



## 查看安全控制面板

---

本章提供有关“安全”(Security)控制面板下显示的安全评分、安全评分类别和范围级别评分的详细信息。

安全控制面板通过汇总 Cisco Secure Workload 中可用的多个信号来提供可操作的安全评分，而这有助于了解当前的安全状况并加以改进。安全控制面板是 Cisco Secure Workload 中许多更丰富的深入分析（例如流搜索、资产搜索、自动策略发现和取证）的跳板。

- [查看安全控制面板, on page 1](#)
- [安全评分, on page 2](#)
- [安全评分类别, on page 2](#)
- [概要视图, on page 2](#)
- [范围级别评分详细信息, on page 2](#)
- [评分详细信息, on page 5](#)

## 查看安全控制面板

要查看安全控制面板，请从导航窗格中选择**概述 (Overview)**。

# 安全评分

安全评分是一个介于 0 到 100 之间的数字，表示类别中的安全位置。评分 100 为最佳，评分 0 为最差。评分越接近 100 越好。

安全评分计算会考虑已安装软件包中的漏洞、进程散列的一致性、不同接口上的开放端口、取证和网络异常事件，以及策略的合规性或不合规性。

## 安全评分类别

有六种不同的评分类别。提供这些类别时考虑了工作负载的大多数安全方面。

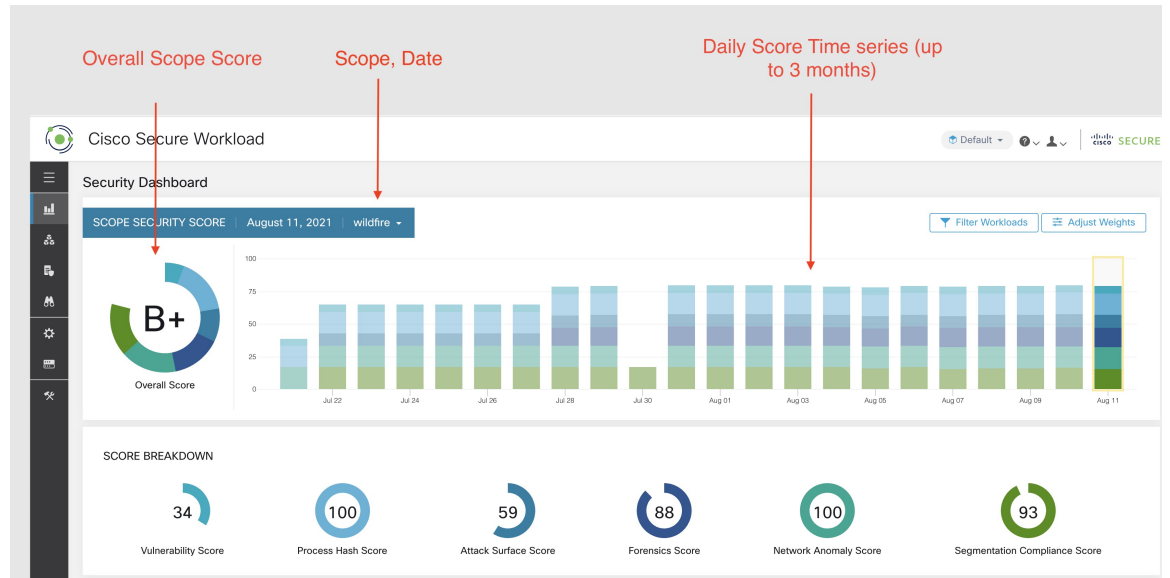
- **漏洞评分：**工作负载上已安装软件包中的漏洞会被用于评分。
- **进程散列评分：**进程散列一致性（和异常）以及良性和标记进程散列用于评分。
- **攻击面评分：**进程可能在多个接口上打开一个或多个端口，以使服务可用。未使用的开放端口会被用于评分。
- **取证评分：**工作负载上取证事件的严重性会被用于评分。
- **网络异常评分：**工作负载上网络异常事件的严重性会被用于评分。
- **分段合规性评分：**自动发现的策略的合规性（允许）和违规（转义）会被用于评分。

## 概要视图

安全控制面板具有所选范围的范围级别评分。有一个包含时间序列和评分细分的总体评分。系统将显示所选范围的六个评分类别的评分详细信息。

## 范围级别评分详细信息

范围级别评分详细信息位于控制面板的顶部。

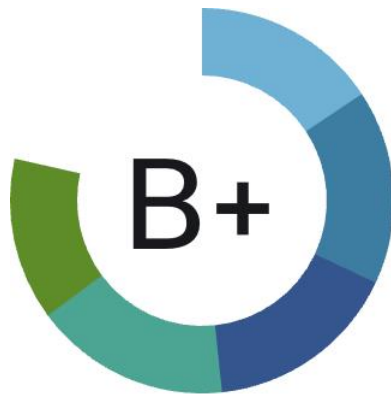


屏幕将显示以下详细信息：

- 范围总体评分：所选范围的总体评分。
- 每日评分时间序列：最多 3 个月的堆叠时间序列。
- 评分明细：时间序列中所选日期的类别评分明细。

## 总体评分

总评分表示为 **A+**, **A**, ..., **F** 中的字母，其中 **A+** 被视为最佳评分，而 **F** 为最差评分。它显示为圆环图，每个切片（彩色编码）代表一个评分类别。

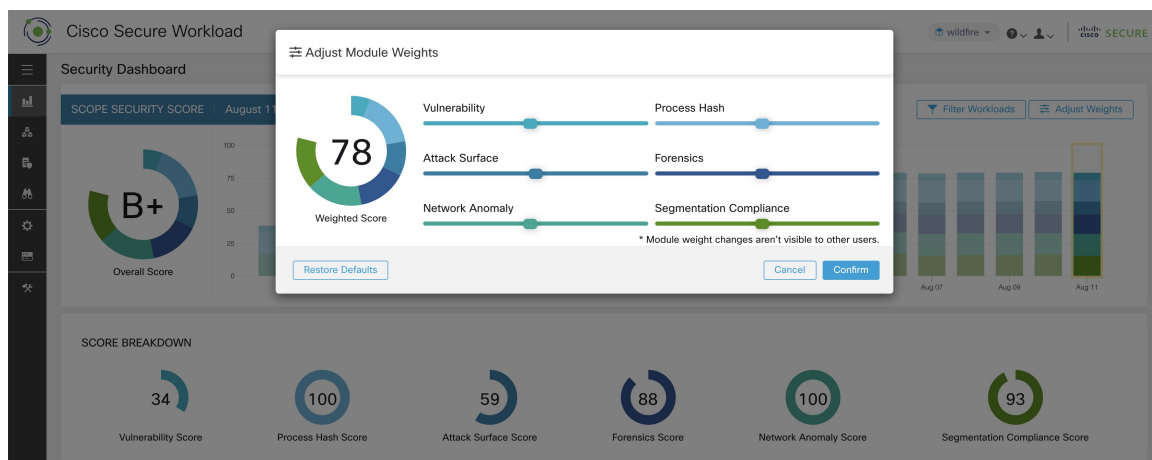


Overall Score

总分是六个评分类别的加权平均值。所有权重均默认为相等。如果评分是 **N/A**，则在总评分计算中被视为 0。

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

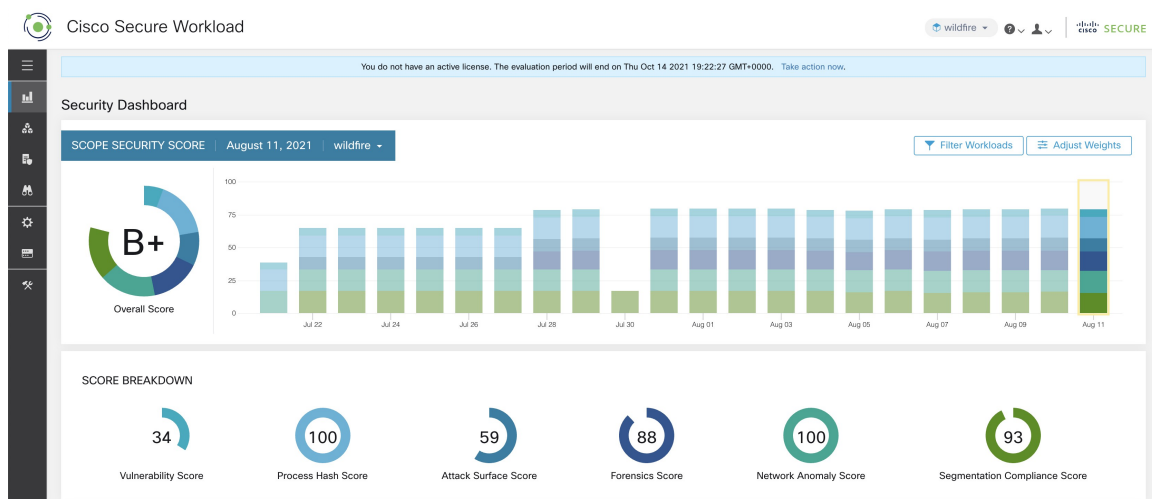
可以使用调整权重模块中的滑块来调整权重。每位用户都可以设置自己的权重调整，这有助于使评分与您的优先级保持一致。



**重要提示：** 如果评分为 **N/A**，则在总分计算中将被视为 **0**。

## 每日时间序列

最长可达 3 个月的堆叠时间序列。它有助于长期跟踪安全位置。每个堆栈代表一天的总评分。堆栈中的每个分段都是一个类别，以不同的颜色表示。您可以点击日期以获取当天的评分明细。



## 评分明细

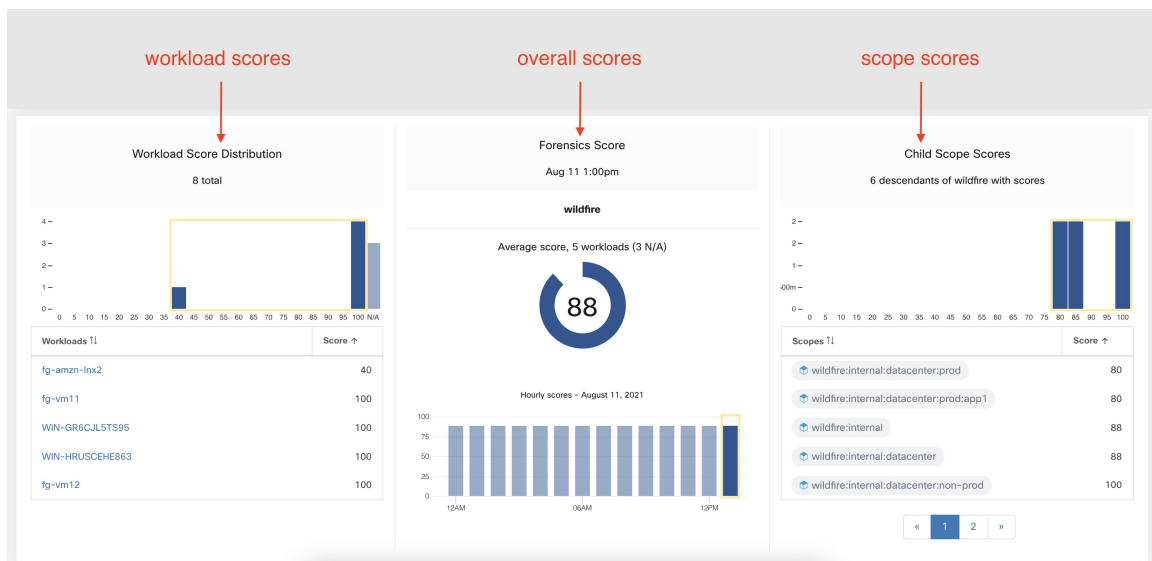
评分明细显示时间序列中所选日期的所有六个类别的评分。评分 **N/A** 表示评分不可用。在计算总评分时，它将被计为 **0**。



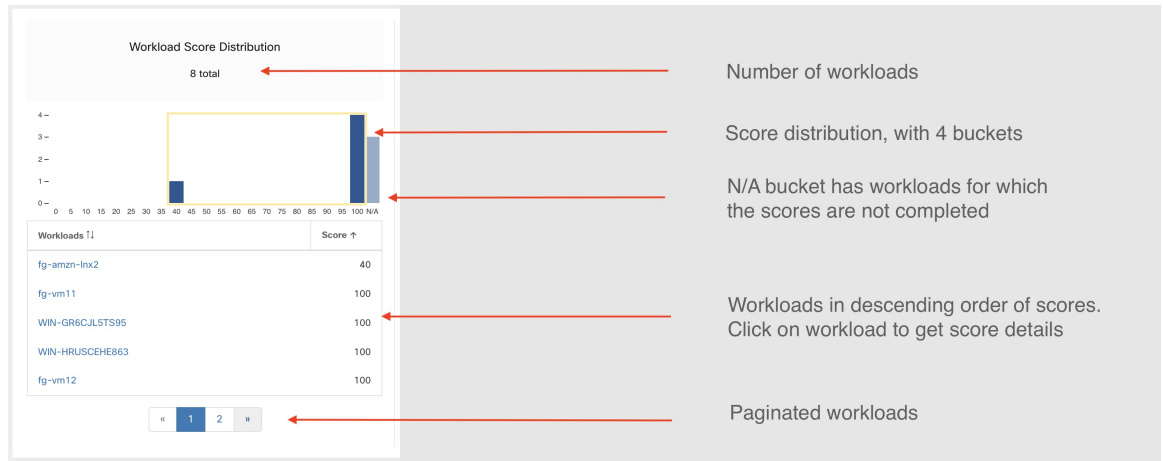
**Important** 如果评分不适用，则在计算总评分时将其视为 **0**。

## 评分详细信息

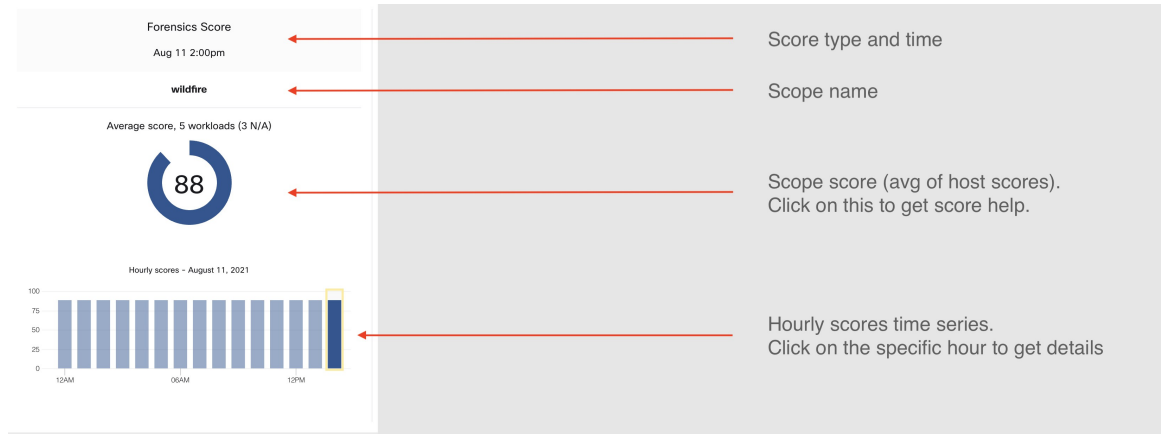
六个类别中的每一个都遵循以下模板。它具有工作负载评分分布、每小时时间序列和子范围评分分布。



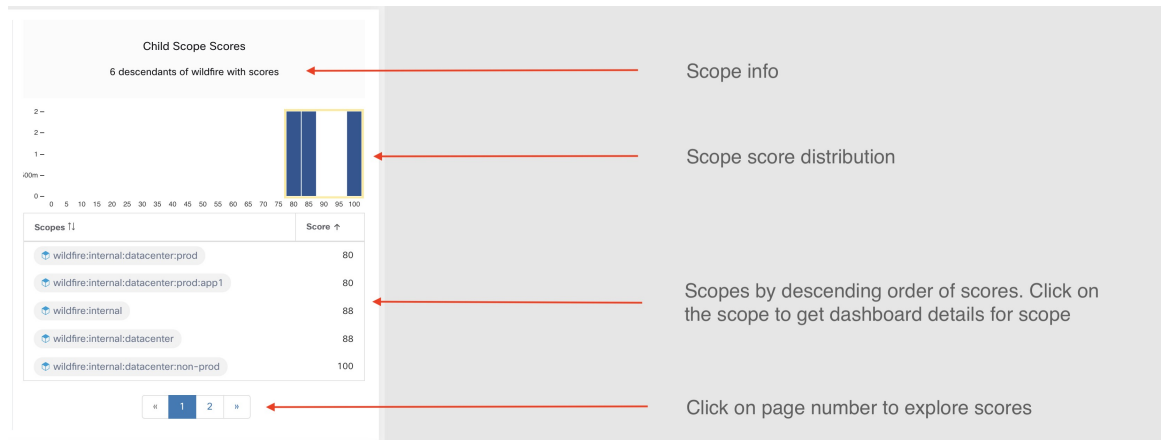
通过工作负载评分分布，可以深入了解所选范围内的工作负载对评分的影响。它有助于让分数最低的工作负载显现，从而加快纠正措施。



每小时时间序列有助于获取所选日期的每小时评分。在每小时时间序列中选择一个小时，就会更新工作负载评分分布和后代范围分布，以显示所选的小时。



后代范围分布有助于我们了解所选范围的子范围的评分贡献。

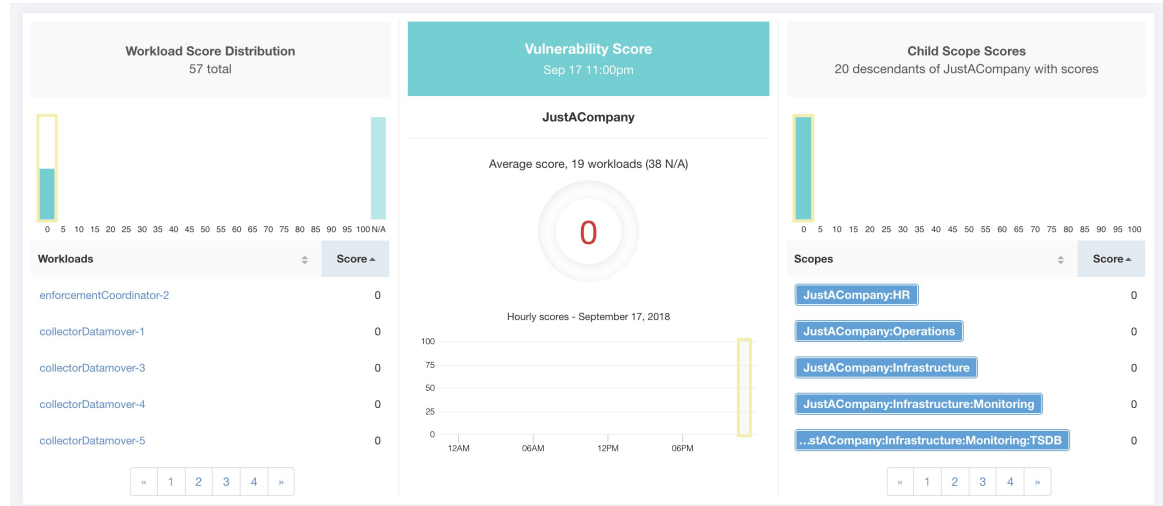


本部分介绍每个评分类别的详细信息。

## 漏洞安全评分

工作负载上安装的软件包中的漏洞用于计算漏洞安全评分。

**Figure 1:** 漏洞安全分数详细信息



评分越低表示：

- 一个或多个已安装的软件包存在严重漏洞。
- 应用补丁或升级以便减少暴露或漏洞攻击的机会

工作负载上的软件包可能与已知漏洞 (CVE) 相关联。CVSS (通用漏洞评分系统) 用于评估 CVE 的影响。CVSS 得分范围为 0-10，其中 10 表示最严重。

CVE 可以具有 CVSS v2 和 CVSS v3 评分。要计算漏洞评分，请考虑 CVSS v3 (如果可用)，否则考虑 CVSS v2。

工作负载的漏洞评分是根据在该工作负载上检测到的漏洞软件评分得出的。工作负载漏洞评分是根据 CVSS 评分和供应商数据计算得出的，当数据缺失或不准确时，我们的安全研究团队可能会进行调整 (常见于新漏洞)。配置威胁源后，此数据每 24 小时会更新一次。最严重漏洞的严重性越高，评分就越低。

范围评分是范围中工作负载评分的平均值。通过识别易受攻击的软件包的工作负载或范围，以及使用更安全的软件包修补或升级来提高评分。

Figure 2: 漏洞安全评分帮助

? Vulnerability Score Help

**Supported Agent Types** 19 supported workloads

<span style="color: red; font-weight: bold;">✘</span> Universal Visibility (38)	<span style="color: green; font-weight: bold;">✔</span> <b>Deep Visibility (19)</b>	<span style="color: green; font-weight: bold;">✔</span> <b>Enforcement (0)</b>
<span style="color: red; font-weight: bold;">✘</span> AnyConnect (0)	<span style="color: red; font-weight: bold;">✘</span> 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.

## 进程散列评分

进程散列评分是对跨工作负载的进程二进制散列（文件散列）一致性的评估。例如：从同一设置配置克隆的运行 Apache 的 Web 服务器场预期会在所有服务器上具有相同的 [httpd](#) 二进制文件散列。不匹配属于异常情况。



Figure 3: 进程散列评分详细信息



较低的评分表示以下至少一项或两项：

- 已标记一个或多个进程散列值。
- 一个或多个进程散列出现异常。

有关详细信息，请参阅[进程散列异常检测](#)。

Figure 4: 进程散列评分帮助

**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?**

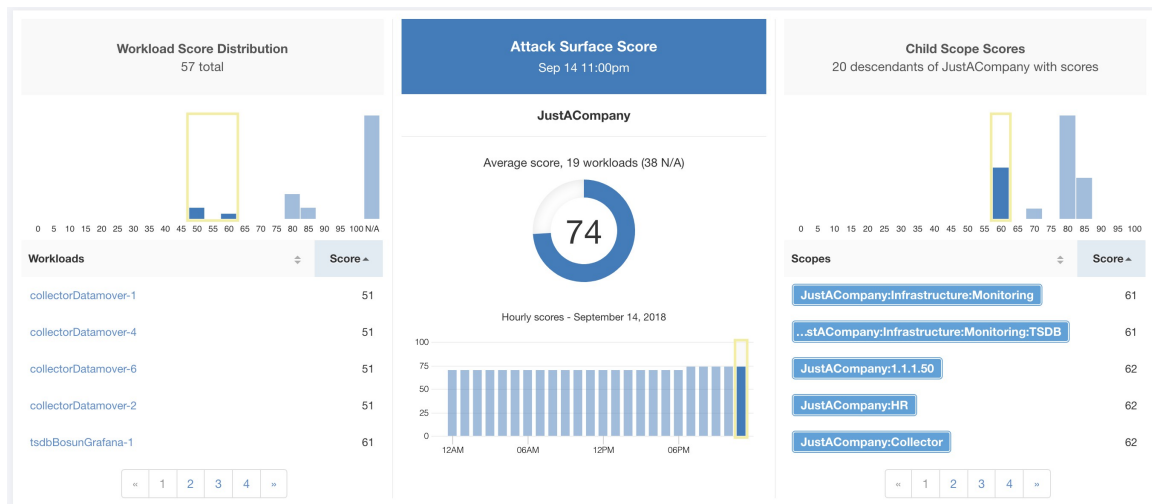
For each process hash we compute a score as follows:

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

## 攻击面评分

攻击面评分突出显示工作负载中的潜在攻击面。打开未使用的端口（打开没有流量的端口）会降低此评分。

Figure 5: 攻击面评分详细信息



评分越低表示：

- 在过去 2 周内无任何流量的许多开放端口
- 已知攻击端口在过去 2 周内可能处于开放状态且未使用。
- 一个或多个开放端口连接到存在严重漏洞的软件包。

攻击面评分是未使用的开放端口相对于总端口的函数，具有平滑系数。在过去 2 周内没有任何流量的开放端口会被视为“未使用的开放端口”。额外的惩罚适用于未使用的开放端口，这些端口是在攻击中使用的已知端口（例如，21、22、8080 等）。

Figure 6: 攻击面得分公式

Attack surface score

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

$$f_v = \max \left\{ \begin{array}{l} cve_{score} = \begin{cases} CVSS_{v3}, & v3 \text{ exist} \\ CVSS_{v2}, & v3 \text{ not exist} \end{cases} \end{array} \right\}$$

拉普拉斯平滑与基于启发式数据的惩罚系数一起使用。每天根据过去 2 周的数据计算评分。

租户评分是范围内工作负载评分的平均值。通过确定具有未使用的开放端口的工作负载或范围，以及关闭未使用的端口，提高评分。

点击某个工作负载链接后，就会打开一个攻击面模式，其中包含该工作负载背景下所有可用端口和接口的详细信息。

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	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 »


### 特点:

- **仅未使用端口 (Unused Ports Only):** 切换到该复选框后，它就会过滤掉已使用的端口，仅显示与工作负载关联的未使用端口。
- **列:** 已批准、端口、程序包名称、允许总数、CVE 最高评分、进程散列、接口、程序包发布服务器、程序包版本、转义总数、拒绝总数、经常被入侵的端口、链接。
- **接口 (Interfaces):** 如果点击“攻击面” (Attack Surface) 表中的任何一个行项目，则可以查看与模式内的每个端口关联的接口。
- **已批准 (Approved):** 切换到该复选框后，您就可以在该工作负载有权访问的范围链上的任何一个范围上有意将“未使用的端口”设置为“已批准”。注意：如果某个端口已在某个范围上获得批准，而该端口没有在任何子范围（如果该范围有子范围）上明确获得批准，那么范围复选框将被禁用，因为这意味着父范围可访问的任何子范围已在该链中获得批准。

### 审批模式:

### 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](#)

接口模式:

### 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](#)

Figure 7: 攻击面评分帮助

? **Attack Surface Score Help**

**Supported Agent Types** 19 supported workloads

<span style="color: red; font-weight: bold;">✘</span> Universal Visibility (38)	<span style="color: green; font-weight: bold;">✔</span> <b>Deep Visibility (19)</b>	<span style="color: green; font-weight: bold;">✔</span> <b>Enforcement (0)</b>
<span style="color: red; font-weight: bold;">✘</span> AnyConnect (0)	<span style="color: red; font-weight: bold;">✘</span> 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.

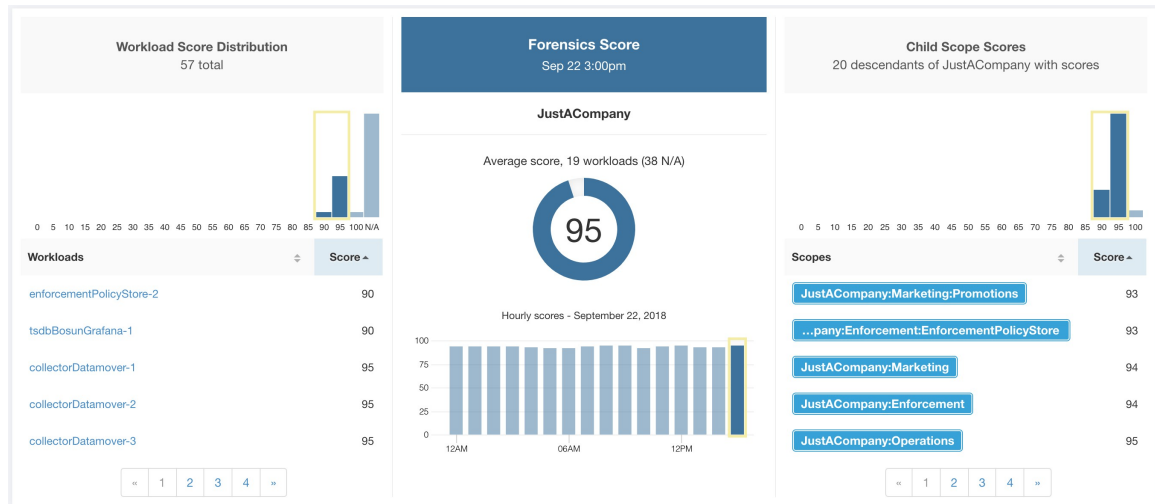
**How do I increase the number of workloads with scores?**

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.

## 取证评分

工作负载上取证事件的严重性用于计算评分。

Figure 8: 取证评分详细信息



评分越低表示：

- 在工作负载上观察到一个或多个取证事件。
- 或者一个/多个取证规则有干扰和/或不正确。

要提高评分，请执行以下操作：

- 如有任何问题，请修复问题，以减少暴露/漏洞攻击的机会。
- 调整取证规则以减少噪音和错误警报。

工作负载的取证评分与取证事件的总影响评分成反比。取证事件的总影响评分越高，取证评分越低。

严重性	影响评分
IMMEDIATE_ACTION	100
严重	10
高	5
严重	3

Figure 9: 取证评分公式

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

有关详细信息，请参阅[取证](#)。

Figure 10: 取证评分的帮助

? 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?**

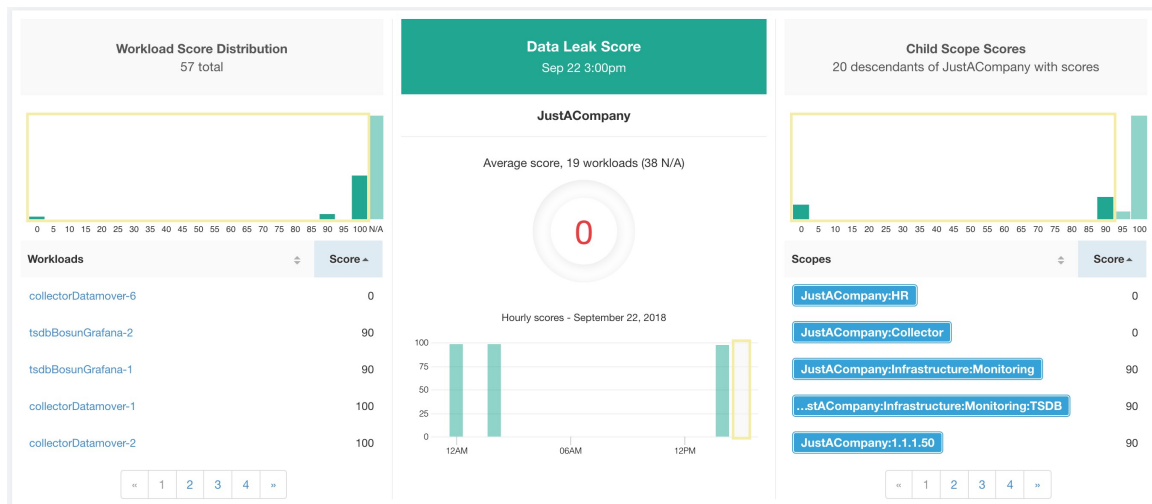
See the compatibility chart above for which sensor types are compatible. Installing the supported sensor types on more Workloads will increase your Forensic coverage.

## 网络异常评分

工作负载上网络异常事件的严重性用于计算评分。



Figure 11: 数据泄漏评分详细信息



评分越低表示：

- 从工作负载中传输出来的数据量异常大。
- 或者，网络异常取证规则不正确或存在干扰。

要提高评分，请执行以下操作：

- 修复问题（如有），以减少数据泄露的可能性。
- 调整网络异常规则，以减少噪音和误报。

工作负载的网络异常评分是网络异常事件的严重性总评分的反函数。严重性总评分越高，网络异常评分越低。

严重性	得分
IMMEDIATE_ACTION	100
严重	10
高	5
严重	3

Figure 12: 数据泄漏评分公式

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

有关详细信息，请参阅[基于 PCR 的网络异常检测](#)。

Figure 13: 数据泄漏评分帮助

?
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.

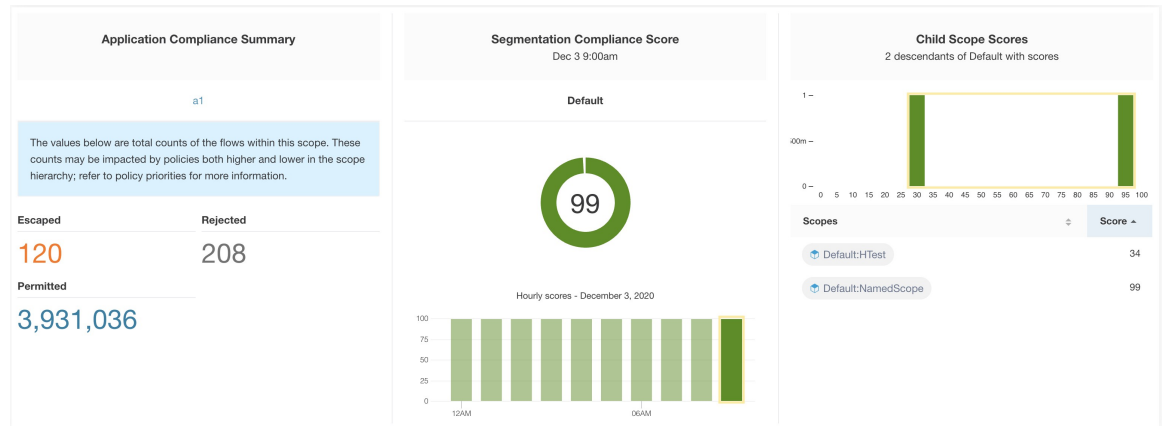
**How do I increase the number of workloads with scores?**

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.

## 分段合规性评分

分段合规性评分提供策略违规的顶级视图，并强调哪些范围和工作空间的违规最多。

Figure 14: 分段合规性评分详细信息



**Note** 根范围的安全控制面板上显示的转义/拒绝/允许计数不会与分别为所有子范围显示的所有计数相加。转义/拒绝/允许计数是对策略的评估，而不仅仅是对源或目标的评估。

评分越低表示：

- 相对于允许的大量转义流（策略违规）
- 当转义流数超过允许数时，评分为 0。

分段合规性评分针对具有强制主工作空间的范围计算。对于没有强制工作空间的范围，评分将作为具有强制策略的后代范围评分的平均值进行计算。

评分通过使用转义和允许之间的比率计算。

Figure 15: 分段合规性评分公式

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

通过减少策略违规数量来提高评分

- 验证策略是否正确涵盖所需行为。
- 验证是否正确执行了策略。

Figure 16: 细分合规性评分详细信息帮助

### 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.

## 当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。