



Afficher le Tableau de bord de sécurité

Ce chapitre fournit des informations sur la note de sécurité, les catégories de note de sécurité et les détails de la note au niveau de la portée présentés dans le tableau de bord de sécurité.

Le tableau de bord de la sécurité présente des évaluations de sécurité exploitables en rassemblant plusieurs signaux disponibles dans Cisco Secure Workload, ce qui aide à comprendre la position actuelle de la sécurité et à l'améliorer. Le tableau de bord de la sécurité sert de tremplin vers de nombreuses analyses plus approfondies dans Cisco Secure Workload, telles que la recherche de flux, la recherche d'inventaire, la découverte automatique des politiques et la criminalistique.

- [Afficher le Tableau de bord de sécurité, on page 1](#)
- [Note de sécurité, on page 2](#)
- [Catégories de notes de sécurité, on page 2](#)
- [Vue générale, on page 2](#)
- [Détails de la note au niveau de la portée, on page 2](#)
- [Détails de la note, on page 5](#)

Afficher le Tableau de bord de sécurité

Pour afficher le Tableau de bord de sécurité, dans le volet de navigation, choisissez **Overview** (Aperçu).

Note de sécurité

La note de sécurité est un nombre compris entre 0 et 100 et indiquant la position de sécurité dans une catégorie. Une note de 100 est la meilleure note et une note de 0 est la pire. Les notes proches de 100 sont les meilleures.

Le calcul de la note de sécurité prend en compte les vulnérabilités des logiciels installés, la cohérence des condensés de processus, les ports ouverts sur différentes interfaces, les événements criminalistiques et d'anomalies de réseau, et la conformité ou la non-conformité aux politiques.

Catégories de notes de sécurité

Il existe six catégories de notes différentes. La plupart des aspects de sécurité d'une charge de travail sont pris en compte pour déterminer ces catégories.

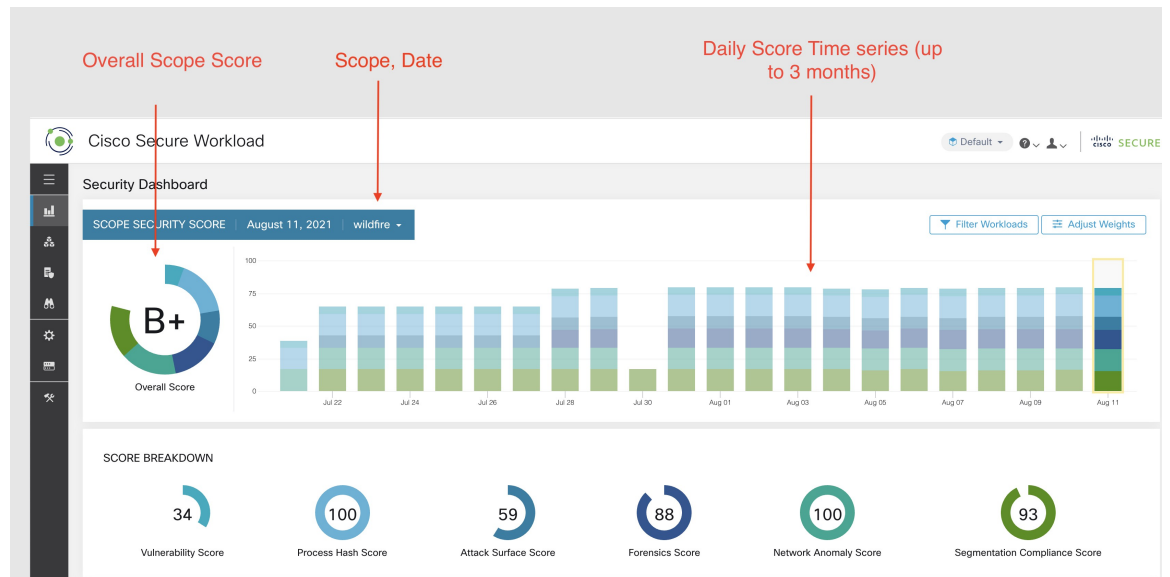
- **Note de vulnérabilité** : les vulnérabilités des paquets installés sur une charge de travail sont utilisées pour l'évaluation.
- **Note de condensé de processus** : La cohérence (et l'anomalie) des condensés de processus ainsi que des condensés de processus bénins et marqués sont utilisées pour l'évaluation.
- **Note de la surface d'attaque** : le processus peut avoir un ou plusieurs ports ouverts sur plusieurs interfaces pour rendre les services disponibles. Les ports ouverts inutilisés sont utilisés pour l'évaluation.
- **Note criminalistique** : la gravité des événements criminalistiques sur une charge de travail est utilisée pour l'évaluation.
- **Note d'anomalie de réseau** : la gravité des événements d'anomalie de réseau sur une charge de travail est utilisée pour l'évaluation.
- **Note de conformité de la segmentation** : la conformité (politiques autorisées) et les violations (politiques échappées) des politiques découvertes automatiquement sont utilisées pour l'évaluation.

Vue générale

Le tableau de bord de sécurité dispose de notes au niveau de la portée sélectionnée. Il existe une note globale avec des séries chronologiques et une ventilation des notes. Les détails des notes pour les six catégories de notes de la portée sélectionnée s'affichent.

Détails de la note au niveau de la portée

Les détails de la note au niveau de la portée s'affichent en haut du tableau de bord.

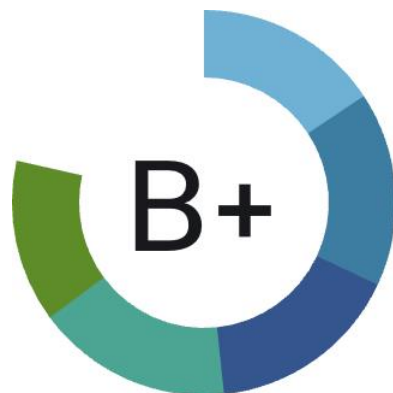


Les renseignements détaillés suivants sont affichés :

- **Note globale de la portée** : note globale de la portée sélectionnée.
- **Séries chronologiques de notes quotidiennes** : séries chronologiques empilées pouvant aller jusqu'à 3 mois.
- **Répartition des notes** : répartition des notes des catégories pour la journée sélectionnée de la série chronologique.

Note globale

La note globale est représentée par une lettre de **A+**, **A**, ..., **F**, **A+** étant considéré comme la meilleure note et **F** comme la plus mauvaise. Elle est affichée sous forme de graphique en anneau, chaque tranche (représentée par un code de couleur) représentant une catégorie de note.

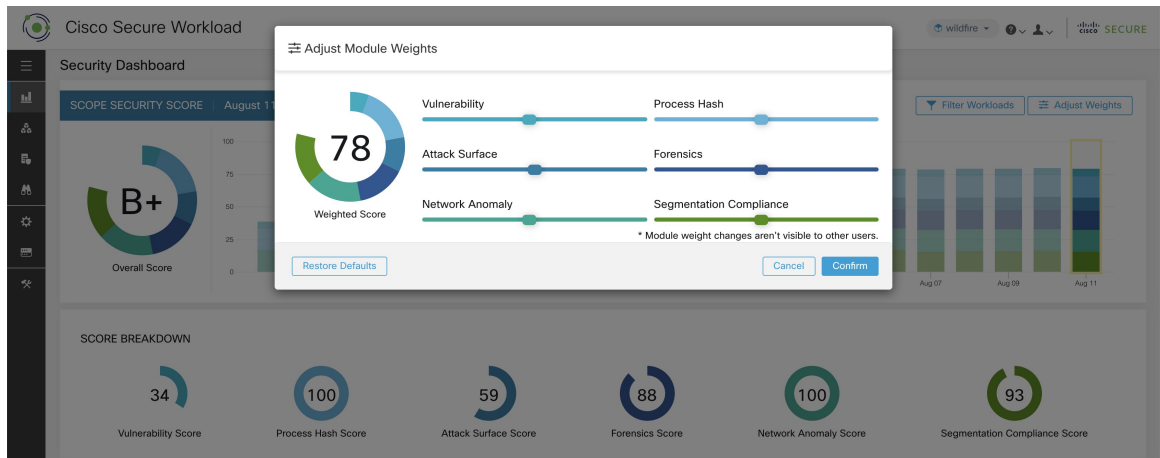


Overall Score

La note globale correspond à la moyenne pondérée des six catégories de note. Par défaut, toutes les pondérations sont égales. Si une note est **S.O.**, elle est considérée comme à 0 dans le calcul de la note globale.

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

La pondération peut être ajustée à l'aide des curseurs du module **d'ajustement de la pondération**. Chaque utilisateur peut définir ses propres ajustements de pondération, ce qui aide à harmoniser les notes avec vos priorités.



Important : Si le score est **S.O.**, il est considéré comme à **0** dans le calcul de la note globale.

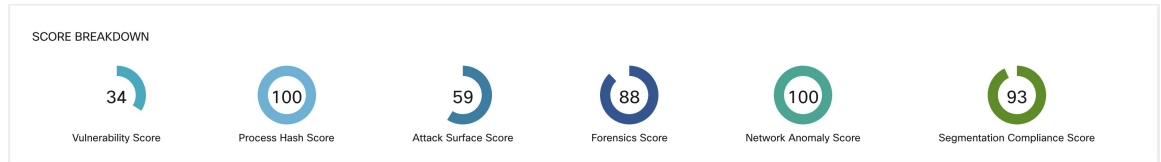
Séries chronologiques quotidiennes

Séries chronologiques empilées pouvant aller jusqu'à trois mois. Cela permet de suivre la situation en matière de sécurité sur une longue période. Chaque pile représente une note globale pour une journée. Chaque segment de la pile est une catégorie qui est représenté par une couleur différente. Vous pouvez cliquer sur un jour pour obtenir la ventilation de la note pour la journée.



Répartition de la note

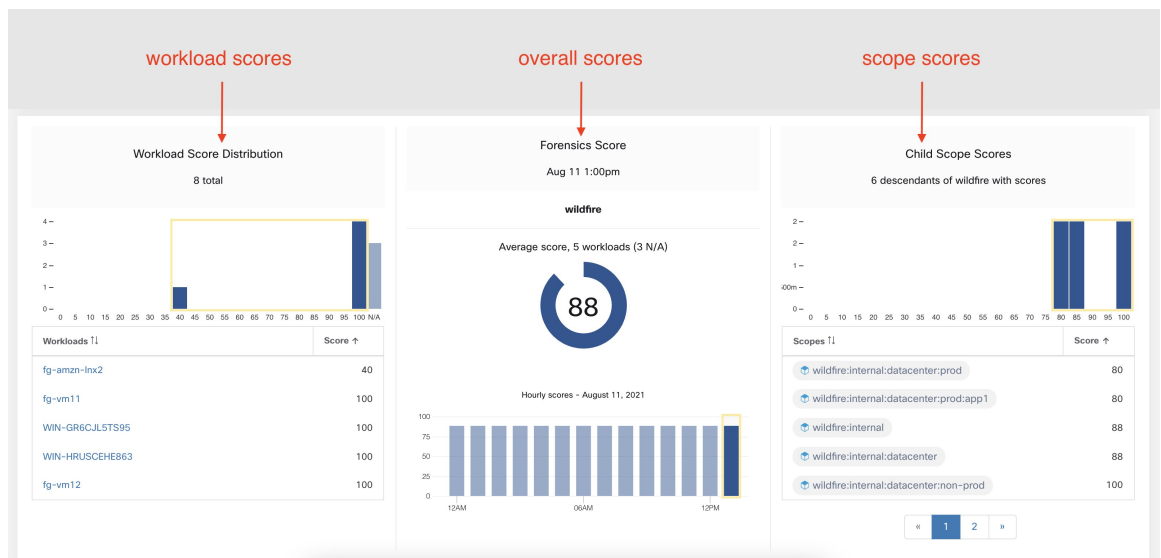
La répartition de la note affiche le résultat pour les six catégories pour la journée sélectionnée dans la série chronologique. Une note **S.O.** indique que la note n'est pas disponible. Elle comptera pour 0 dans le calcul de la note globale.



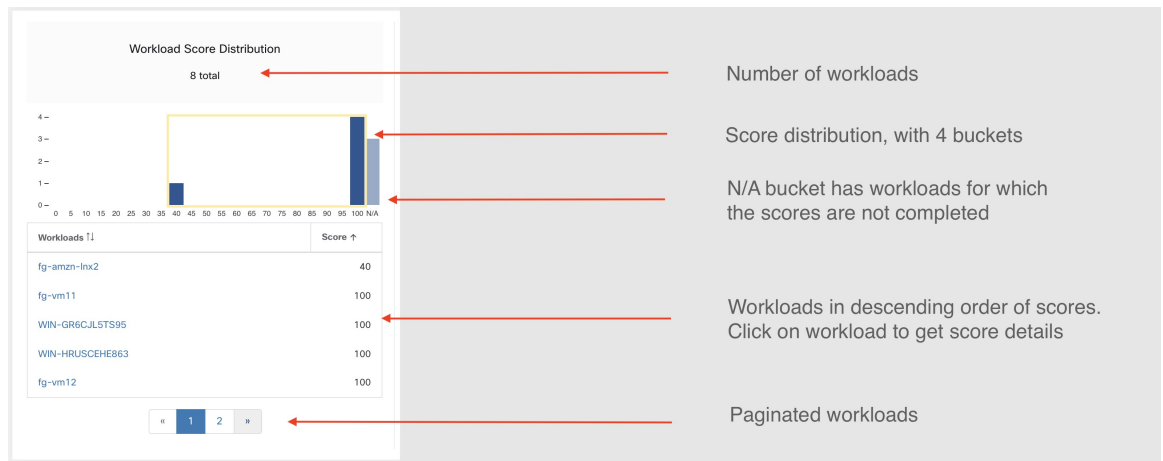
Important Si la note est **S.O.**, elle est considérée comme **0** dans le calcul de la note globale.

Détails de la note

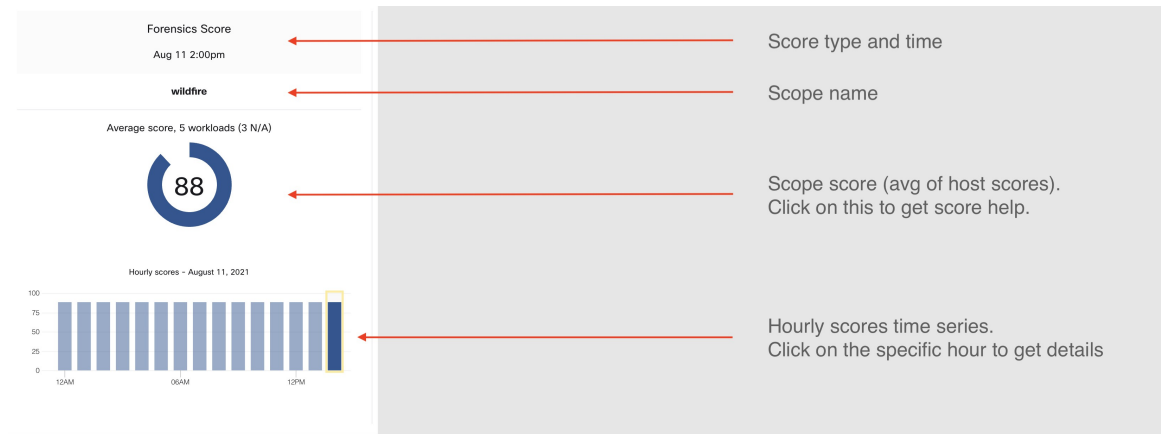
Chacune des six catégories suit le modèle suivant. Ce modèle présente la répartition des notes de la charge de travail, des séries chronologiques horaires et la distribution des notes de la portée enfant.



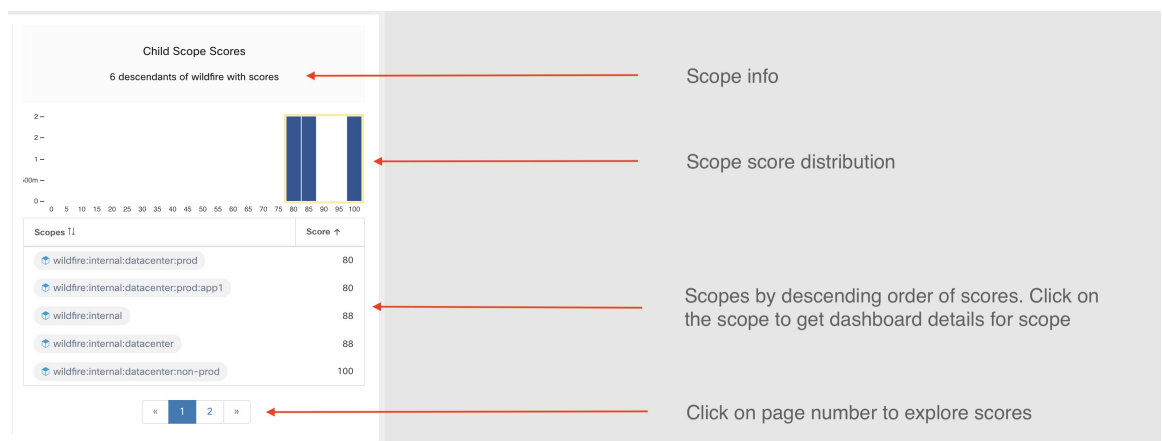
La répartition des notes des charges de travail fournit des indications sur la contribution aux notes des charges de travail dans le cadre de la portée sélectionnée. Il permet de faire ressortir les charges de travail les moins performantes pour accélérer les mesures correctives.



Les séries chronologiques horaires permettent d'obtenir le résultat horaire au cours d'une journée donnée. La sélection d'une heure dans la série chronologique met à jour la répartition des notes de la charge de travail et la répartition de la portée descendante afin d'afficher l'heure sélectionnée.



La répartition des portées descendantes fournit des informations sur la contribution au score des portées enfants de la portée sélectionnée.

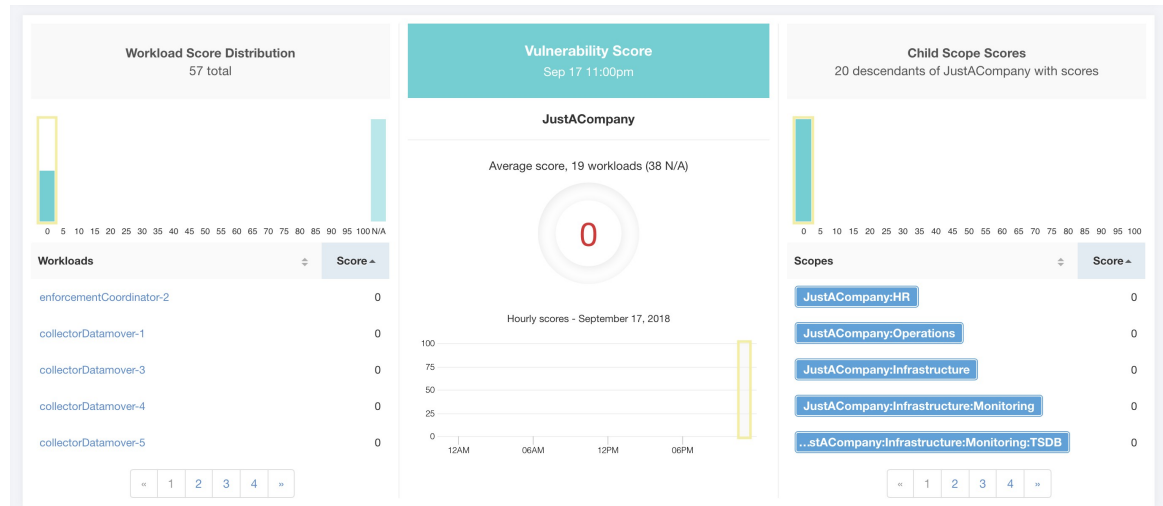


Les détails de chaque catégorie de note sont expliqués dans cette section.

Note de sécurité des vulnérabilités

Les vulnérabilités des paquets logiciels installés sur les charges de travail sont utilisées pour calculer la note de sécurité et de vulnérabilité.

Figure 1: Détails de la note de sécurité liée à la vulnérabilité



La note la plus faible indique :

- Un ou plusieurs paquets logiciels installés présentent de graves vulnérabilités.
- Appliquer un correctif ou une mise à niveau pour réduire les risques d'expositions ou d'exploits

Les paquets logiciels sur les charges de travail pourraient être associés à des vulnérabilités connues (CVE). Le système CVSS (Common Vulnerability Scoring System) est utilisé pour évaluer l'impact d'une CVE. La plage de résultats CVSS va de 0 à 10, 10 étant la plus élevée.

Une CVE peut avoir une note CVSS v2 et CVSS v3. Pour calculer la note de vulnérabilité, CVSS v3 est pris en compte s'il est disponible, sinon CVSS v2 est pris en compte.

La note de vulnérabilité pour une charge de travail est dérivée des notes des logiciels vulnérables détectés sur cette charge de travail. La note de vulnérabilité de la charge de travail est calculée en fonction des résultats CVSS et des données des fournisseurs, et peut être ajustée par notre équipe de recherche sur la sécurité lorsque les données sont manquantes ou inexactes (ce qui est courant pour les nouvelles vulnérabilités). Ces données sont mises à jour toutes les 24 heures lors de la configuration du flux des menaces. Plus la gravité de la vulnérabilité la plus grave est élevée, plus la note est faible.

La note de portée est la moyenne des notes de charge de travail de la portée. Améliorez la note en identifiant les charges de travail ou les portées comportant des paquets logiciels vulnérables, et en appliquant des correctifs ou des mises à niveau avec des paquets plus sûrs.

Figure 2: Aide sur la vulnérabilité et la note de sécurité

? 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 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.

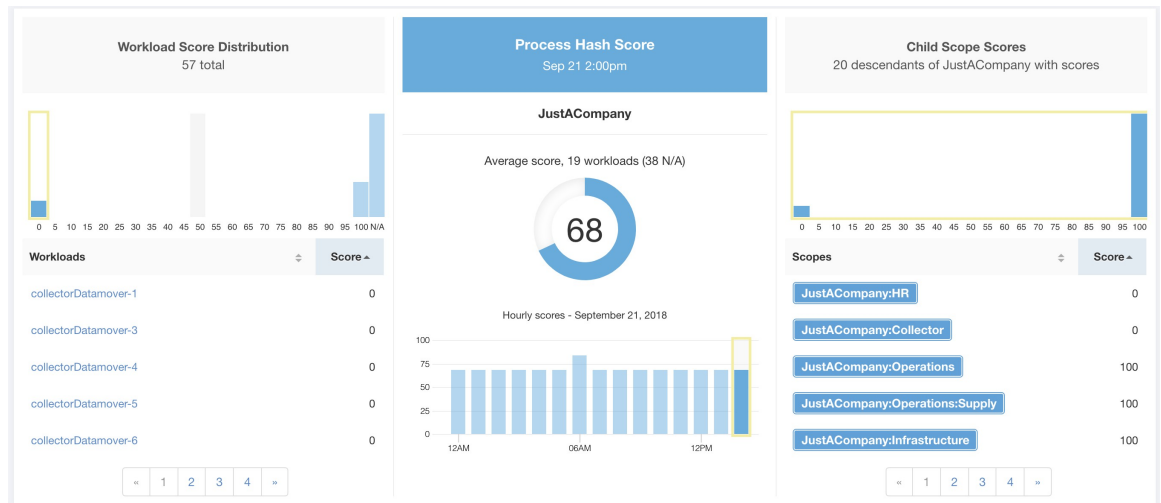
How do I increase the number of workloads with scores?

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

Note de condensé de processus

La note de condensé de processus est une évaluation de la cohérence du condensé binaire du processus (condensé de fichier) dans l'ensemble des charges de travail. Par exemple, une batterie de serveurs Web exécutant Apache qui est clonée à partir de la même configuration d'installation doit avoir le même condensé pour les fichiers binaires [httpd](#) sur tous les serveurs. Une incohérence est une anomalie.

Figure 3: Détails de la note de condensé de processus



Une note plus basse indique qu'au moins l'un des éléments suivants, ou les deux, sont présents :

- Un ou plusieurs condensés de processus sont marqués par un indicateur.
- Un ou plusieurs condensés de processus sont anormaux.

Reportez-vous à la section [Processus de détection des anomalies de condensé](#) pour plus de détails.

Figure 4: Aide sur la note de condensé de processus

? Process Hash Score Help

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?

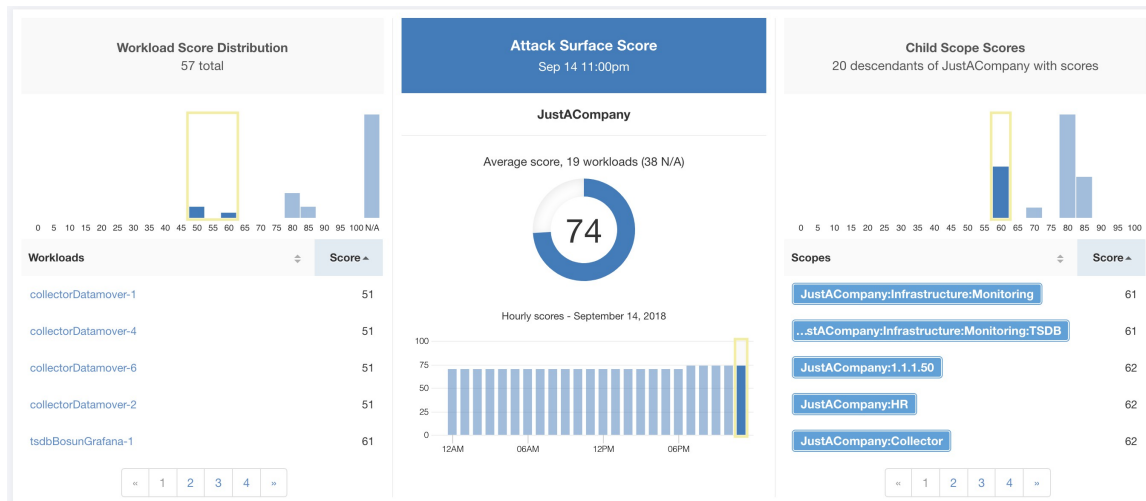
For each process hash we compute a score as follows:

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

Note de surface d'attaque

La note de surface d'attaque met en évidence la surface d'attaque potentielle dans une charge de travail. Les ports ouverts inutilisés (ports ouverts sans trafic) contribuent à abaisser ce score.

Figure 5: Détails de la note de surface d'attaque



Une note inférieure indique :

- De nombreux ports ouverts sans trafic au cours des 2 dernières semaines
- Des ports d'attaque bien connus peuvent être ouverts et inutilisés au cours des 2 dernières semaines.
- Un ou plusieurs ports ouverts sont associés à des paquets qui présentent de graves vulnérabilités.

La note de surface d'attaque est en fonction des ports ouverts inutilisés par rapport au nombre total de ports, avec un facteur de lissage. Les ports ouverts sans trafic au cours des deux dernières semaines sont considérés comme des « ports ouverts inutilisés ». Une pénalité supplémentaire est appliquée aux ports ouverts inutilisés qui sont des ports bien connus qui sont utilisés dans des attaques (par exemple, 21, 22, 8080, etc.).

Figure 6: Formule de la note de surface d'attaque

$$\begin{aligned}
 & \text{Attack surface score} \\
 &= \frac{\alpha + \sum \text{used open ports}}{\alpha + \sum \text{open ports} + (\rho * \sum \text{unused common attack ports}) + f_v(\text{vulnerability pkgs})} \\
 & f_v = \max \left(\left\{ \begin{array}{l} \text{cve_score} = \{ CVSS_{v3}, \quad v3 \text{ exist} \\ \quad \quad \quad \quad \quad \quad \quad \quad v3 \text{ not exist} \} \end{array} \right\} \right)
 \end{aligned}$$

Le lissage de Laplace est utilisé avec un facteur de pénalité basé sur des données heuristiques. La note est calculée quotidiennement avec les deux dernières semaines de données.

La note du détenteur est la moyenne des notes de la charge de travail de la portée. Améliorer le score en identifiant la charge de travail ou les portées avec des ports ouverts inutilisés, et en fermant les ports inutilisés.

Lorsque vous cliquez sur le lien d'une charge de travail, une boîte de dialogue modale de surface d'attaque est ouverte avec des détails sur tous les ports et toutes les interfaces disponibles dans le contexte de cette charge de travail.

33
Attack Surface Details - [redacted]
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	Packag
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 »


Caractéristiques :

- Ports inutilisés uniquement : cochez cette case lorsque cette option filtre les ports utilisés et affiche uniquement les ports inutilisés associés à la charge de travail.
- Colonnes : approuvé, port, nom du paquet, total autorisé, note CVE maximale, condensé de processus, interfaces, serveur de publication du paquet, version du paquet, total échappé, total rejeté, ports couramment piratés, liens.
- Interfaces : Si vous cliquez sur l'un des éléments de ligne du tableau Surface d'attaque, vous pouvez afficher les interfaces associées à chaque port dans une boîte de dialogue modale.
- Approuvé : case à cocher, lorsqu'elle est cochée, vous permet de définir intentionnellement un « port inutilisé » comme « approuvé » sur l'un des champs de la chaîne de portées à laquelle cette charge de travail a accès. Remarque : si un port est approuvé pour une portée et que ce port n'est explicitement approuvé sur aucune des portées enfants (si cette portée a des enfants), les cases de la portée sont désactivées, car il est implicite que toute portée enfant à laquelle la portée parente a accès à est déjà approuvé dans cette chaîne.

Boîte de dialogue modale d'approbation :

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

Boîte de dialogue modale des interfaces :

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

Figure 7: Aide sur la note de surface d'attaque

? **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 an 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.

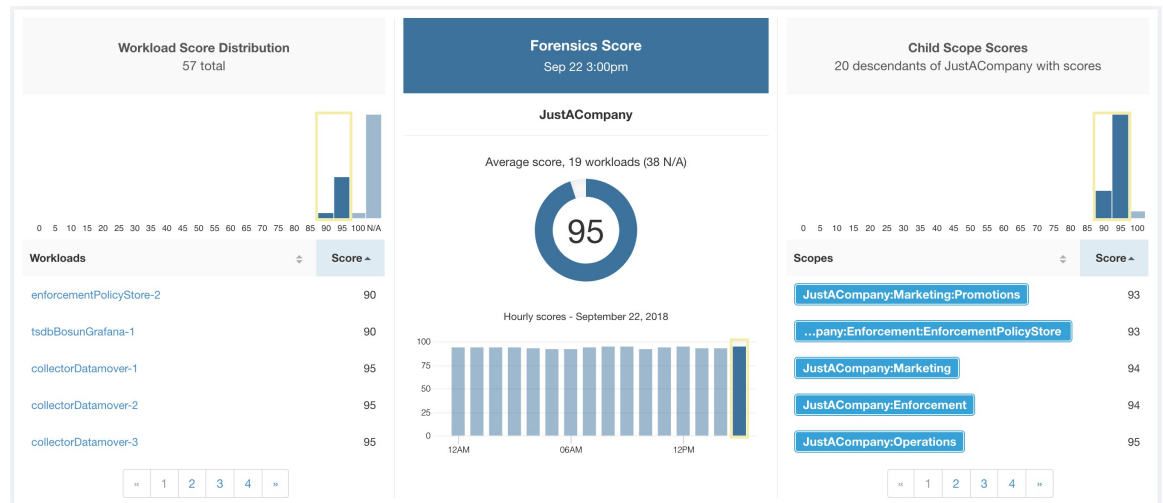
How do I increase the number of workloads with scores?

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.

Note de criminalistique

La gravité des événements criminalistiques sur les charges de travail est utilisée pour calculer les notes.

Figure 8: Détails de la note criminalistique



La note la plus faible indique :

- Un ou plusieurs événements criminalistiques ont été observés sur la charge de travail.
- Ou une ou plusieurs règles criminalistiques sont parasitées ou incorrectes.

Pour améliorer le résultat :

- Corrigez le problème, le cas échéant, pour réduire les risques d'expositions ou d'exploitations.
- Ajustez les règles criminalistiques pour réduire le bruit et les fausses alertes.

La note criminalistique pour une charge de travail est inversement proportionnelle à la note d'impact totale des événements criminalistiques. Plus la note d'incidence totale des événements criminalistiques est élevée, plus leur incidence est faible.

Gravité	Note d'incidence
IMMEDIATE_ACTION (ACTION_IMMÉDIATE)	100
CRITIQUE	10
ÉLEVÉE	5
CRITIQUE	3

Figure 9: Formule de note criminalistique

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

Reportez-vous à la section [Criminalistique](#) pour plus de détails.

Figure 10: Aide relative à la note criminalistique

? Forensics Score Help

Supported Agent Types 19 supported workloads

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

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.

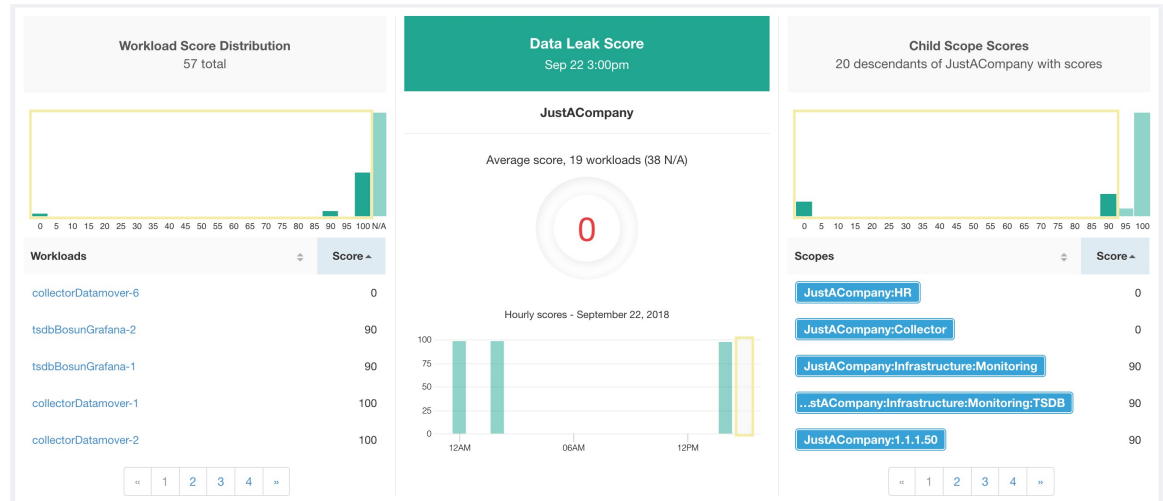
How do I increase the number of workloads with scores?

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

Note d'anomalie de réseau

La gravité des événements d'anomalie de réseau sur les charges de travail est utilisée pour calculer les notes.

Figure 11: Détails de la note de fuite de données



La note la plus faible indique :

- Une quantité inhabituellement élevée de données est transférée à partir des charges de travail.
- Ou la règle criminalistique d'anomalie de réseau est incorrecte ou parasitée par du bruit.

Pour améliorer le résultat :

- Corrigez le problème, le cas échéant, pour réduire les risques d'exfiltration de données.
- Ajustez les règles d'anomalies de réseau pour réduire le bruit et les fausses alertes.

La note d'anomalie de réseau pour une charge de travail est inversement proportionnelle à la note de gravité totale des événements d'anomalie de réseau. Plus la note d'anomalie totale de réseau est élevée, plus la note d'anomalie de réseau est faible.

Gravité	Résultat
IMMEDIATE_ACTION (ACTION_IMMÉDIATE)	100
CRITIQUE	10
ÉLEVÉE	5
CRITIQUE	3

Figure 12: Formule de la note de fuite de données

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

Reportez-vous à la section [Détection des anomalies de réseau par PCR](#) pour en savoir plus.

Figure 13: Aide sur la note de fuite de données

? Data Leak 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 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.

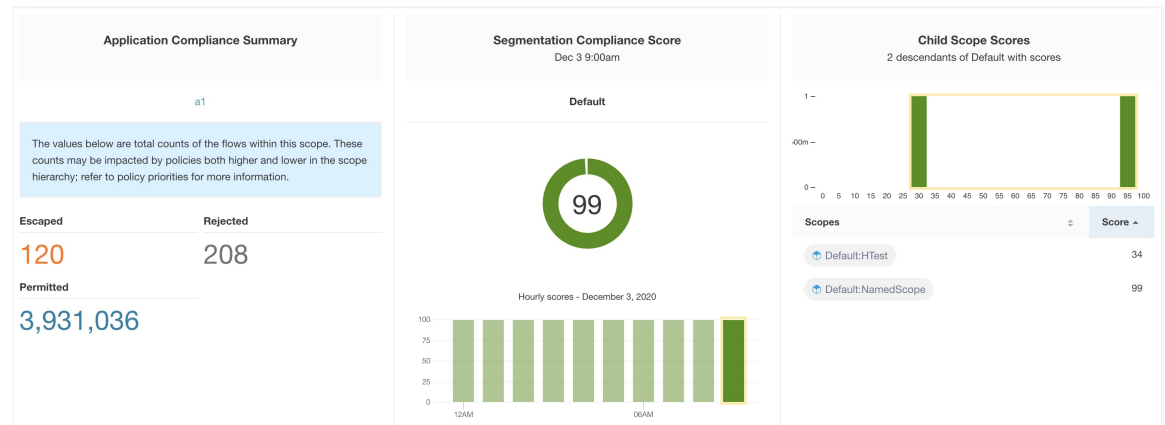
How do I increase the number of workloads with scores?

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.

Note de conformité de la segmentation

La note de conformité de la segmentation présente une vue générale des violations de politique et souligne les portées et les espaces de travail qui ont subi le plus grand nombre de violations.

Figure 14: Détails de la note de conformité de la segmentation



Note Le nombre d'échappés, de refus ou d'autorisations affiché dans le tableau de bord de sécurité pour la portée racine ne correspond pas à tous les nombres affichés respectivement pour toutes les portées enfants. Le nombre d'échappés, de refus ou d'autorisations est une évaluation de la politique et pas seulement de la source ou de la destination.

La note la plus faible indique :

- Nombre important de flux échappés (violations de politique) par rapport à la valeur autorisée
- La note est de 0 lorsqu'il y a plus de flux échappés que celui autorisé.

La note de conformité de la segmentation est calculée pour les portées avec un espace de travail principal appliqué. Pour les portées sans espaces de travail appliqués, la note sera calculée comme la moyenne des notes des portées descendantes comportant des politiques appliquées.

La note est calculée en utilisant le rapport entre échappé et autorisé.

Figure 15: Formule de la note de conformité de la segmentation

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

Améliorer le score en réduisant le nombre de violations de politique

- Vérifiez que les politiques couvrent correctement le comportement souhaité.
- Vérifiez que les politiques sont correctement appliquées.

Figure 16: Aide pour les détails sur le niveau de conformité de la segmentation

? Segmentation Compliance Score Help

Supported Agent Types 5,059 supported workloads

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

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.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d'incohérence, la version anglaise du présent contenu prévaudra.