Cisco Secure Workload 入门

如今的网络包括在混合多云环境中运行的应用，而这些环境使用裸机、虚拟化以及基于云和容器的工作负载。在这种环境下，关键的挑战是在不影响灵活性的前提下提高应用和数据的安全性。Cisco Secure Workload 通过使安全更接近应用并根据应用行为定制安全状态，提供全面的工作负载保护。Cisco Secure Workload 通过使用高级机器学习和行为分析技术来实现这种定制。它提供了一个即用型解决方案，以支持下列安全用例：

- 实施零信任模式，采用只允许业务所需流量的微分段策略。
- 使用行为基线和分析来识别工作负载的异常。
- 检测服务器上安装的软件包中的常见漏洞和风险。
- 如果在执行策略和阻止通信后漏洞仍然存在，则建议隔离服务器。

Cisco Secure Workload 中的工作负载和 IP 地址

在 Cisco Secure Workload 中，工作负载是 IP 地址；安装了软件代理和无代理云工作负载的主机被称为工作负载，未安装代理和无代理云工作负载的主机被称为 IP 地址。

注释 要查看产品的最终用户许可协议和补充最终用户许可协议，请参阅最终用户许可协议和补充最终用户许可协议。

- 支持的 Web 浏览器, on page 1
- 快速启动向导 ， 第 2 页
- 开始使用分段和微分段 ， 第 2 页

支持的 Web 浏览器

Cisco Secure Workload 支持以下 Web 浏览器：

- Google Chrome
- Microsoft Edge

快速启动向导

可选向导可指导您创建范围树的第一个分支，这是为您选择的应用生成和执行策略的第一步。该向导会介绍标签和范围的概念和优势。

以下用户角色可以访问该向导：

- 站点管理员
- 技术支持
- 根范围所有者

要访问该向导，请执行以下任一操作：

- 登录 Cisco Secure Workload。
- 点击蓝色横幅中的链接。蓝色横幅会显示在所有页面的顶部。
- 从主菜单中选择**概述 (Overview)**。

注释 如果已在**整理 (Organize)** > **范围和资产 (Scopes and Inventory)** 中定义范围，则无法访问该向导。删除现有范围以访问向导。

开始使用分段和微分段

使用此处提供的概要程序，以便通过使用 Cisco Secure Workload来设置分段和微分段策略。

实施微分段的一般过程

分段和微分段的目的是仅允许业务用途所需的流量，同时阻止所有其他流量。

过程

步骤 1 确保 Cisco Secure Workload 支持运行您的工作负载的平台和版本，以及为您的策略提供必要信息的系统。请参阅 Cisco Secure Workload 兼容性矩阵。

步骤 2 在工作负载上安装代理。

代理会收集 Cisco Secure Workload 所需的流数据和其他信息，以便对工作负载进行分组并确定适当的策略。代理还会执行已批准的策略。有关详细信息（包括指向受支持平台和要求列表的链接），请参阅部署软件代理。

步骤 3 收集或上传描述工作负载的标签。

通过标签，您可以轻松了解每个工作负载的用途，并提供有关每个工作负载的其他关键信息。

您需要这些信息来对工作负载进行分组，应用适当的策略，并了解 Cisco Secure Workload 建议的策略。标签是维护可简化策略管理的组的基础。有关详细信息，请参阅工作负载标签和 导入自定义标签。

步骤 4 根据工作负载标签来创建范围树。

标签可帮助您创建的工作负载逻辑组称为“范围”，精心选择的一组标签可帮助您创建一个被称为“范围树”的网络层次结构图。这种网络工作负载的层次结构视图是高效创建和维护策略的关键。通过层次结构视图，您只需创建一次策略，就能将其自动应用到该树分支上的每个工作负载。通过该视图，您还可以将某些应用（或网络的某些部分）的责任委派给具有必要专业知识的人员，以便为这些工作负载确定正确的策略。

您可以查询工作负载，并根据其标签将它们归入范围。例如，您可以创建一个名为“Email-app”的范围，其中包括具有“Application = Email-app”和“Environment = Production”标签的所有工作负载。您可以使用查询 Environment = Production 为 Application = Email-app 范围创建父范围。Production 范围包括生产 Email-app 和标有 Environment = Production 的所有其他工作负载。

有关详细信息，请参阅范围和资产。

如果尚未创建任何范围，则可以使用快速入门向导创建范围树。有关详细信息，请参阅快速启动向导，第 2 页。

步骤 5 为要为其创建策略的每个范围创建一个工作空间。

工作空间用于管理该范围内工作负载的策略。有关详细信息，请参阅工作空间。

步骤 6 手动创建应用于整个网络的策略。

例如，您可能希望允许所有内部工作负载访问 NTP 服务器，并拒绝所有外部流量，或者拒绝所有非内部主机的访问，除非明确允许。策略可以是绝对的，即不能被更具体的策略覆盖；也可以是默认的，即可以被更具体的策略覆盖。

有关详细信息，请参阅手动创建策略。

Cisco Secure Workload 具有可简化策略创建的策略模板。有关详细信息，请参阅策略模板。

您可以执行手动创建的策略，而无需等待策略被发现。有关详细信息，请参阅执行策略。

步骤 7 根据现有流量模式自动发现策略。

Cisco Secure Workload 会分析工作负载之间的流量，根据行为对工作负载进行分组，并建议一组允许组织所需流量的策略，以便您可以阻止所有其他流量。

在更长的时间段内对更多的数据流进行分析，可以得出更准确的策略建议。

您可以反复发现策略。（本程序后面部分提供了更多相关信息。）

1. 发现范围树分支的策略。

   如果您才刚刚开始，则可以制定一组临时策略，针对未来的威胁提供保护。

2. 发现单个范围的策略。

通常，您将对位于范围树底部或附近的范围执行此操作。这些范围通常包括单个应用的工作负载。

有关详细信息，请参阅自动策略发现和 发现一个范围或范围树分支的策略。

步骤 8 查看并分析您的策略。

仔细检查您的策略，确保它们能达到预期的效果，并且没有意外的副作用。

与组织中的主题专家和应用所有者合作，了解组织的需求以及所建议策略的适当性。

a) 查看 Cisco Secure Workload 建议的策略和集群。

（集群是指范围内密切相关的工作负载组，策略可能需要比针对整个范围的策略更有针对性。有关详细信息，请参阅分组工作负载：集群和资产过滤器。）

有关详细信息，请参阅审核自动发现的策略。

b) 分析您的策略，了解它们会如何影响网络上的实际流量。

使用 Cisco Secure Workload 中的策略分析和其他工具，确认您的策略允许贵组织开展业务所需的流量。有关详细信息，请参阅实时分析。和策略可视化表示。

在分析策略结果时，请记住以下几点：

- 分支较高范围工作空间的策略可能会影响分支较低范围的工作负载。有关详细信息，请参阅策略继承和范围树。
- 微分段可在每个工作负载周围创建一个微型防火墙。为了使连接成功，交易的使用者和提供者都必须制定允许流量的策略。如果两个工作负载不在同一范围内，则创建这些策略可能需要额外的步骤。有关详细信息，请参阅当使用者和提供者处于不同范围时：策略选项。

步骤 9 根据需要反复发现策略。

更多的流量流会产生更准确的策略建议。例如，对于月度报告而言，即使是三周的数据也可能无法捕获所有必要流量。继续发现策略，查看和分析新的策略建议。每次发现运行都会根据当前流量流提出策略建议。

您还可以反复发现策略，以捕获策略发现设置和已批准集群中的变化。有关详细信息，请参阅反复修改策略。

在重新运行自动策略发现之前，请确保已批准要保留的策略和集群。

每次重新发现策略时，都必须对其进行查看和分析。

步骤 10 在准备就绪后执行策略。

在确定与工作空间（以及关联范围）关联的策略适当且将阻止不需要的流量而不中断基本服务后，您可以执行这些策略。

您可以反复执行策略；例如，您可能最初仅在树顶部附近的范围中执行手动创建的策略，然后随着时间的推移，在树中较低的范围中执行发现的策略。

有关详细信息，请参阅 执行策略。

为裸机或虚拟机上运行的工作负载设置微分段

过程

步骤 1 收集网络上工作负载的 IP 地址。

对于每个工作负载，您还需要了解应用名称、应用所有者、环境（生产或非生产）以及其他信息，如决定要应用策略的地理区域。

如果您没有配置管理数据库 (CMDB)，则可以在电子表格中收集此信息。

要开始使用，请选择您可以关注的单个应用。

步骤 2 在支持的基于裸机或虚拟工作负载上安装代理。

有关详细信息，请参阅部署软件代理。

步骤 3 上传描述这些工作负载的标签。

有关详细信息，请参阅工作负载标签和 导入自定义标签。

或者，您可以运行快速启动向导，。有关该向导的详细信息，请参阅快速启动向导。

步骤 4 如有需要，请根据标签创建或更新范围树。

有关详细信息，请参阅范围和资产。

步骤 5 为要应用策略的每个范围创建一个工作空间。

有关详细信息，请参阅工作空间。

步骤 6 创建适用于整个网络的手动策略。

有关详细信息，请参阅手动创建策略。

步骤 7 有关特定于平台的策略的详细信息，请参阅特定于平台的策略。

步骤 8 自动发现与较低级别范围关联的工作空间中的策略。

有关详细信息，请参阅自动策略发现和子主题。

步骤 9 查看并分析建议的策略。

有关信息，请参阅 查看和分析策略 和子主题。

步骤 10 根据需要反复发现策略。

有关信息，请参阅 反复修改策略 和子主题。

步骤 11 准备就绪后，请执行策略。

当您对每个工作空间中策略的行为感到满意时，即可执行策略。

您必须在工作空间和代理配置中执行策略。

有关详细信息，请参阅执行策略。

为基于云的工作负载设置微分段

过程

步骤 1 如有需要，在基于云的工作负载上安装代理。

云连接器在策略发现和执行中提供 VPC/VNet 级别的粒度。如果需要更精细的策略发现和执行，请在支持的平台上安装代理。

根据运行云服务的操作系统安装代理。有关详细信息，请参阅部署软件代理。

步骤 2 设置云连接器以收集标签和流数据。

有关详情，请参阅：

- AWS 连接器。
- Azure 连接器。
- GCP 连接器

步骤 3 为连接器创建的范围创建工作空间。

有关详细信息，请参阅工作空间。

步骤 4 自动发现策略。

发现每个 VPC/VNet 定义范围的策略，并在适用时发现更精细的范围。

有关详细信息，请参阅自动策略发现。

步骤 5 查看并分析建议的策略。

请参阅查看和分析策略以及子主题。

步骤 6 根据需要反复发现策略。

请参阅反复修改策略以及子主题。

步骤 7 为每个范围批准和执行策略。

您必须在适用的工作空间和连接器中为每个 VPC 或 VNet 以及在单个工作负载上安装的任何代理启用执行。

- 有关信息，请参阅 执行策略 和子主题。

- 有关详细信息：
  - 基于 AWS 的工作负载，请参阅对 AWS 资产执行分段策略时的最佳实践。
  - 基于 Azure 的工作负载，请参阅对 Azure 资产执行分段策略时的最佳实践。
  - 基于 GCP 的工作负载，请参阅对 GCP 资产执行分段策略时的最佳实践。

为基于 Kubernetes 的工作负载设置微分段

过程

步骤 1 在基于 Kubernetes 的工作负载上安装代理。确保检查要求和前提条件。

有关详细信息，请参阅 Kubernetes/OpenShift 代理 - 深度可视性和执行。

系统会在适用的 Kubernetes 服务管理的所有未来工作负载上自动安装代理。

步骤 2 为基于 Kubernetes 的工作负载收集标签。

有关详细信息：

- 普通 Kubernetes 和开源工作负载，请参阅Cisco Secure Workload 中的外部协调器和 Kubernetes/OpenShift。
- 在 Amazon Web 服务 (AWS) 上运行的弹性 Kubernetes 服务 (EKS)，请参阅AWS 连接器和在 AWS (EKS) 上运行的托管 Kubernetes 服务。
- Azure Kubernetes 服务 (AKS)，请参阅Azure 连接器和在 Azure 上运行的托管 Kubernetes 服务 (AKS)
- 在 Google Cloud 平台 (GCP) 上运行的 Google Kubernetes Engine (GKE)，请参阅在 GCP (GKE) 上运行的托管 Kubernetes 服务。

步骤 3 根据标签创建或更新范围树。

有关详细信息，请参阅范围和资产。

步骤 4 为要应用策略的每个范围创建一个工作空间。

有关详细信息，请参阅工作空间。

步骤 5 自动发现每个低级范围的策略。

有关详细信息，请参阅自动策略发现。

步骤 6 有关适用的其他选项的详细信息，请参阅特定于平台的策略。

步骤 7 查看并分析建议的策略。

有关详细信息，请参阅查看和分析策略。

步骤 8 根据需要反复发现、查看和分析策略。

有关详细信息，请参阅反复修改策略。

步骤 9 准备就绪后，为每个范围批准并执行策略。

您必须在工作空间和代理中启用策略执行。

有关详细信息，请参阅执行策略和容器上的执行。

下一步做什么

相关信息：

- 工作负载标签
- 范围和资产
- 部署软件代理
- 在 Cisco Secure Workload 中管理策略生命周期
- Cisco Secure Workload 快速入门指南

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。