



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 \(2 ページ\)](#)
- [セキュリティスコア \(2 ページ\)](#)
- [セキュリティスコアのカテゴリ \(2 ページ\)](#)
- [ハイレベルビュー \(3 ページ\)](#)
- [範囲レベルスコアの詳細 \(3 ページ\)](#)
- [スコアの詳細 \(5 ページ\)](#)

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。

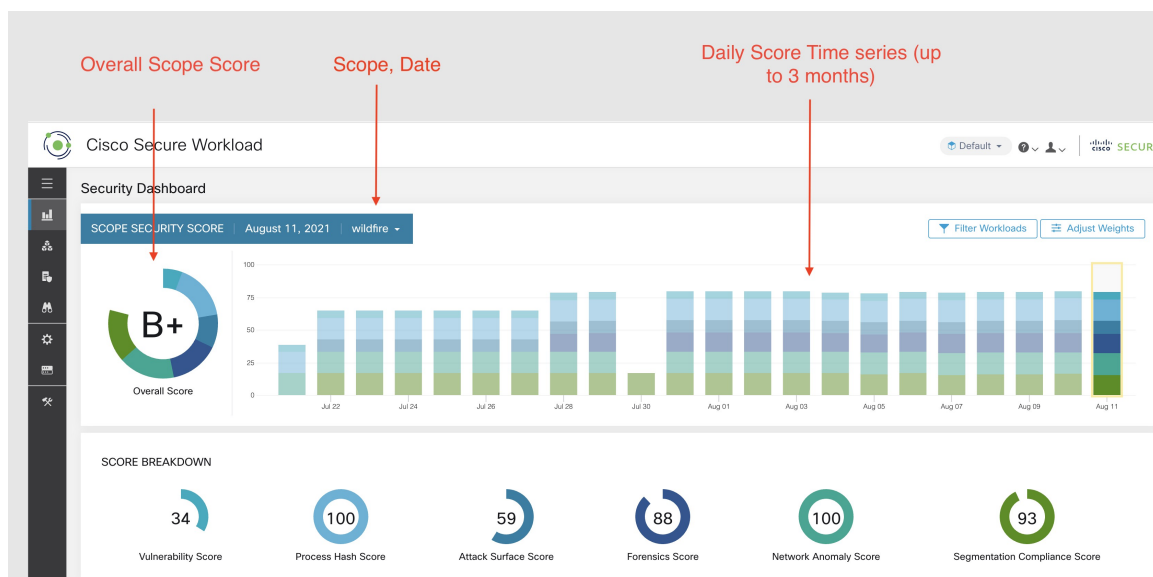
- [セグメンテーションコンプライアンススコア (Segmentation Compliance Score)] : 自動的に検出されたポリシーに対する遵守 (許可) および違反 (エスケープ) がスコアリングに使用されます。

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。

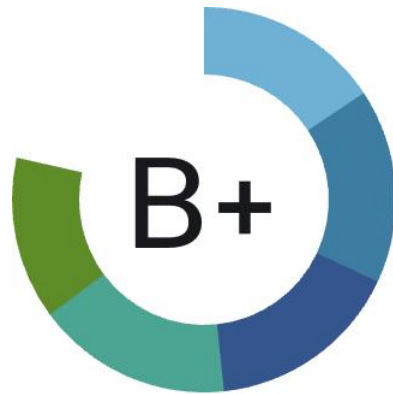


以下の内容が表示されます。

- 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。

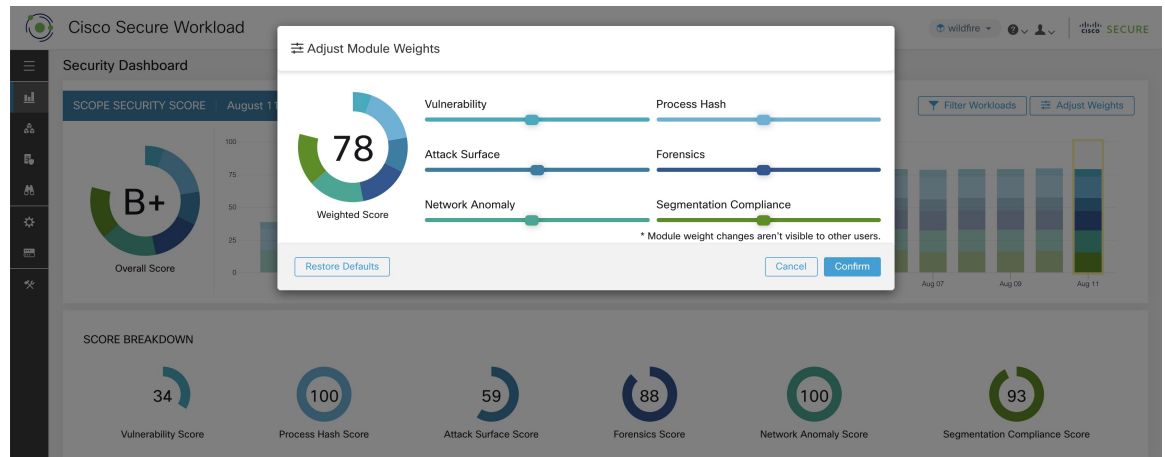


Overall Score

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。

$$\text{Overall score} = \frac{\sum W_{\text{category}} \times \text{Score}_{\text{category}}}{\sum W_{\text{category}}}$$

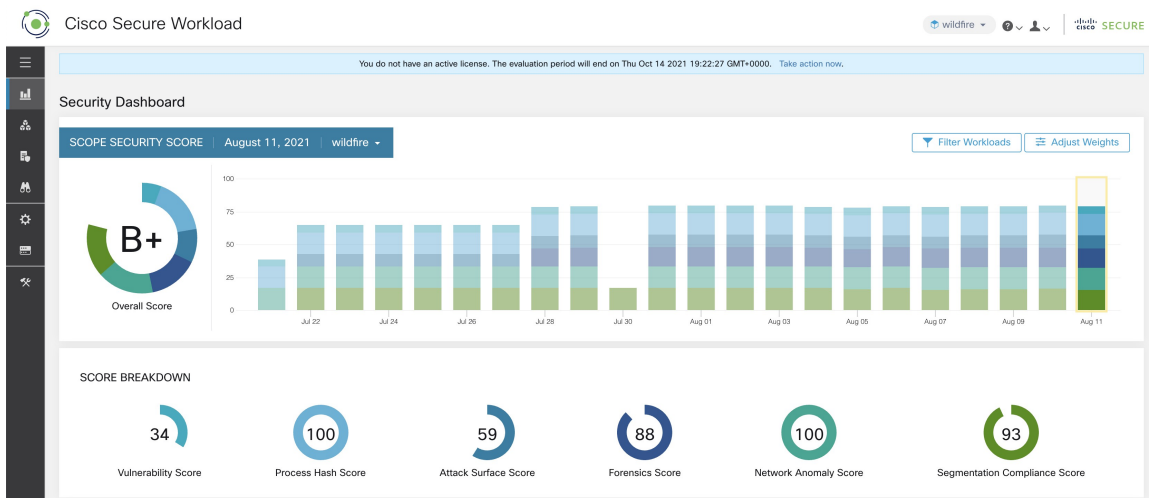
重みは、**重みの調整**モジュールのスライドを使用して調整できます。ユーザーごとに独自の重み調整を設定できるため、スコアをユーザーの優先順位に合わせるすることができます。



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。

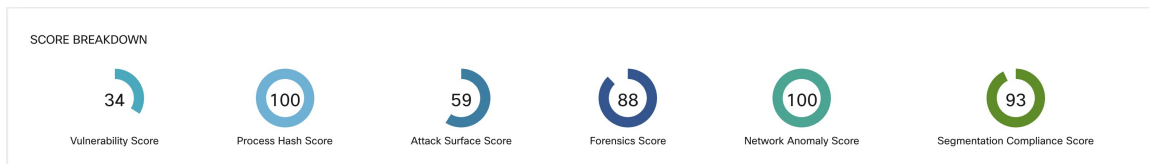
日次時系列

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

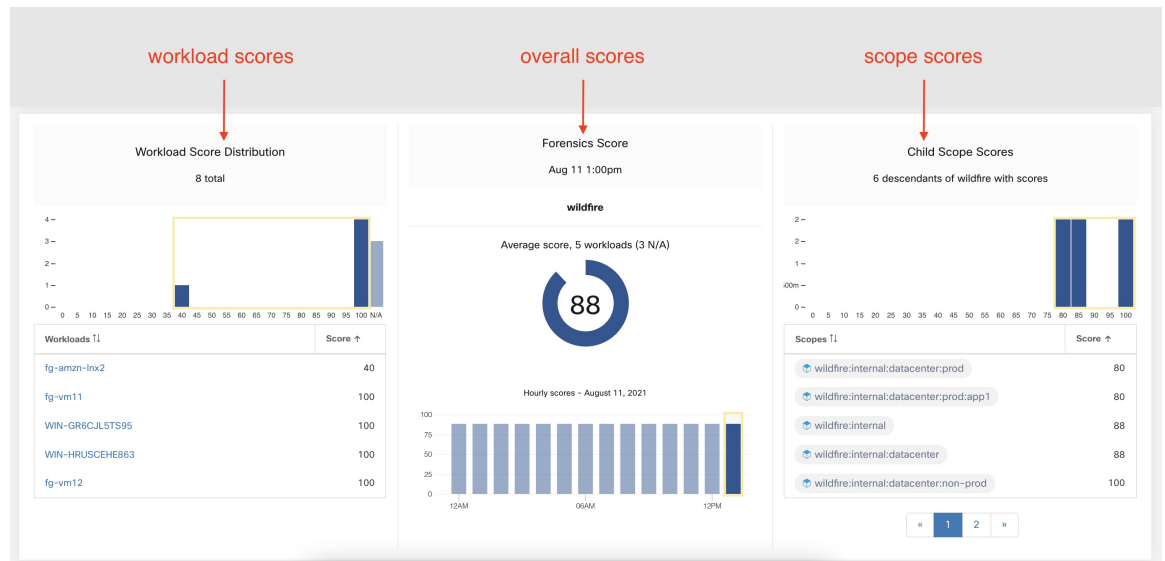
[Score Breakdown (スコアの内訳)]には、時系列で選択された日の6つのカテゴリすべてのスコアが表示されます。スコア **N/A** は、スコアが利用できないことを示します。全体のスコア計算では **0** としてカウントされます。



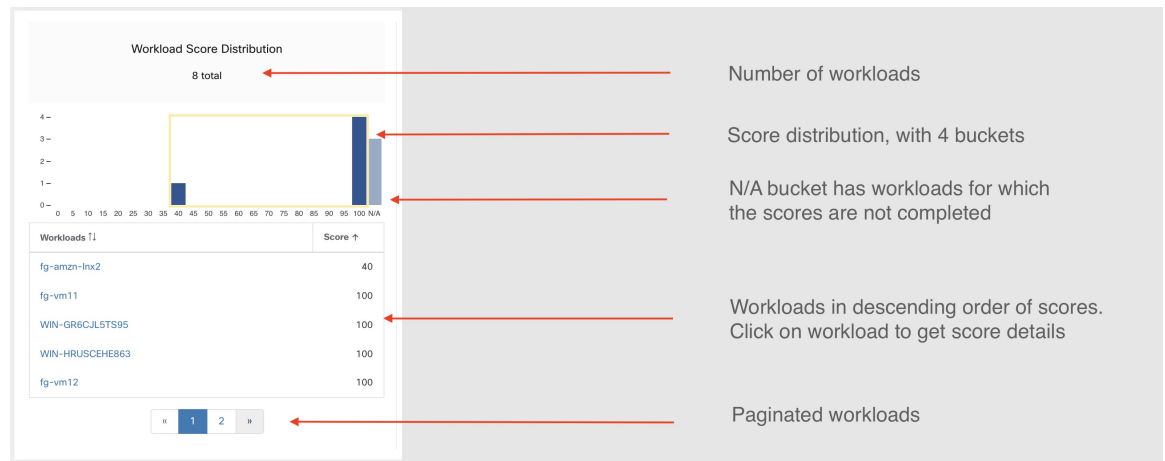
重要: スコアが **N/A** の場合、全体のスコア計算では **0** と見なされます。

スコアの詳細

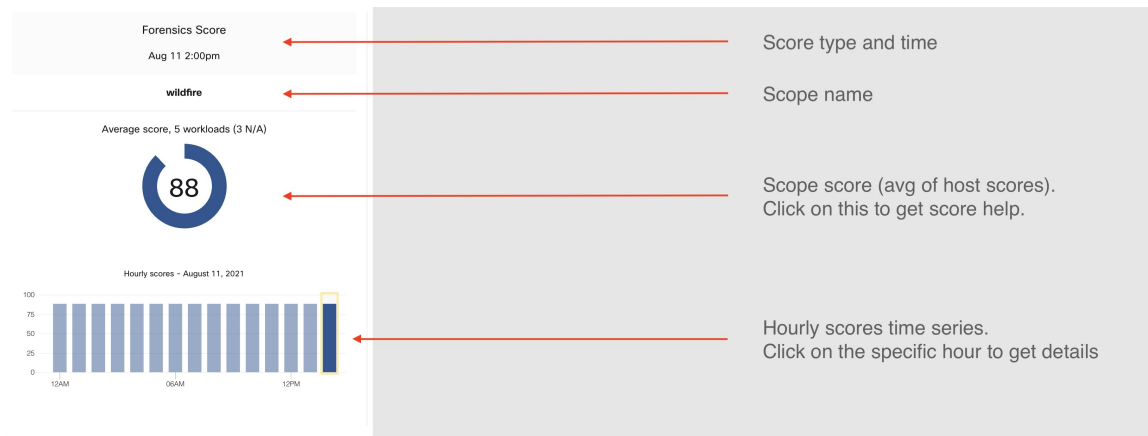
6つのカテゴリは、それぞれ次のテンプレートに従います。テンプレートには、ワークロードスコアの分布、1時間ごとの時系列、および子範囲のスコア分布があります。



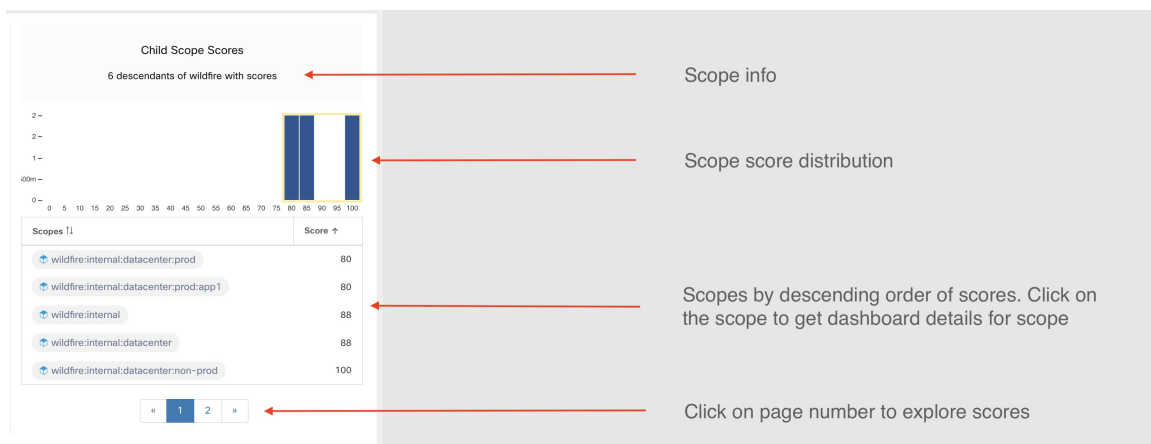
ワークロードスコアの分布では、選択した範囲の下のワークロードからのスコアの貢献度についての分析情報が得られます。分析情報により、最も低いスコアのワークロードをバブルアップして修正措置を迅速化するのに役立ちます。



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。

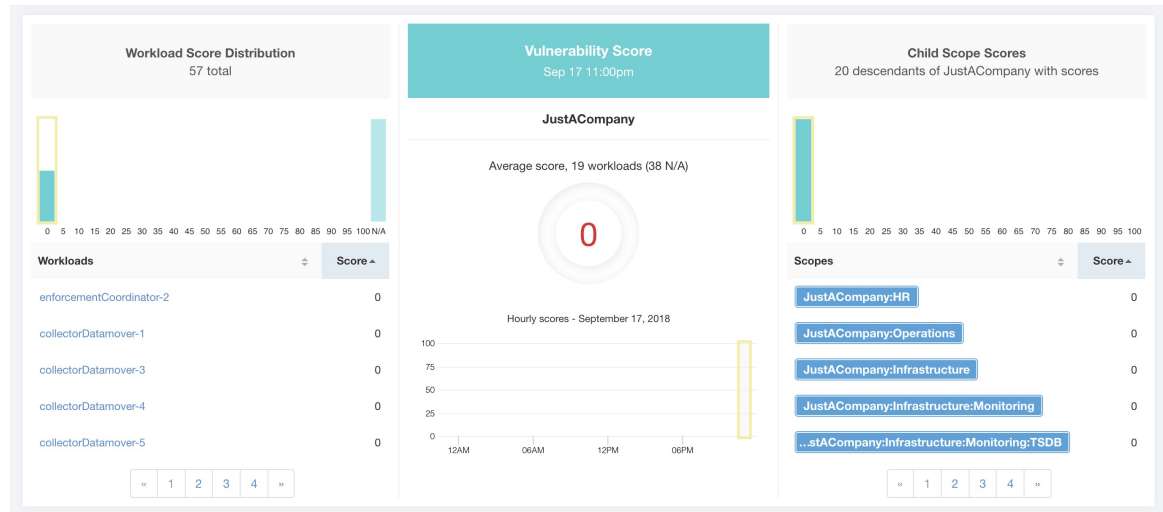


このセクションでは、各スコアカテゴリの詳細について説明します。

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

? **Vulnerability Score Help**

Supported Agent Types 19 supported workloads

✗ Universal Visibility (38)	✔ Deep Visibility (19)	✔ Enforcement (0)
✗ AnyConnect (0)	✗ Hardware Switch (0)	

What is a Vulnerability Score?

A Vulnerability Score is an indicator of security posture in your deployment as it relates to software package vulnerabilities. We use standard [Common Vulnerability Scoring System](#) (CVSS score) to assess the impact of a vulnerability. The Vulnerability Score is calculated based on CVSS scores of vulnerabilities detected on a workload. Like all other Security Scores, a higher score is better, with 0 meaning there is a workload that requires immediate action, and 100 meaning there are no vulnerable packages observed within this Scope.

How is the Vulnerability Score calculated?

A Workload's Vulnerability Score is derived from the scores of vulnerable software detected on that workload. We use the vulnerable package's CVSS score to assess the impact of a vulnerability. Vulnerability score of a workload depends on the most severe vulnerability present in the system; higher the severity of most severe vulnerability, lower is the workload's score. The Vulnerability Score for a Scope is the average Vulnerability score of all workloads within that Scope.

How do I improve my score?

Updating software packages on the most vulnerable workloads to versions without (or with less severe) vulnerabilities is the best way to improve the score.

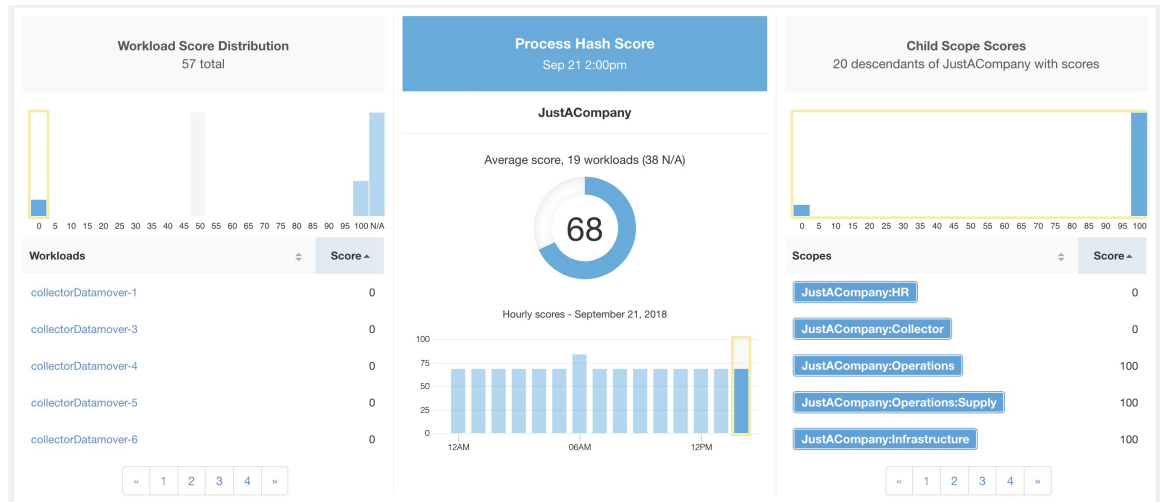
How do I increase the number of workloads with scores?

Vulnerability Scores can only be calculated when Deep Visibility Sensors are present. Install Deep Visibility Sensors on more workloads to improve your score coverage.

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

Supported Agent Types 19 supported workloads

✗ Universal Visibility (38)	✓ Deep Visibility (19)	✓ Enforcement (0)
✓ AnyConnect (0)	✗ Hardware Switch (0)	

What is a Process Hash Score?

A Process Hash Score gives an assessment of the consistency of a process binary hash across the system. For example, if you have a farm of web servers running Apache that are cloned from the same configured setup, you would expect that the hashes of [httpd](#) binaries on all servers are the same. If there is a mismatch, it is an anomaly and worth a further investigation. To reduce false alarms, we use the [NIST RDS hash dataset](#) as a whitelist. A whitelisted hash is considered "safe." You can also upload your own hash whitelist and blacklist. A blacklisted hash, if detected, will require immediate action.

Like all Security Scores, a higher score is better, with 0 meaning there is a blacklisted process hash in the system, and 100 meaning there is no hash anomaly observed in the system.

How is the Process Hash Score calculated?

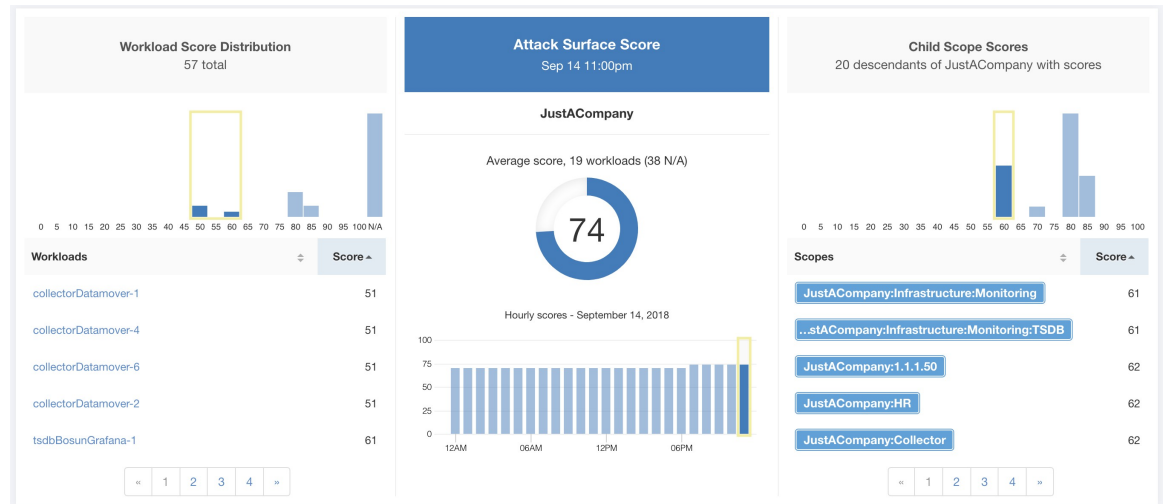
For each process hash we compute a score as follows:

1. If hash is blacklisted: score = 0
2. Else, if hash is whitelisted: score = 100
3. Else, if hash is an anomaly: score is in the range of [1, 99], the higher the better
4. Else: score = 100

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

$$= \frac{\alpha + \sum \text{used open ports}}{\alpha + \sum \text{open ports} + (\rho * \sum \text{unused common attack ports}) + f_v(\text{vulnerability pkgs})}$$

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

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。

33
Attack Surface Details - XXXXXXXXXX
Jun 19 12:00pm to Jun 19 1:00pm

22 Total Ports (12 unused ports on this workload) Unused Ports Only

These are open ports and interfaces that haven't had traffic in the last 15 days (see help for specifics). Consider closing them to reduce your attack surface (and increase your Attack Surface Score) if they aren't needed.

Port	Package Name	Total Permitted	CVE Max Score	Process Hash	Interfaces	Package Publisher	Package Version
22 (SSH)	openssh-server	16226	None	...cec50428	2	CentOS BuildSystem	5.3p1
25 (SMTP)	None	16254	None	...6ed2d10f	2	N/A	None
53 (DNS)	dnsmasq	36540	9.8	...5d28e929	2	CentOS BuildSystem	2.48
68	dhclient	N/A	None	...69235c25	1	CentOS BuildSystem	4.1.1
123 (NTP)	ntp	100425	7.5	...7c8791b1	6	CentOS BuildSystem	4.2.6p5
631	cups	N/A	7.5	...d417c9ea	1	CentOS BuildSystem	1.4.2
3128	squid	N/A	8.6	...7dc4807b	1	CentOS BuildSystem	3.1.23
5111	collector	15998	None	...a506dd9f	1	(none)	3.4.2.4f
5222	None	7999	None	...524a83d7	1	N/A	None
5640 (Tetration)	collector	N/A	None	...a506dd9f	1	(none)	3.4.2.4f

« 1 2 3 »

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 :

Edit Approval of port 22

Make sure to be as specific as you can while approving higher up the scope chain as you will be approving this port in all of its children.

- Tetration : Collector
- Tetration ⚠
- Default

Confirm
Cancel

インターフェイスモーダル :

Interfaces for port: 4242

Interface	Permitted *	CVE Score	PID	Escaped	Rejected	Links
0.0.0.0	8518443	None	25642	N/A	N/A	None
0.0.0.0	8518443	None	21680	N/A	N/A	None

* Based on Host Firewall

Close

図 7: 攻撃対象領域スコアに関するヘルプ

?

Attack Surface Score Help

Supported Agent Types 19 supported workloads

✗ Universal Visibility (38)	✔ Deep Visibility (19)	✔ Enforcement (0)
✗ AnyConnect (0)	✗ Hardware Switch (0)	

What is an Attack Surface Score?

An Attack Surface Score is an indicator of security posture in your deployment as it relates to unused open ports on the workloads. Intuitively, the more open ports available to an attacker, the larger the attack surface. Unused ports are ones that can be easily remedied by blocking those ports if they aren't needed.

Ports are considered unused if no traffic is observed on them over the previous 2 weeks. When this feature is initially enabled - either in a new deployment (or upgrade to 3.1) or a new Deep Visibility sensor is installed on a workload - the score will gradually improve over the course of those two weeks as the system stabilizes and learns what ports are in fact unused. Scores are computed daily; newly added sensors will not have scores immediately.

Like all Security Scores, a higher score is better, with 0 meaning there is an open port on a host that needs to be immediately closed, and 100 meaning there are no unused open ports observed in the system.

How is the Attack Surface Score calculated?

The Attack Surface Score is based on the ratio of unused ports to total opened ports, with a additive smoothing to adjust the score so smaller numbers of unused ports will give better scores. E.g. 1 unused port and 2 total ports should give a better score than 100 unused ports and 200 total ports even though the ratio in both cases is 1/2.

The most well-known ports that are commonly hacked are penalized with a much greater weight since they often expose many more vectors of attack. Examples of those ports are 21-FTP, 22-SSH, 23-Telnet, and 8080, 8088, 8888, etc (which are often used for web servers).

How do I improve my score?

Currently, the only way to improve your Attack Surface Score is by closing unused interfaces and/or ports. We will be incorporating more sophisticated approaches in the future, including combining open ports with known vulnerabilities, and allowing unused ports to be present if there are policies that apply to that port.

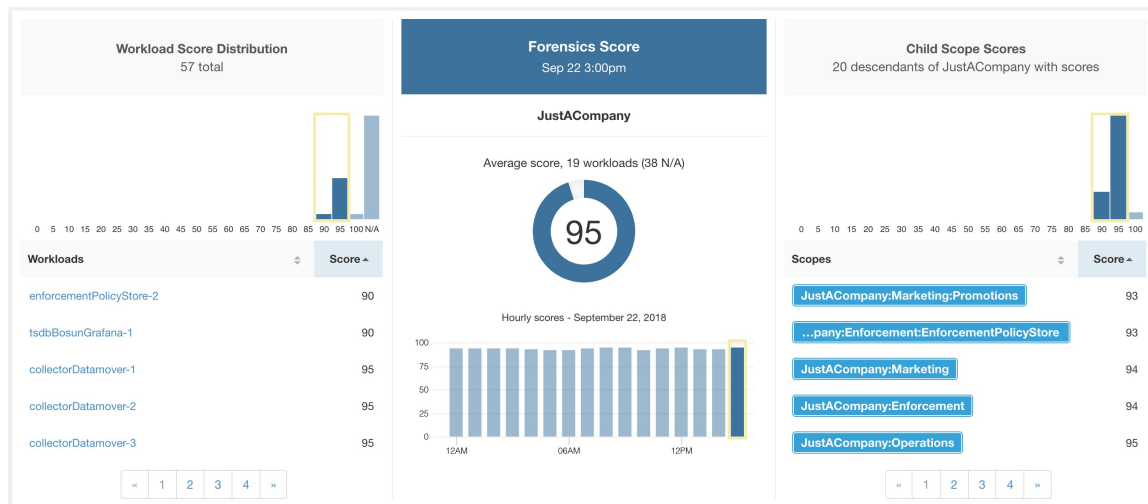
How do I increase the number of workloads with scores?

Attack Surface Scores can only be calculated when Deep Visibility, Enforcement, or AnyConnect Sensors are present. Install more of these sensors to increase your Attack Surface Score coverage.

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

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

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

? **Forensics Score Help**

Supported Agent Types 19 supported workloads

<p>✗ Universal Visibility (38)</p> <p>✗ AnyConnect (0)</p>	<p>✔ Deep Visibility (19)</p> <p>✗ Hardware Switch (0)</p>	<p>✔ Enforcement (0)</p>
------------------------------------------------------------	------------------------------------------------------------	--------------------------

What is a Forensics Score?

A Forensics Score is one of the Security Scores that when combined will give a simple assessment of your overall security posture. Like all other Security Scores, a higher score is better, with 0 meaning there is a workload that requires immediate action, and 100 meaning there are no Forensic Events observed within this Scope.

How is the Forensics Score calculated?

For each Workload we compute a Forensics Score. A Workload's Forensics Score is derived from the Forensic Events observed on that Workload based on the [profiles enabled for this scope](#). A score of 100 means no Forensic Events were observed, and a score of 0 means there is a Forensic Event detected that requires immediate action. The Forensic Score for a Scope is the average Workload score within that Scope.

- A Forensic Event with the severity **CRITICAL** reduces a workload's score with the weight of **10**.
- A Forensic Event with the severity **HIGH** reduces a workload's score with the weight of **5**.
- A Forensic Event with the severity **MEDIUM** reduces a workload's score with the weight of **3**.
- A Forensic Event with the severity **LOW** doesn't contribute to the Forensics Score. This is recommended for new rules where the quality of the signal is still being tuned and is likely to be noisy.
- A Forensic Event with the severity **REQUIRES IMMEDIATE ACTION** will reduce the Score for the entire Scope to zero.

How do I improve my score?

Tuning your Forensics Score can be done by adjusting the Forensic Rules [enabled for this Scope](#). Creating rules that are less noisy will give you a more accurate score. Acting upon and preventing legitimate Forensic Events (events that are evidence of an intrusion or other bad activity) is another good way to improve your Forensic Score.

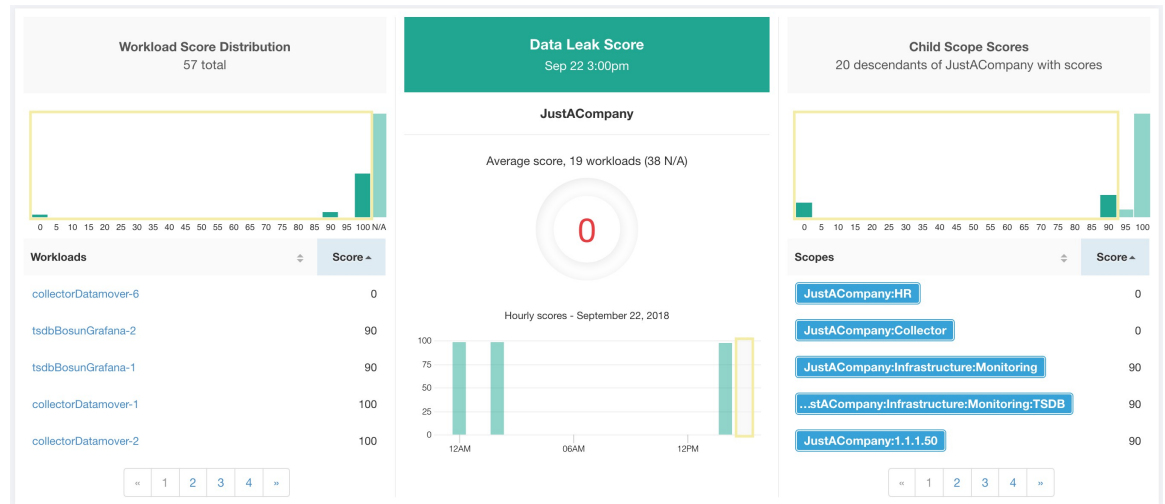
How do I increase the number of workloads with scores?

See the compatibility chart above for which sensor types are compatible. Installing the supported sensor types on more Workloads will increase your Forensic coverage.

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

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

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

?
Data Leak Score Help

Supported Agent Types 19 supported workloads

✗ Universal Visibility (38)	✔ Deep Visibility (19)	✔ Enforcement (0)
✔ AnyConnect (0)	✗ Hardware Switch (0)	

What is a Data Leak Score?

A Data Leak Score gives you an assessment of whether there are any symptoms of unusually significant amounts of data being transmitted out of your workloads. Like all Security Scores, a higher score is better, with 0 meaning there is a workload that requires immediate action, and 100 meaning there are no Data Leak Events observed within this Scope.

How is the Data Leak Score calculated?

The Data Leak Score is also computed similarly to the Forensics Score. For each Workload we compute a Data Leak Score. A Workload's Data Leak Score is derived from the Data Leak Events observed on that Workload based on the profiles enabled for this scope. A score of 100 means no Data Leak Events were observed, and a score of 0 means there is a Data Leak Event detected that requires immediate action. The Data Leak Score for a Scope is the average Workload score within that Scope.

- A Data Leak Event with the severity CRITICAL reduces a workload's score with the weight of 10.
- A Data Leak Event with the severity HIGH reduces a workload's score with the weight of 5.
- A Data Leak Event with the severity MEDIUM reduces a workload's score with the weight of 3.
- A Data Leak Event with the severity LOW doesn't contribute to the Data Leak Score. This is recommended for new rules where the quality of the signal is still being tuned and is likely to be noisy.
- A Data Leak Event with the severity REQUIRES IMMEDIATE ACTION will reduce the Score for the entire Scope to zero.

How do I improve my score?

Tuning your Data Leak Score can be done by adjusting the Forensic Rules for Data Leak Events enabled for this Scope. Creating rules that are less noisy will give you a more accurate score. Acting upon and preventing legitimate Data Leak Events (events that are evidence of anomalous exfiltration activities) is another good way to improve your Data Leak Score.

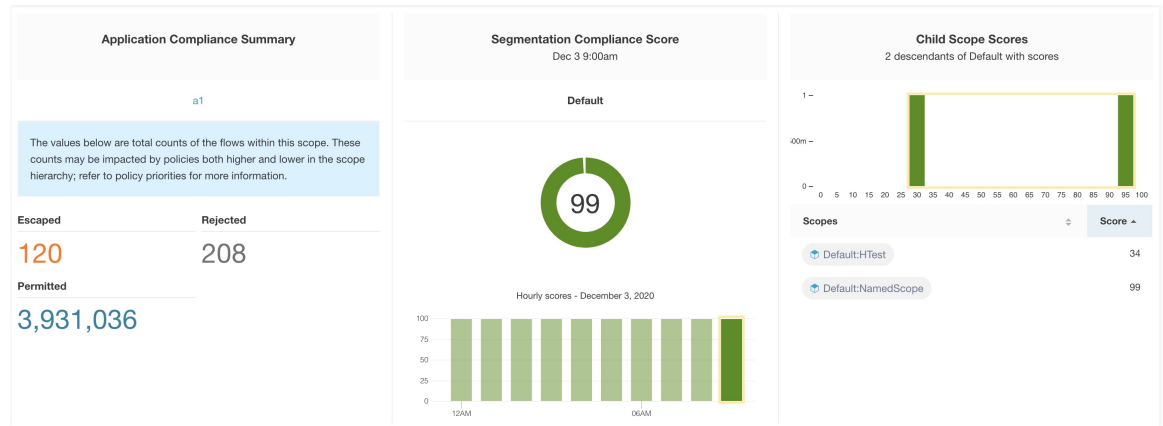
How do I increase the number of workloads with scores?

Data Leak Scores can only be calculated when Deep Visibility Sensors are present. Install Deep Visibility Sensors on more workloads to improve your score coverage.

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

$$\text{compliance score} = \left[100 - \frac{100 \times \text{escaped}}{\text{permitted}} \right]$$

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

Segmentation Compliance Score Help

Supported Agent Types 5,059 supported workloads

- ✔ Universal Visibility (8)
- ✔ AnyConnect (5,002)
- ✔ Deep Visibility (23)
- ✔ Hardware Switch (1)
- ✔ Enforcement (25)

What is a Segmentation Compliance Score?

A Segmentation Compliance Score is an indication of how effectively enforced Applications are based on observed Rejected and Escaped flows. Rejected and Escaped flows are a sign that enforcement isn't reliable and should be investigated. This score is only applicable if you have Applications with policies that are enforced.

How is the Segmentation Compliance Score calculated?

Segmentation Compliance differs from the other modules in that the score applies only to Scopes and not to specific workloads. If the Scope has an enforced Application, the score is derived from the number of Rejected and Escaped flows relative to the total number of flows observed. The counts are displayed in the left pane, clicking them will take you to the enforced application view. For Scopes that don't have an enforced application, the score is the average of the child scope scores.

How do I improve my score?

Investigating and reducing the number of Rejected and Escaped flows will improve and increase your Segmentation Compliance Score.

How do I increase the number of Scopes with scores?

Create more Enforced Applications will increase your Segmentation Compliance coverage.

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。