# セキュリティ ダッシュボード

セキュリティダッシュボードは、Cisco Secure Workload で利用可能な複数のシグナルをまとめることで、実用的なセキュリティスコアを提示します。現在のセキュリティポジションを把握し、改善するのに役立ちます。

セキュリティダッシュボードは、フロー検索、インベントリ検索、自動ポリシー検出、近隣、フォレンジックなど、Cisco Secure Workload 内での多くの詳細なドリルダウンの出発点として機能します。

# セキュリティダッシュボードへの移動

セキュリティダッシュボードを表示するには、ウィンドウの左側にあるナビゲーションバーで [概要（Overview）] をクリックします。

# セキュリティスコア

セキュリティスコアは、0～100の数値で、カテゴリ内のセキュリティポジションを示します。100 のスコアが最高のスコアで、0 のスコアが最悪です。スコアは 100 に近いほど良くなります。

セキュリティスコアの計算では、インストールされているソフトウェアパッケージの脆弱性、プロセスハッシュの一貫性、さまざまなインターフェイスの開いているポート、フォレンジックおよびネットワーク異常イベント、ポリシーへの準拠/非準拠が考慮されます。

# セキュリティスコアのカテゴリ

6 種類のスコアカテゴリがあります。ワークロードのセキュリティ面の大部分が、これらのカテゴリを導出するために考慮されます。

- [脆弱性スコア（Vulnerability Score）]：ワークロードにインストールされているパッケージの脆弱性がスコアリングに使用されます。
- [プロセスハッシュスコア（Process Hash Score）]：プロセスハッシュの一貫性（および異常）に加え、無害なプロセスハッシュおよびフラグ付きプロセスハッシュがスコアリングに使用されます。
- [攻撃対象スコア（Attack Surface Score）]：プロセスでは、サービスを利用可能にするために、複数のインターフェイスで1つ以上のポートが開いている場合があります。未使用のオープンポートが、スコアリングに使用されます。
- [フォレンジックスコア（Forensics Score）]：ワークロードのフォレンジックイベントの重大度がスコアリングに使用されます。
- [ ネットワーク異常スコア（Network Anomaly Score）]：ワークロードのネットワーク異常イベントの重大度がスコアリングに使用されます。

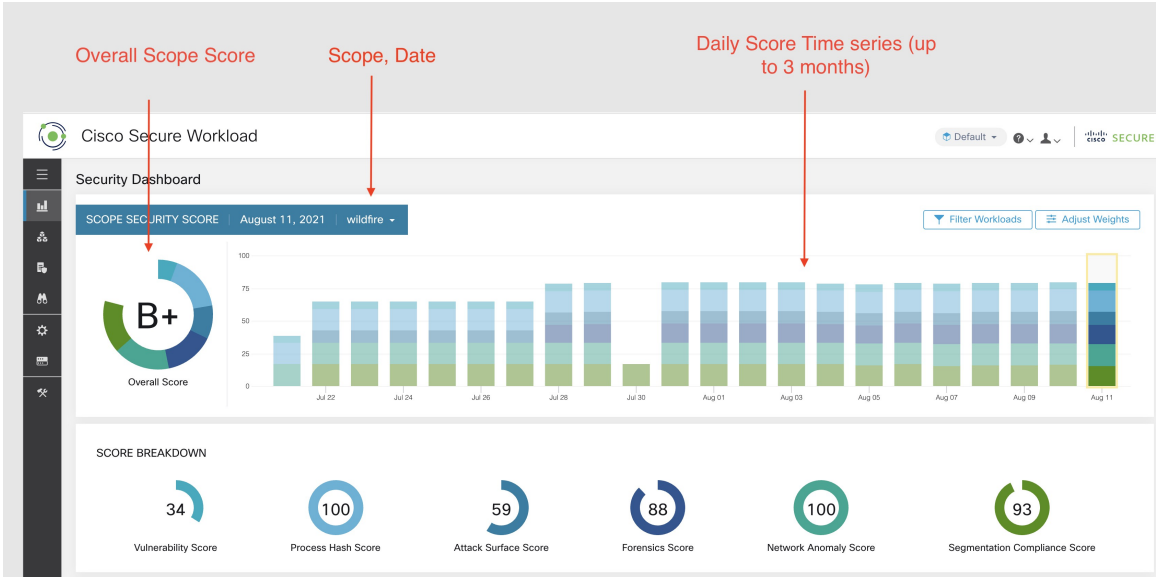
- [セグメンテーションコンプライアンススコア（Segmentation Compliance Score）]：自動的に検出されたポリシーに対する遵守（許可）および違反（エスケープ）がスコアリングに使用されます。

# ハイレベルビュー

セキュリティダッシュボードには、選択した範囲の範囲レベルスコアが表示されます。時系列の総合スコアとスコアの内訳があり、選択した範囲の 6 つのスコアカテゴリのスコア詳細が 1 つずつ下に表示されます。

# 範囲レベルスコアの詳細

範囲レベルスコアの詳細はダッシュボードの上部にあります。

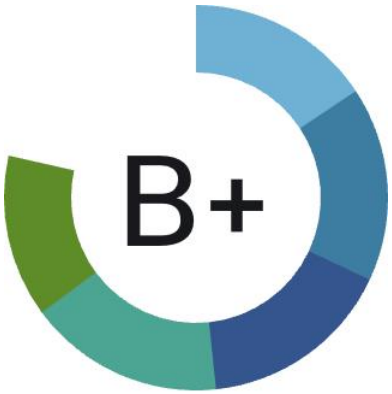



以下の内容が表示されます。

- **全体的な範囲スコア**：選択した範囲の全体的なスコア。
- **日次スコア時系列**：3 か月までの積み上げ時系列。
- **スコアの内訳**：時系列での選択した日のカテゴリスコアの内訳。

## 総合スコア

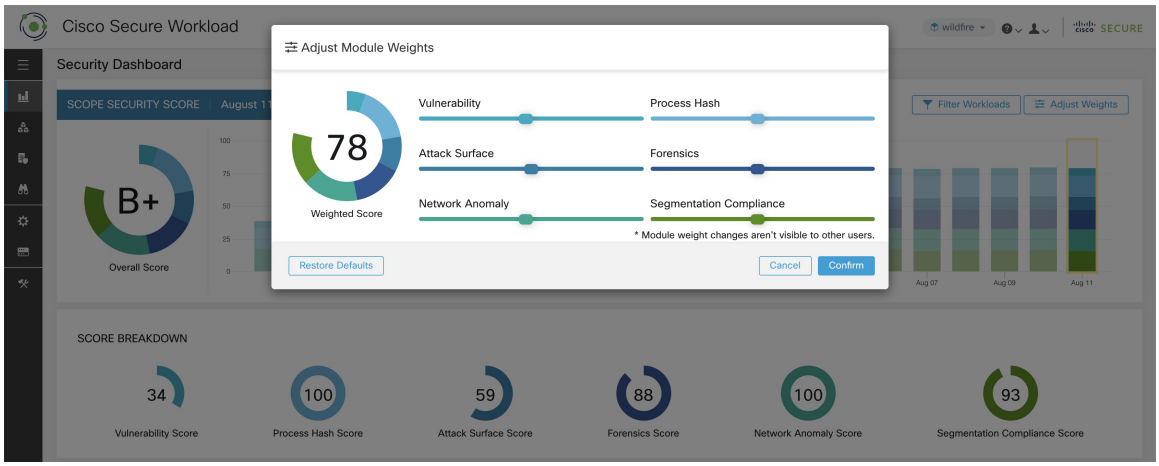
総合スコアは、**A+**、**A** ～ **F** の文字です。**A+** が最も良いスコアです。**F** が最も悪いスコアです。これは、スコアカテゴリを表す各スライス（色分け）で構成されるドーナツグラフです。




総合スコアは、スコアの6つのカテゴリの加重平均です。デフォルトでは、すべての重みは等しくなっています。スコアが **N/A** の場合、全体のスコア計算では 0 と見なされます。

$$Overall\ score = \frac{\sum W_{category} \times Score_{category}}{\sum W_{category}}$$

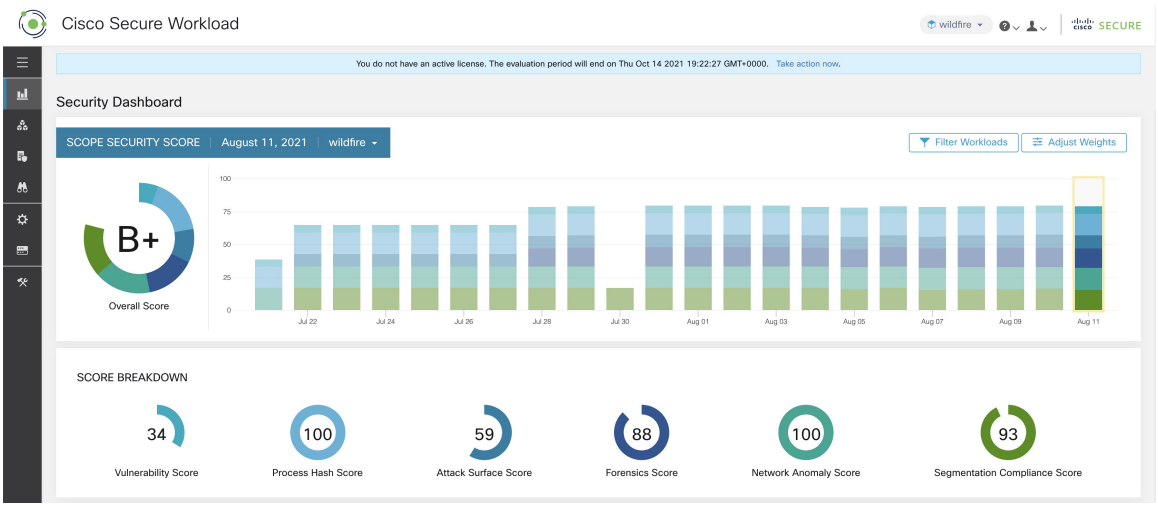
重みは、**重みの調整**モジュールのスライドを使用して調整できます。ユーザーごとに独自の重み調整を設定できるため、スコアをユーザーの優先順位に合わせることができます。




**重要**：スコアが **N/A** の場合、全体のスコア計算では **0** と見なされます。

# 日次時系列

最大3か月までの積み上げ時系列です。長期間にわたるセキュリティポジションの追跡に役立ちます。各スタックは、1 日の全体的なスコアを表します。スタック内の各セグメントは、異なる色で表されるカテゴリです。日をクリックすると、その日のスコアの内訳が表示されます。



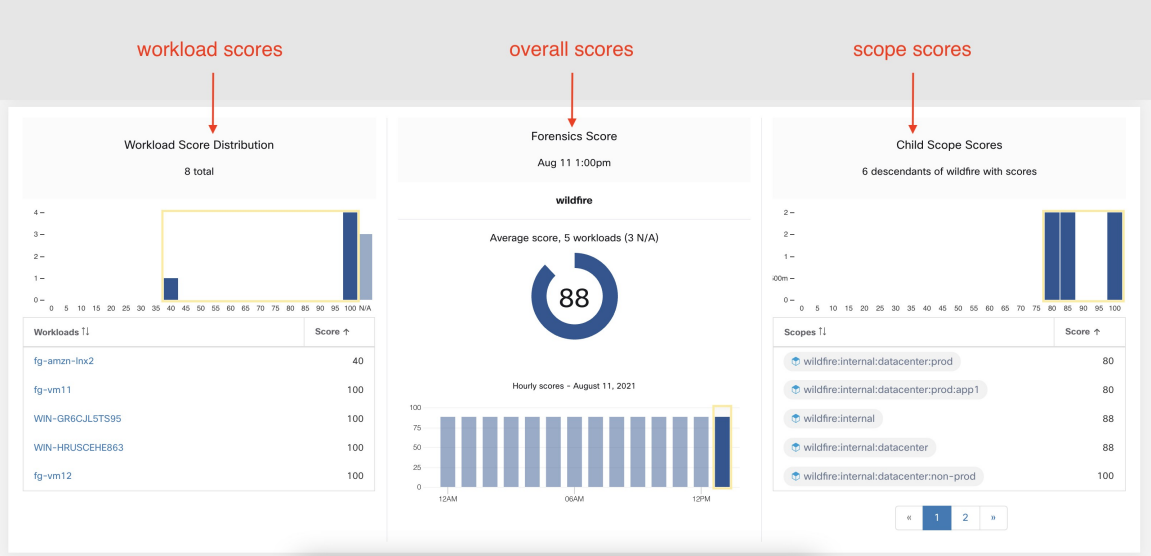

# スコアの内訳

[Score Breakdown（スコアの内訳）] には、時系列で選択された日の 6 つのカテゴリすべてのスコアが表示されます。スコア **N/A** は、スコアが利用できないことを示します。全体のスコア計算では 0 としてカウントされます。

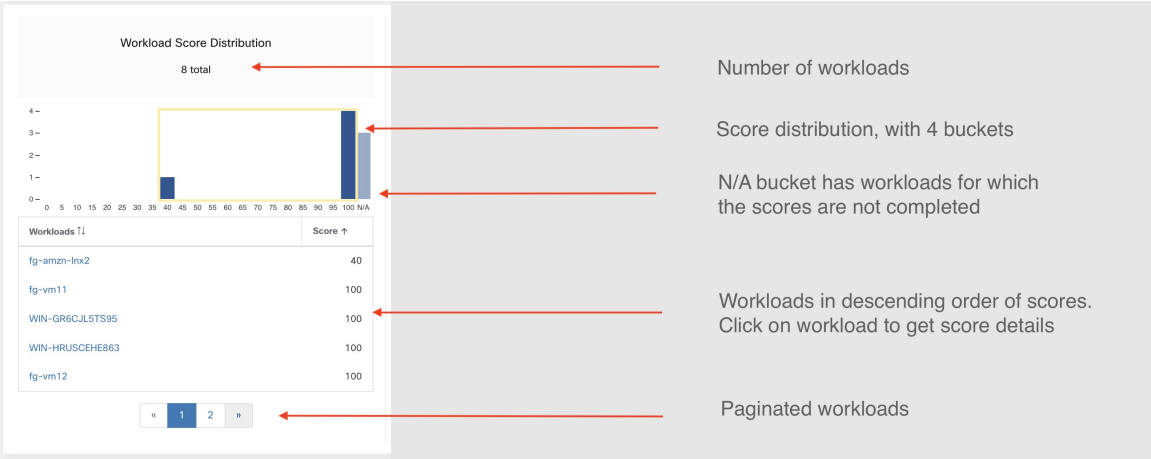

**重要**：スコアが **N/A** の場合、全体のスコア計算では **0** と見なされます。

# スコアの詳細

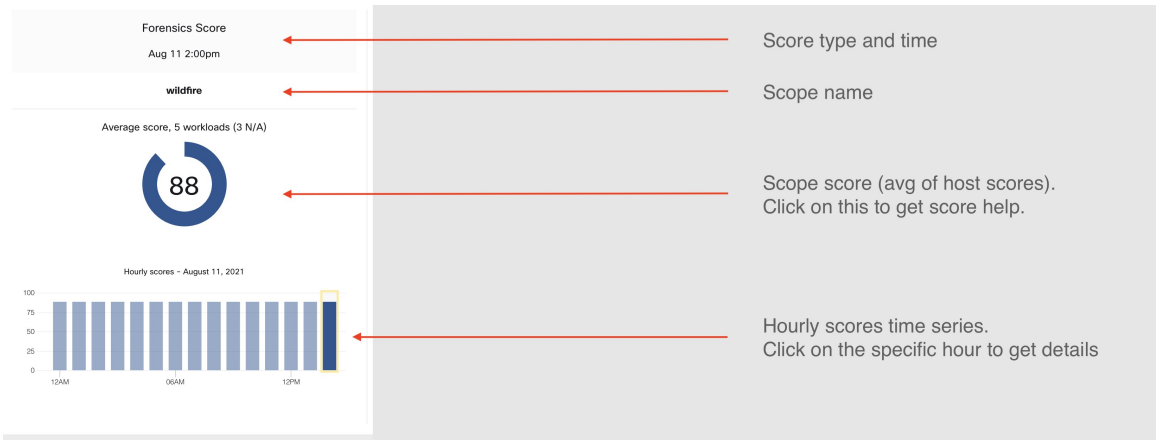
6 つのカテゴリは、それぞれ次のテンプレートに従います。テンプレートには、ワークロードスコアの分布、1 時間ごとの時系列、および子範囲のスコア分布があります。



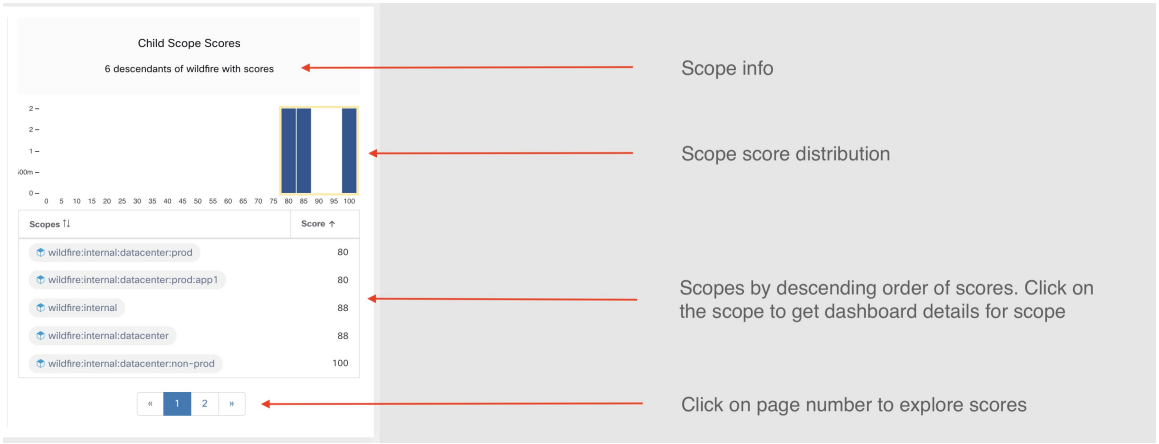

ワークロードスコアの分布では、選択した範囲の下のワークロードからのスコアの貢献度についての分析情報が得られます。分析情報により、最も低いスコアのワークロードをバブルアップして修正措置を迅速化するのに役立ちます。




1時間ごとの時系列は、選択した1日を通して1時間ごとのスコアを取得するのに役立ちます。1時間ごとの時系列で時間を選択すると、ワークロードスコアの分布と子孫範囲の分布が更新され、選択した時間が表示されます。




子孫範囲の分布では、選択した範囲の子範囲のスコア貢献度に関する分析情報が得られます。

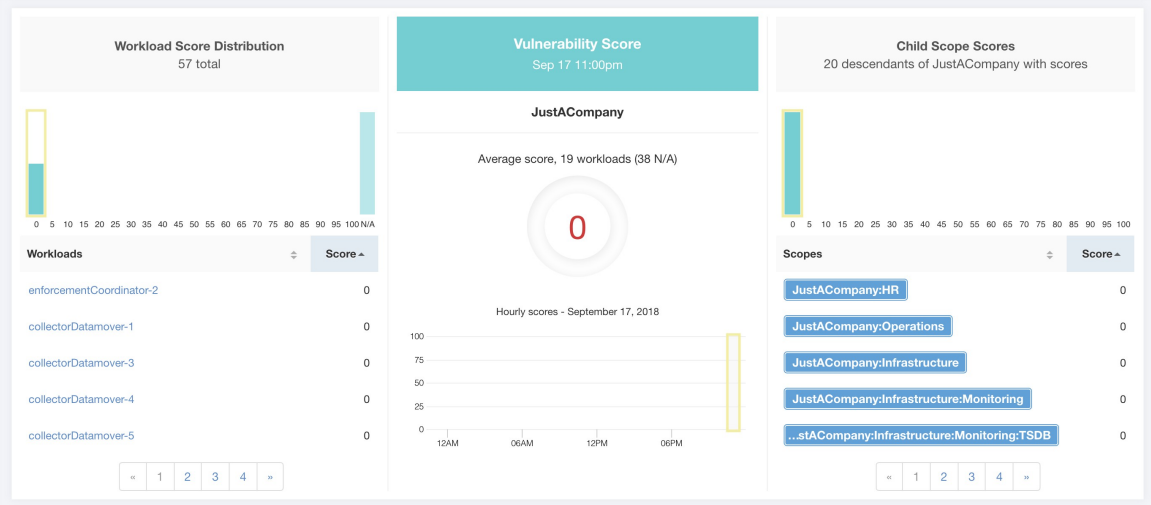



このセクションでは、各スコアカテゴリの詳細について説明します。

# 脆弱性セキュリティスコア

ワークロードにインストールされたソフトウェアパッケージの脆弱性は、脆弱性セキュリティスコアの計算に使用されます。

図 *1:* 脆弱性セキュリティスコアの詳細




低いスコアは次のことを示しています。

- インストールされている 1 つ以上のソフトウェアパッケージに深刻な脆弱性がある
- パッチまたはアップグレードを適用して、セキュリティリスクやエクスプロイトの可能性を減らせる

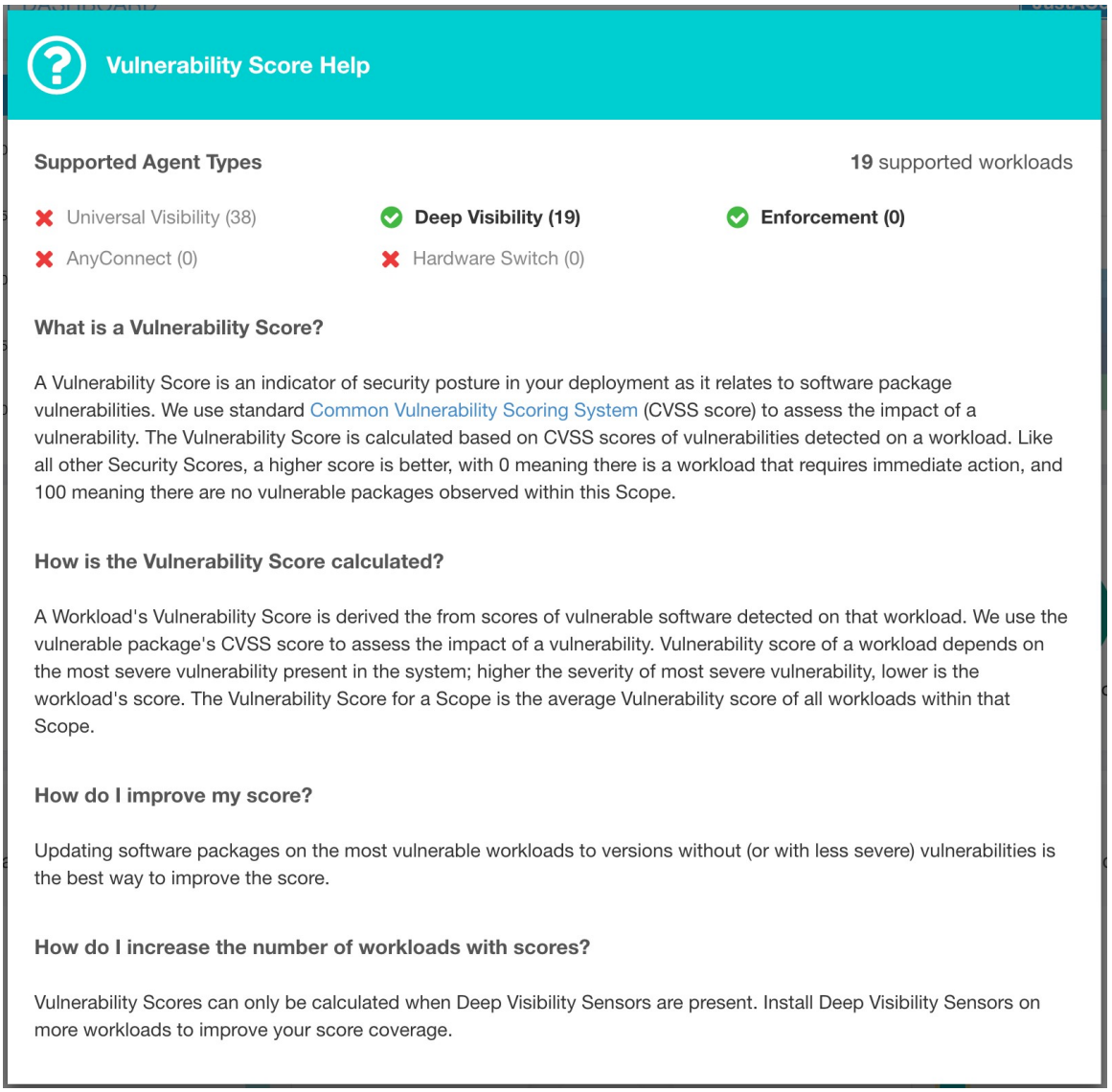
ワークロード上のソフトウェアパッケージは、既知の脆弱性（CVE）に関連付けられている可能性があります。CVSS（共通脆弱性評価システム）は、CVE の影響を評価するために使用されます。CVSS スコアの範囲は 0 ～ 10 で、10 が最も重大です。

CVE には、CVSS v2 および CVSS v3 スコアを設定できます。脆弱性スコアを計算するために、使用可能な場合は CVSS v3 が考慮され、それ以外の場合は CVSS v2 が考慮されます。

ワークロードの脆弱性スコアは、そのワークロードで検出された脆弱なソフトウェアのスコアから導き出されます。ワークロード脆弱性スコアは、CVSS スコアおよびベンダーデータに基づいて計算され、データが欠落しているか不正確な場合（新しい脆弱性に共通の問題）、シスコのセキュリティ調査チームによって調整される場合があります。このデータは、脅威フィードが設定されている場合、24 時間ごとに更新されます。最も重大な脆弱性の重大度が高いほど、スコアは低くなります。

範囲スコアは、範囲内のワークロードスコアの平均です。脆弱なソフトウェアパッケージでワークロードまたは範囲を特定し、より安全なパッケージでパッチまたはアップグレードすることでスコアを改善します。

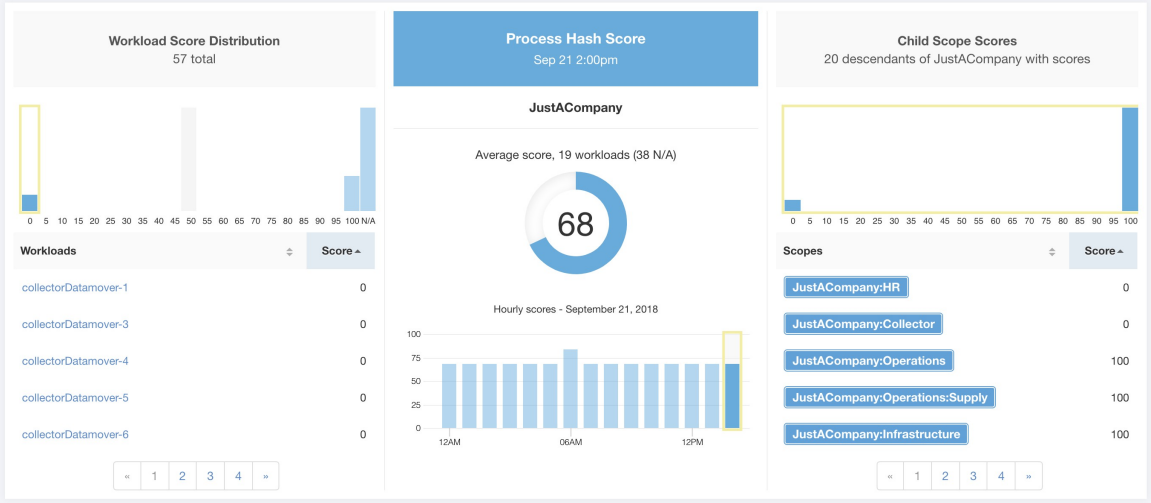
図 *2*: 脆弱性セキュリティスコアのヘルプ




# プロセスハッシュスコア

プロセスハッシュスコアは、ワークロード全体でのプロセスバイナリハッシュ（ファイルハッシュ）の一貫性の評価です。例：同じセットアップ構成から複製された Apache を実行している Web サーバーファームは、すべてのサーバーの httpd バイナリに対して同じハッシュを持つことが期待されるため、不一致の場合は異常です。

**図 *3:* プロセスハッシュスコアの詳細**

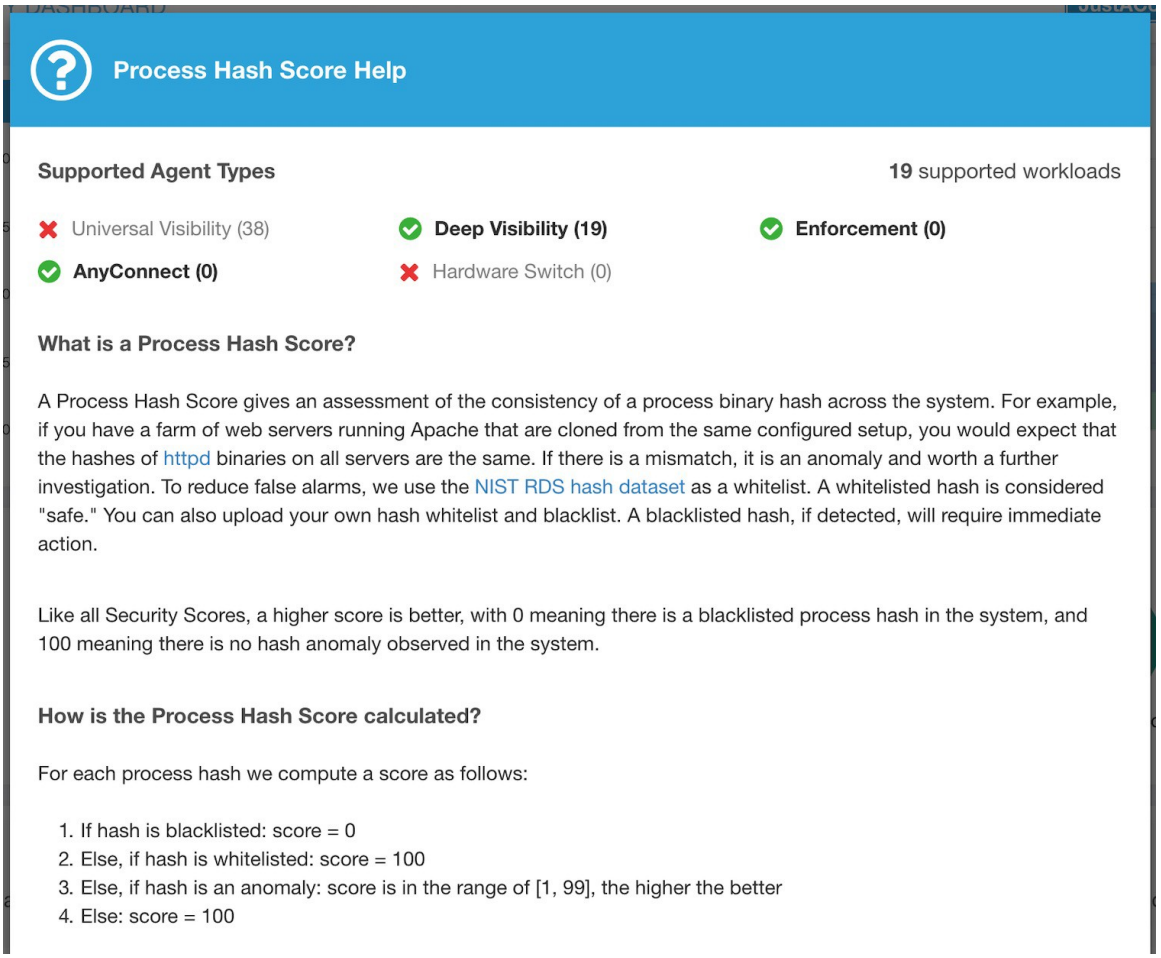



スコアが低い場合、少なくとも次のいずれか 1 つ、または両方に該当します。

- 1 つ以上のプロセスハッシュにフラグが設定されている
- 1 つ以上のプロセスハッシュが異常である

詳細については、「プロセスハッシュの異常検出」を参照してください。

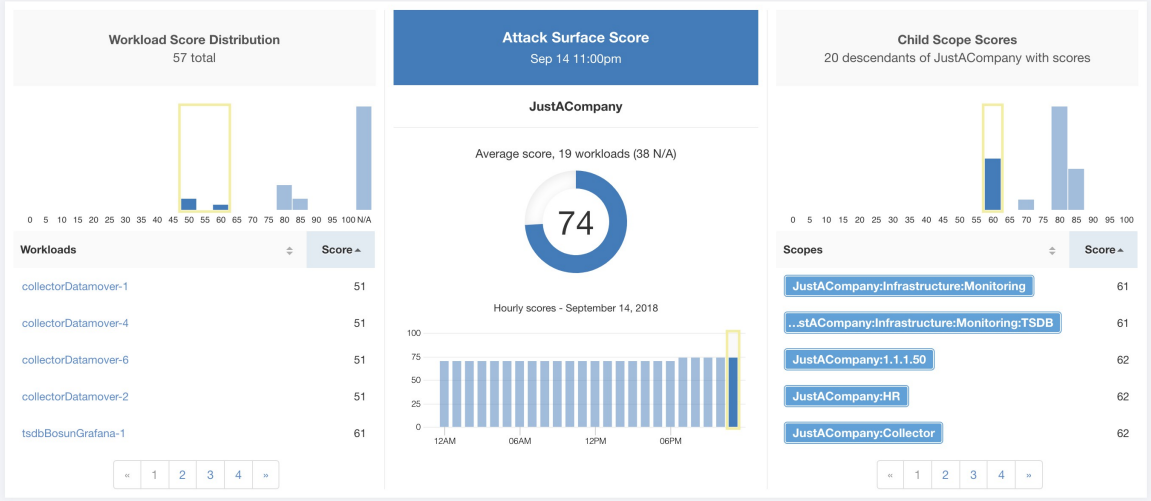
図 *4:* プロセスハッシュスコアに関するヘルプ




# 攻撃対象領域スコア

攻撃対象領域スコアは、ワークロードの潜在的な攻撃対象領域を強調します。未使用のオープンポート（トラフィックのないオープンポート）は、このスコアが低くなります。

**図 5 : 攻撃対象領域スコアの詳細**




低いスコアは次のことを示します。

- 過去 2 週間にトラフィックのないオープンポートが多数ある
- 既知の攻撃対象ポートが、過去 2 週間オープン状態で使用されていない可能性がある
- 1 つ以上のオープンポートが、深刻な脆弱性があるパッケージに割り当てられている

攻撃対象領域スコアは、合計ポートに対する未使用オープンポートの平滑化係数を使用した関数です。過去2週間にトラフィックのないオープンポートは、「未使用のオープンポート」と見なされます。未使用のオープンポートが攻撃で使用された既知のポート（21、22、8080 など）である場合は、追加のペナルティが適用されます。

**図 6 : 攻撃対象領域スコアの計算式**

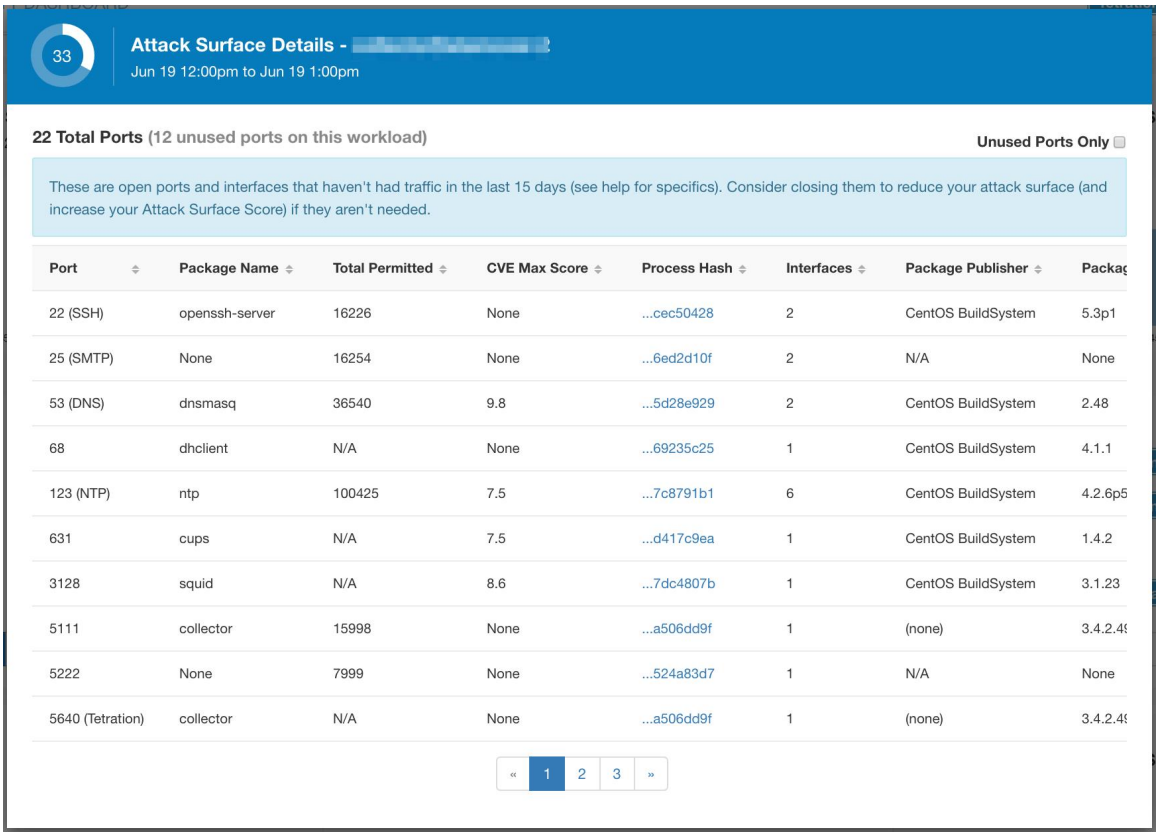
$$Attack\ surface\ score = \frac{\alpha + \sum used\ open\ ports}{\alpha + \sum open\ ports + (\rho * \sum unused\ common\ attack\ ports\ ) + f_v(vulnerablity\ pkgs)}$$

$$f_v = \max\left(\left\{cve_{score} = \begin{cases} CVSS_{V3}, & v3\ exist \\ CVSS_{V2}, & v3\ not\ exist \end{cases}\right\}\right)$$

ラプラススムージングは、ヒューリスティックデータに基づくペナルティ係数とともに使用されます。スコアは、過去 2 週間のデータを使用して毎日計算されます。

テナントスコアは、範囲内のワークロードスコアの平均です。未使用のオープンポートがあるワークロードや範囲を特定し、未使用のポートを閉じることで、スコアを改善します。

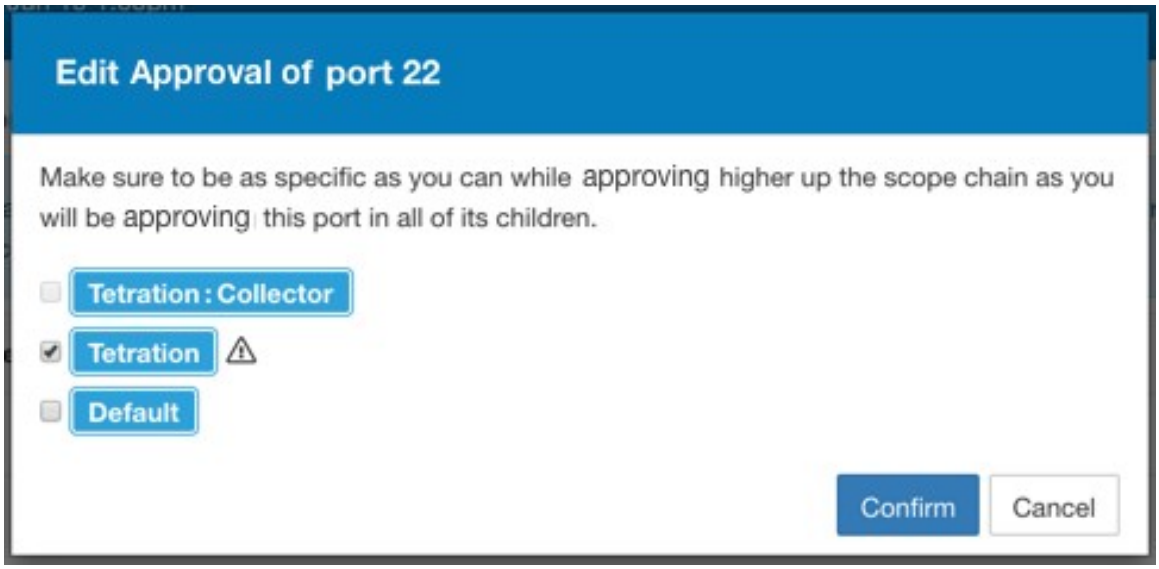
ワークロードリンクをクリックすると、攻撃対象領域モーダルが開き、そのワークロードのコンテキスト内で使用可能なすべてのポートとインターフェイスに関する詳細が表示されます。




機能：

- [未使用のポートのみ（Unused Ports Only）]：チェックボックスをオンにすると、使用中のポートが除外され、ワークロードに関連付けられている未使用ポートのみが表示されます。
- 列：[承認済み（Approved）]、[ポート（Port）]、[パッケージ名（Package Name）]、[合計許可数（Total Permitted]、[CVE最大スコア（CVE Max Score）]、[プロセスハッシュ（Process Hash）]、[インターフェイス（Interfaces）]、[パッケージ発行元（Package Publisher）]、[パッケージバージョン（Package Version）]、[合計エスケープ数（Total Escaped）]、[合計拒否数（Total Rejected）]、[一般的なハッキングポート（Commonly Hacked Port）]、[リンク（Links）]。
- インターフェイス：攻撃対象領域テーブルのいずれかの項目をクリックすると、モーダル内の各ポートに関連付けられているインターフェイスを表示できます（以下のスクリーンショットを参照してください）。
- [承認済み（Approved）]：チェックボックスをオンにすると、ワークロードがアクセスできる範囲チェーンのいずれかの範囲で、意図的に「未使用ポート」を「承認済み」として設定できます。注：ポートが範囲で承認され、そのポートがどの子範囲でも明示的に承認されていない場合（その範囲に子がある場合）、その範囲のチェックボックスは無効になります。親範囲がアクセスできる子範囲が、そのチェーンですでに承認されていることを意味するためです（以下のスクリーンショットを参照してください）。

承認済みモーダル：




インターフェイスモーダル：

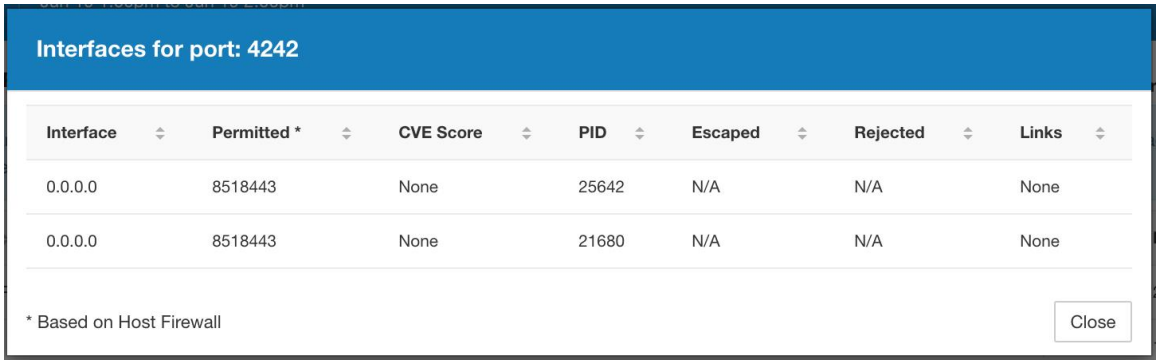
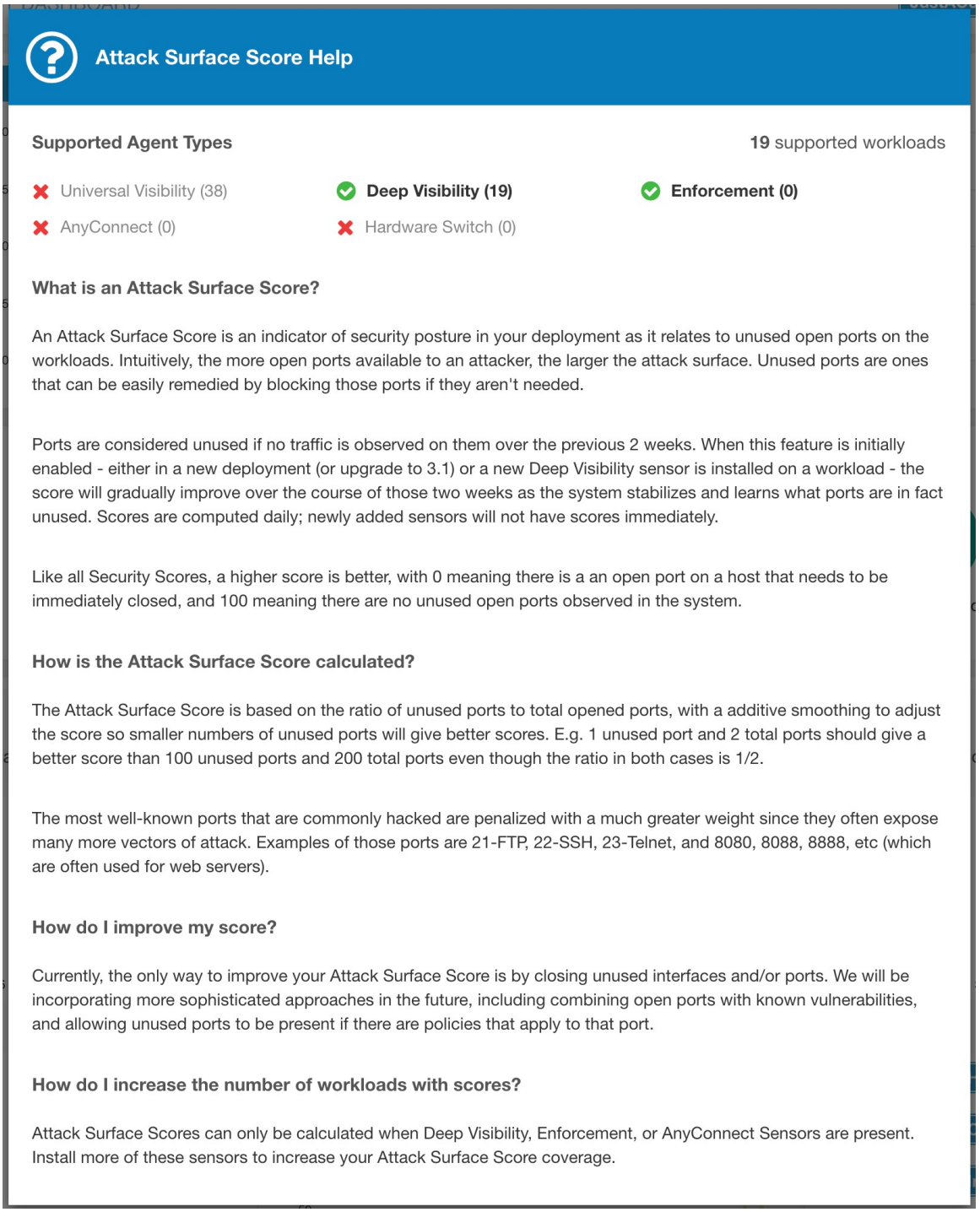


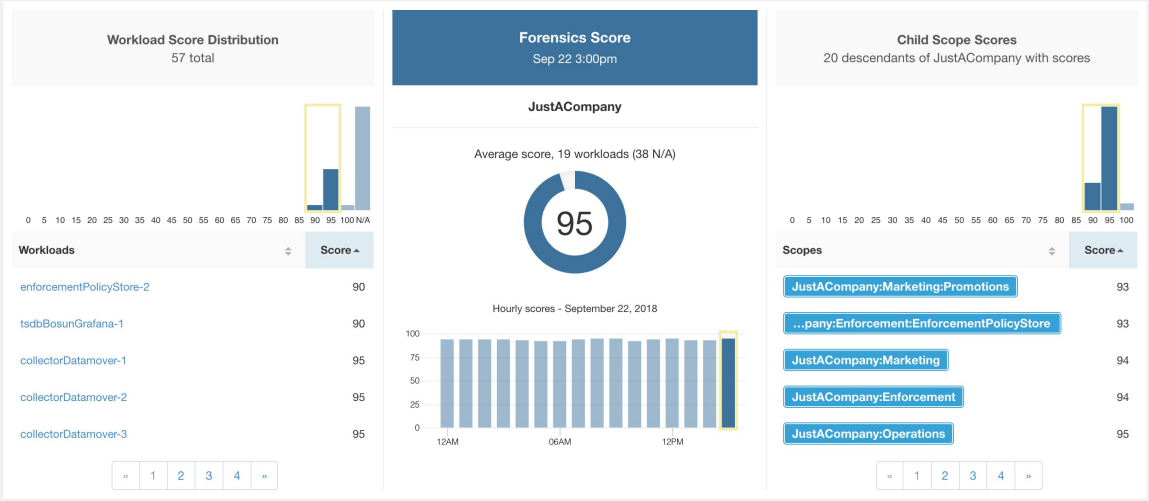
図 *7*:攻撃対象領域スコアに関するヘルプ




# フォレンジックスコア

ワークロードでのフォレンジックイベントの重大度は、このスコアの計算に使用されます。

**図 *8:* フォレンジックスコアの詳細**




低いスコアは次のことを示しています。

- ワークロードで 1 つ以上のフォレンジックイベントが観測された
- あるいは、1 つまたは複数のフォレンジックルールにノイズが多い、および/または正しくない

スコアを改善する方法は次のとおりです。

- 問題があれば修正して、セキュリティリスクやエクスプロイトの可能性を減らす
- フォレンジックルールを微調整して、ノイズと誤報を減らす

ワークロードのフォレンジックスコアは、フォレンジックイベントの総合影響スコアの逆関数です。フォレンジックイベントの総合影響スコアが高いほど、フォレンジックスコアは低くなります。

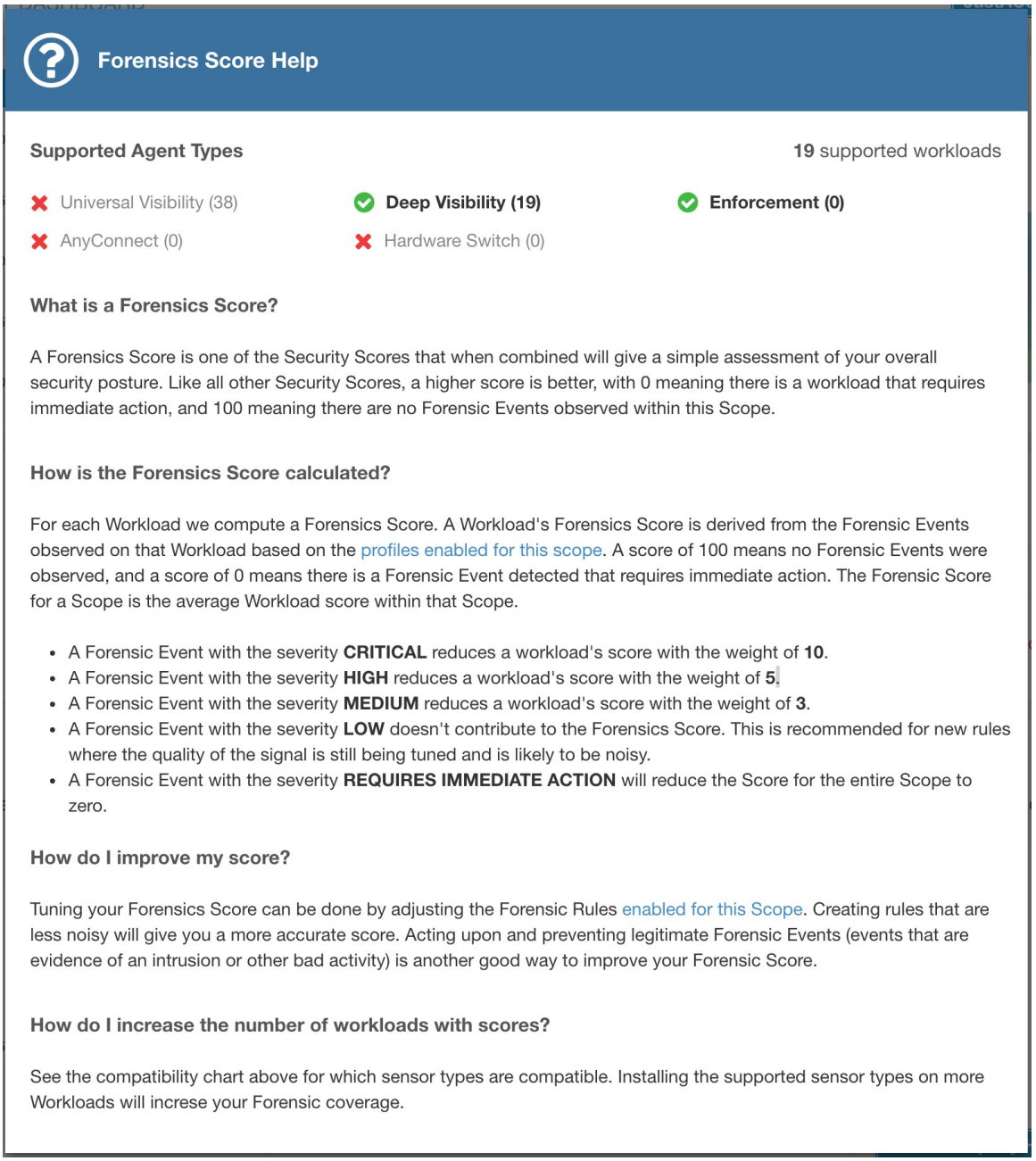
| 重大度 | [Impact Score] |
|---|---|
| IMMEDIATE_ACTION | 100 |
| CRITICAL | 10 |
| HIGH | 5 |
| CRITICAL | 3 |

**図 *9:* フォレンジックスコアの数式**

$$forensics\ score = max\left(0, (100\ -\ \sum forensics\ event\ impact\ score)\right)$$

詳細については、「フォレンジック」を参照してください。

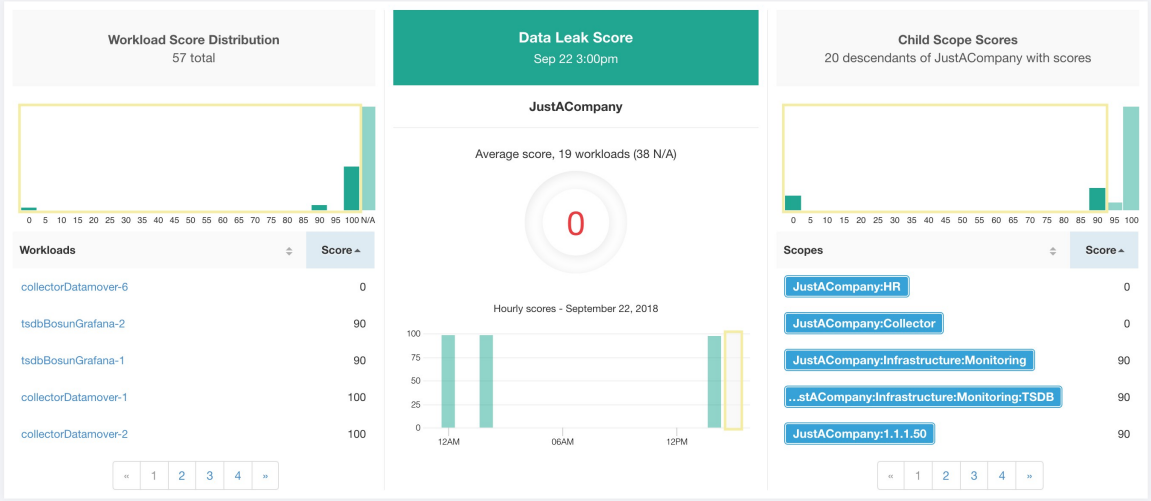
図 *10* : フォレンジックスコアのヘルプ




# ネットワーク異常スコア

ワークロードのネットワーク異常イベントのシビラティ（重大度）は、スコアの計算に使用されます。

**図 *11* : データ リークスコアの詳細**




低いスコアは次のことを示しています。

- ワークロードから異常に大量のデータが転送されている
- またはネットワーク異常フォレンジックルールが正しくないか、ノイズが多い

スコアを改善する方法は次のとおりです。

- 問題があれば修正して、データ漏洩の可能性を減らします
- ネットワーク異常ルールを調整して、ノイズと誤報を減らします

ワークロードのネットワーク異常スコアは、ネットワーク異常イベントの合計シビラティ（重大度）スコアの逆関数です。高い方が合計シビラティ（重大度）スコアで、低い方がネットワーク異常スコアです。

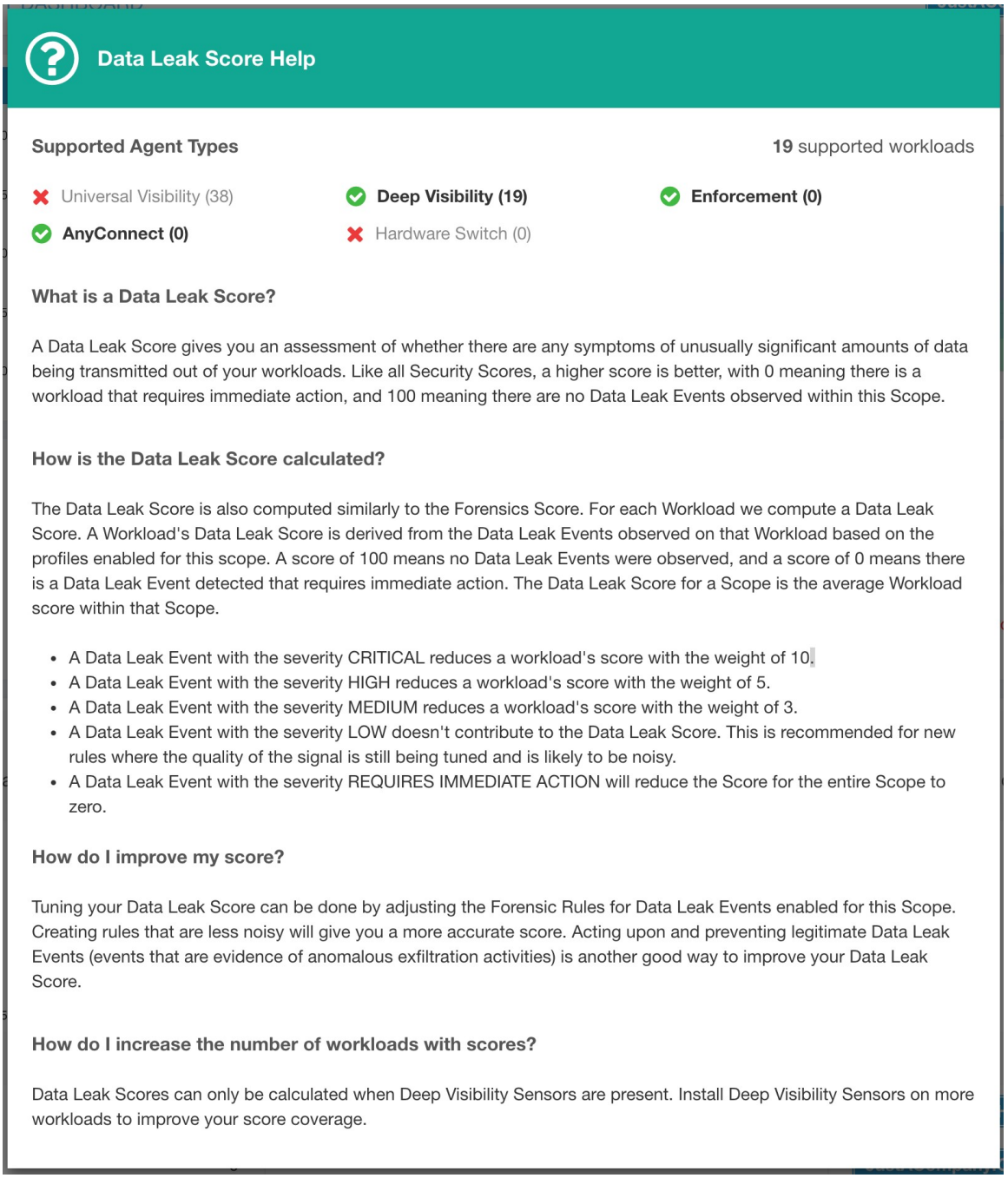
| 重大度 | スコア |
|---|---|
| [即時対応（IMMEDIATE_ACTION）] | 100 |
| CRITICAL | 10 |
| HIGH | 5 |
| CRITICAL | 3 |

**図 *12* : データ リークスコアの数式**

$$data\ leak\ score = max\left(0, (100 - \sum data\ leak\ event\ severity\ score)\right)$$

詳細については、「PCR ベースのネットワーク異常検出」を参照してください。

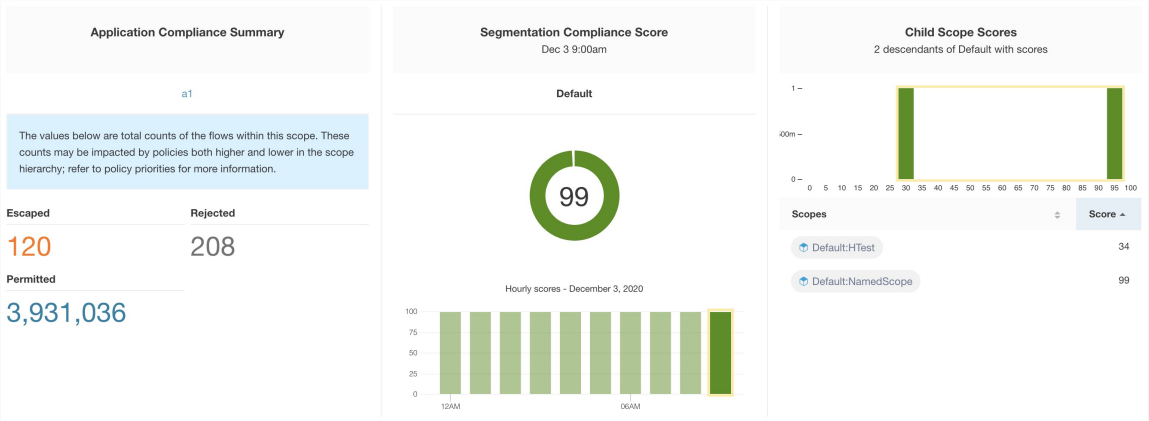
図 *13* : データ リークスコアのヘルプ




# セグメンテーション コンプライアンス スコア

セグメンテーション コンプライアンス スコアには、ポリシー違反のトップレベルのビューが表示され、最も違反が多い範囲とワークスペースが強調表示されます。

**図 *14* : セグメンテーション コンプライアンス スコアの詳細**




（注） ルート範囲のセキュリティダッシュボードに表示される [エスケープ/拒否/許可（Escaped/Rejected/Permitted）] カウントは、すべての子範囲についてそれぞれ表示されるすべてのカウントに加算されません。[エスケープ/拒否/許可（Escaped/Rejected/Permitted）] カウントは、送信元や宛先だけではなく、ポリシーに関する評価です。

低いスコアは次のことを示しています。

- 許可されたフローと比較して、エスケープされたフロー（ポリシー違反）の数がかなり多い
- エスケープされたフローが許可されたフローより多い場合、スコアは 0 になる

セグメンテーション コンプライアンス スコアは、プライマリワークスペースが適用されている範囲に対して計算されます。ワークスペースが適用されていない範囲の場合、スコアは、ポリシーが適用された子孫範囲スコアの平均として計算されます。

スコアは、エスケープされたフローと許可されたフローの比率を使用して計算されます。

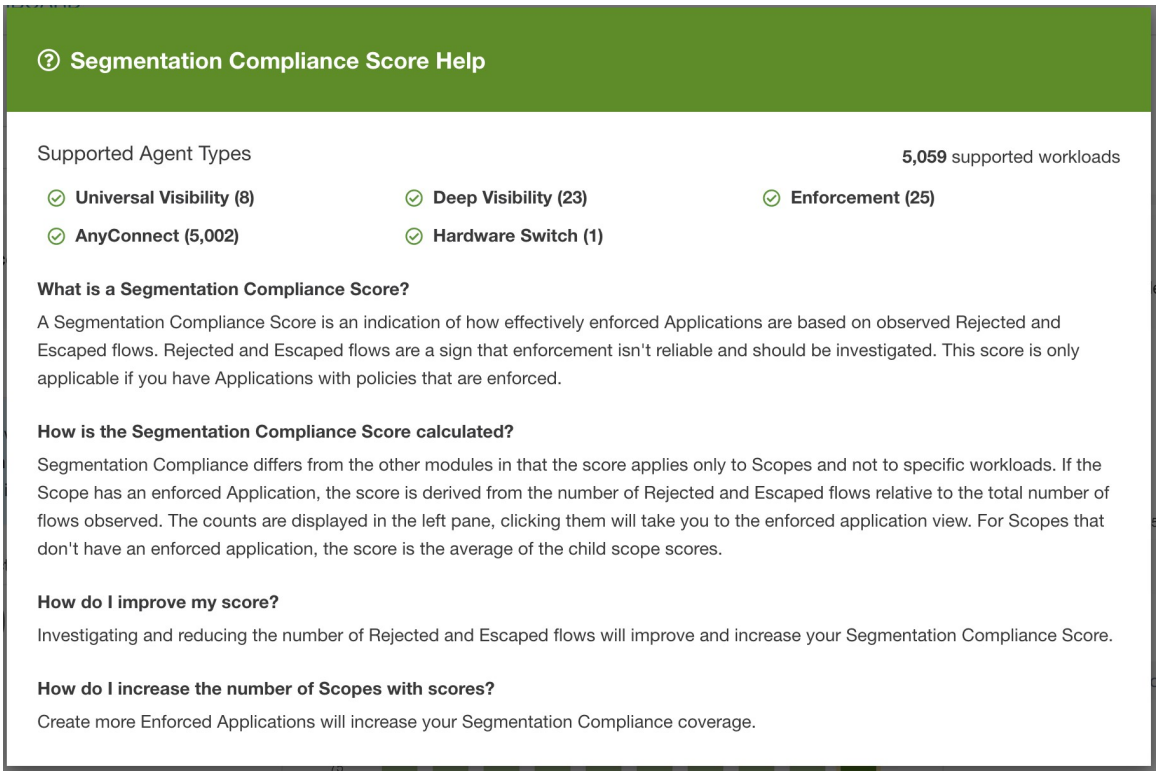
**図 *15* : セグメンテーション コンプライアンス スコアの計算式**

$$compliance\ score = \left\lfloor 100 - \frac{100 \times escaped}{permitted} \right\rfloor$$

ポリシー違反の数を減らしてスコアを向上させる

- ポリシーが目的の動作を正しくカバーしていることを確認する
- ポリシーが正しく適用されていることを確認する

図 *16* : セグメンテーション コンプライアンス スコアの詳細のヘルプ



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。