 RU のシングルテナントまたはマルチテナントは、最大 75K のワークロードをサポートできます（会話モード）。 • 8 RU のシングルテナントまたはマルチテナントは、最大 20K のワークロードをサポートできます（会話モード）。
ハイブリッド マルチクラウド ワークロード	
GCP コネクタの拡張機能	GCP コネクタは、タグの取り込み、VPC フローログの取り込み、GCP 組み込みファイアウォールを使用したセグメンテーションなどの新機能をサポートするようになりました。
AWS コネクタのセキュリティ強化	AWS コネクタに AWS IAM ロールベース認証のサポートが追加されました。
AWS コネクタのトラブルシューティングの拡張機能	各 AWS コネクタのイベントを表示する新しい [イベントログ（Event Log）] タブが追加されました。このログは、さまざまな機能から AWS コネクタごとに発生する重要なイベントを理解するために役立ちます。

機能名	説明

ワークフロー改善のためのバックエンドと UI のアップグレード	AWS コネクタページが強化され、ワークフローが改善されました。次の拡張機能が含まれます。
	• 改善された UI では、各クラウドコネクタに対して作成されたすべての設定の概要が表示されます。
	• テンプレートの生成と開始が別のビューに追加されました。
	• Assume Role の登録/更新/削除とその状態およびトリガーアクションが追加されました。
	• 登録の状態が設定ごとに一目でわかるように追加されました。
	• UI での使用スペースを減らすための機能強化：
	  • Assume Role ワークフローが [設定（Settings）] に追加されました。
	  • リソース選択は、各レベルでリソースを取得するツリー状の構造で行うことができます。
	• 別個の [インベントリ（Inventory）] タブが追加され、選択したリソースおよびスコープコンテキストのインベントリテーブルが表示されます。これにより、ユーザーはそれらの違いを比較できます。
	• [設定（Settings）] を除き、リソース/範囲の選択に役立つフィルタがすべてのビューに追加されました。

Azure コネクタのトラブルシューティングの拡張機能	各 Azure コネクタのイベントを表示する新しい [イベントログ（Event Log）] タブが追加されました。このログは、さまざまな機能から Azure コネクタごとに発生する重要なイベントを理解するために役立ちます。
データのバックアップと復元	
S3 バケット設定チェックの詳細なステータスとエラーメッセージ	データのバックアップを設定するときに、S3 バケット設定の詳細なステータスチェックを表示できるようになりました。
バックアップの失敗をデバッグするためのエラーレポートの強化	エラーレポートが強化され、チェックポイントの表形式のビューがバックアップ ステータス ページに追加のフィルタオプションとともに表示されます。

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。

（注） M4 のサポートはリリース 3.8.1.1 に限定されており、リリース 3.8.1.1 より後のリリースでは M4 はサポートされません。

廃止された機能

機能	機能説明	
フローテーブル列は廃止されました	フローテーブルの次の列は使用できなくなりました。	
	• [TCPのパフォーマンス（TCP Performance）] • [順方向TCPボトルネック（Fwd TCP Bottleneck）] • [逆方向TCPボトルネック（Rev TCP Bottleneck）] • [順方向輻輳ウィンドウの削減（Fwd Congestion Window Reduced）] • [逆方向輻輳ウィンドウの削減（Rev Congestion Window Reduced）] • [変更された順方向MSS（Fwd MSS Changed）] • [変更された順方向MSS（Fwd MSS Changed）] • [変更された逆方向MSS（Rev MSS Changed）]	• [順方向TCP受信Window Zero（Fwd TCP Rcv Window Zero?）] • [逆方向TCP受信Window Zero（Rev TCP Rcv Window Zero?）] • [順方向ファブリックパス（Fwd Fabric Path）] • [逆方向ファブリックパス（Rev Fabric Path）] • [順方向バーストインジケータ（Fwd Burst Indicator）] • [逆方向バーストインジケータ（Rev Burst Indicator）] • [順方向最大バーストサイズ（KB）（Fwd Max Burst Size (KB)）] • [逆方向最大バーストサイズ（KB）（Rev Max Burst Size (KB)）] • フローフィルタ
アラート機能は廃止されました	近接アラートとファブリックアラート、および外部 Kafka（データタップ）パブリッシャは、このリリースから廃止されました。	

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。