资产和库存发现

发现是 多云防御的 “**发现**、**部署和防御**”方法的重要组成部分。

发现功能提供对任何已注册云账户中部署的当前资源的实时可视性。此外，它还提供VPC流日志和DNS 日志的接口，以提供云部署的完整视图。 多云防御控制器通过授予 IAM 角色 (AWS)、AD 应用注册 (Azure) 或服务账户 (GCP) 的权限，定期对云资源进行爬网，并密切关注更改，以保持“常青”资源的资产模型。

使用 **发现** 选项卡，您可以查看资源的属性及其互连方式。 多云防御 将这些信息整理到有关配置和流量情景的所有资源的安全状态的简明视图中。

资产

通过授予 IAM 角色 (AWS)、AD 应用注册 (Azure) 或服务账户 (GCP) 的权限， 多云防御 持续维护云资源的“常青”资产模型以及存在于您的与应用高级网络安全相关的云服务提供商账户、订用和项目。资源一旦被发现，即可在工作流程中使用，使管理员能够快速部署安全规则，以缓解应用暴露的风险。任何活动都会立即通过 多云防御控制器报告。

启用资产后， 多云防御控制器 将定期执行完整的资产发现。默认值为 60 分钟，但可调谐。在部署了 CloudFormation 模板的区域上启用了实时资产发现。

发现过程的一部分会突出显示每个云服务提供的日志。请注意每个服务提供商的以下日志类型：

- **AWS** - VPC 流日志、Mount53 流日志和 DNS 日志。
- **Azure** - NSG 流日志。
- **GCP** - VPC 流日志。

请注意， 多云防御 为所有云服务提供商提供相同级别的支持。

应用

应用显示云账户的所有负载均衡器和API网关。在资产的应用部分下，有三个过滤器按钮：**已知标签**、**标签**和**应用**。在**应用**中，用户可以调用工作流程来为特定应用创建和应用保护。

有关如何配置应用标记的详细信息，请参阅 应用标记, on page 2 。

已知标签

已知标签 显示由您的云账户中的应用负载均衡器识别的管理员已通过已知标签识别的应用。这些已知标签在 **设置** > **管理** > **账户** > **应用标签**中列出。

标记

标签显示应用负载均衡器识别的所有应用，其中的字段显示标签密钥和标签值，以及这些应用是否受 多云防御网关保护。

应用标记

创建将用于识别应用的**应用标签**列表。在资产发现期间，所有已发现的具有指定标签的负载均衡器都被视为应用。

例如，您可以将**应用标记**标记分配给充当应用的所有负载均衡器。此标记的值在已发现的资产中显示为 **应用标记** 。请参阅下表作为直观示例：

负载均衡器	标签	值
负载均衡器 1	ApplicationName	计费
负载均衡器 2	ApplicationName	用户管理

已发现的资产将显示已发现的应用资产中的 **账单** 和 **用户管理** 应用。

要创建 **应用标签**列表，请点击 **创建**。

参数	说明
名称 (Name)	预填写。
说明	用户指定的说明。
值	将用于分配给负载均衡器的标记值。

发现的资产

在区域中为云账户启用资产发现时，多云防御控制器会持续发现云资产。要查看已发现的资产，请导航至 **发现** 或 **管理** > **资产**。默认视图显示所有云账户的已发现资产。要过滤到特定云账户，请使用 **选择账户** 指定特定云账户并查看已发现的资产。

已发现的资产类别及其所指的内容如下：

- 安全组 - AWS 安全组 (SG) 和 Azure 网络安全组 (NSG)。
- 网络 ACL - AWS 网络访问控制列表 (NACL)。
- 子网。
- 路由表。
- 网络接口。
- VPC/VNet - AWS VPC、Azure VNet 和 GCP VPC。
- 应用 - 应用由 AWS 应用负载均衡器 (ALB) 识别。
- 负载均衡器。
- 实例 - AWS 实例、Azure 虚拟机和 GCP 计算实例。
- 标签 - AWS 标签、Azure 标签和 GCP 标签。
- 证书 - AWS Certificates Manager (ACM) 证书。

启用资产发现和清点

要启用云账户中的资产发现，请执行以下操作：

步骤 1 导航至 **管理** > **账户**。

步骤 2 选中云账户旁边的复选框，然后点击 **管理资产**。

步骤 3 选择您希望发现 多云防御 的云资产的 **区域** 。刷新间隔是资产刷新前的时间（以分钟为单位）（建议默认值为 60 分钟）。 多云防御 还使用云服务提供商的 API 和事件（而不是常规轮询）执行持续发现。此处指定的刷新时间间隔用于完全重新爬网；这会在实时发现期间协调所有资产的任何遗漏事件。

请注意，通过添加新行并选择所需的区域，可以为不同的区域定义不同的刷新间隔。一个区域只能属于一个刷新间隔。

步骤 4 点击 **完成** 以保存。

Note 多云防御控制器 将在保存后立即请求新添加区域的资产清单。

What to do next

要查看已发现的资产，请导航至 **管理** > **资产**。

Security Insights

见解是对 AWS、Azure 和 GCP 中发现的资产的基于规则的评估，显示为调查结果。可以在不部署多云防御网关的情况下使用见解，因为它们在 多云防御控制器提供的定期和实时资产监控上运行。

步骤 1 在 多云防御控制器 接口中，点击 **添加账户**。作为替代方案，我们强烈建议使用 轻松设置 向导连接到账户。完成相关步骤以连接账户。

步骤 2 连接并激活账户后，请 启用资产发现和清点。

步骤 3 导航至 **发现** > **发现摘要**。此页面显示所有已发现资产和见解 **调查结果**的摘要视图。

安全洞察力类型

通读以下类型的安全见解，了解控制面板的功能。

安全组

客户通常难以应对 **安全组**的激增。安全组通常在可能存在风险的资源之间共享。对用于特定资源的安全组所做的更改可能会影响更大的资源组。

安全组提供所有安全组的列表、安全组的详细信息以及使用安全组的资源集。 **Is Inbound Public** 和 **Is Outbound Public** 字段表示配置了 0.0.0.0/0 的安全组。

在搜索窗口中，根据字段及其值定义搜索条件，并提供基于搜索条件创建规则的选项。

规则

规则根据其配置的入站和出站规则提供安全组的视图。

端口

端口提供基于其配置的入站和出站端口的安全组视图。

网络 ACL

网络 ACL 提供所有网络 ACL 及其详细信息的列表。 **Is Inbound Public** 和 **Is Outbound Public** 字段表示使用 0.0.0.0/0 配置的网络 ACL。

规则

规则根据其配置的入站和出站规则提供网络 ACL 视图。

子网

子网提供所有子网及其详细信息的列表。 **Is Public** 字段根据是否启用自动分配公共 IP 指示可公开访问的子网。

路由表

路由表提供所有路由表及其详细信息的列表。 **Is Inbound Public** 和 **Is Outbound Public** 字段表示配置为提供互联网默认访问的路由表。

网络接口

网络接口提供所有网络接口及其详细信息的列表。 **Is Inbound Public** 和 **Is Outbound Public** 字段表示使用开放的安全组 (0.0.0.0/0) 或允许默认访问互联网的路由表配置的网络接口。

VPC\VNet

VPC/VNet 提供所有 VPC/VNet 及其详细信息的列表。

应用

应用提供所有已部署的应用负载均衡器及其详细信息的列表。 **安全** 字段标识是否应用 多云防御网关 和安全策略来保护应用，并提供调用工作流程来保护应用的功能。

负载均衡器

负载均衡器提供所有已部署的应用、网络和网关负载均衡器及其详细信息的列表。 **公共** 字段显示资源是否为面向互联网的负载均衡器。已启用 **CSP WAF** 显示是否已为应用负载均衡器启用 CSP WAF。

实例 (Instances)

实例提供所有实例的列表，以及有关为资源分配和配置的安全组和接口数量的摘要信息。 **Is Inbound Public** 和**Is Outbound Public** 字段表示具有使用开放安全组 (0.0.0.0/0) 配置的网络接口的实例，或允许默认访问互联网的路由表。

标签

标签提供配置了标签的所有 VPC/VNet、子网、安全组、实例和负载均衡器的列表。

证书

证书提供 AWS 证书管理器中所有可用证书的列表，以及有关颁发者、域名和到期日期的摘要信息。

拓扑

按云账户中的云资产显示高级地图视图。

洞察

见解是对在 AWS、Azure 和 GCP 中发现的资产进行的基于规则的评估，以调查结果的形式显示。

规则

规则是一组用于识别已发现资产中的调查结果的评估。多云防御提供一组默认规则。可以通过以下方式创建新规则：选择资产类别（例如，安全组、应用、负载均衡器、标签等），定义搜索条件，选择 **添加规则** 并指定其他所需信息。导航到 **见解** > **规则** 以查看新规则。在这里，您可以对现有资产和新发现的资产进行操作。

调查结果

调查结果是与定义的规则集匹配的已发现资产的列表。

规则和调查结果

可以将规则配置为对云资源进行检查和防护。

规则和调查结果

可以将规则配置为对云资源进行检查和防护。

预定义规则

多云防御控制器 有一些基本的预定义规则：

- 未启用云服务提供商 WAF 的应用负载均衡器。
- 打开入口的实例很少（<5个）的安全组。许多低利用率的安全组可能会造成难以察觉的漏洞，并可能使其容易被利用。
- 具有两个或多个网络接口的实例。
- 具有开放出站 (0.0.0.0/0) 访问权限的安全组。
- 公共子网 - 启用了 **自动分配公共 IP 的** 所有 AWS 子网。
- 向互联网开放的出口端口过多（25 个或更多）的安全组。
- 向互联网开放的入口端口过多（5 个或更多）的安全端口。
- 在启用公共访问的情况下，为入口打开 65,535 个端口的安全组。
- 30 天后到期的证书 - 仅限 AWS Certificate Manager。

与规则匹配的云资源将被标记为具有匹配严重性的调查结果。

自定义规则

用户可以为资源配置其他规则。

1. 导航到 **发现** > **资产** 并选择资源，例如负载均衡器。

2. 在文本区域中创建规则条件，然后选择 **添加规则**。
3. 输入以下条目的内容以及符合规则条件的结果数量。
    - 名称
    - 说明
    - 严重性
    - 默认操作
    - 类型
    - 账户
4. 点击**保存**。

规则的默认操作可以是 **信息** 或 **警报**。如果规则配置了默认操作警报，则该规则的任何新发现都会导致 多云防御控制器发出警报通知。如果您想要警报的默认操作，则需要以下配置。

- 配置 **警报配置文件** 以指示用户是否需要 ServiceNow、PagerDuty 或 Webhook 通知。
- 配置 **发现类型的警报规则** 和具有指定严重性级别的子类型 **见解规则** 。

调查结果

根据预定义和自定义规则，您可以查看资源的调查结果。为便于访问， **调查结果摘要** 位于控制面板中，也位于“资产”选项卡的“摘要”视图中。

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。