Cisco Secure Cloud Analytics 产品手册

2022 年 12 月

目录

Cisco Secure Cloud Analytics 产品手册

本文档介绍 Cisco Secure Cloud Analytics（此前的 Stealthwatch）的产品概述和订购信息。

有关产品的更多详细信息，请访问 https://www.cisco.com/go/securecloudanalytics。

获得保护公共云、本地部署和混合环境所需的可视性和持续的威胁检测。

产品概述

随着组织将更多 IT 资源迁移到公共云，分散业务服务，并让员工能够从任何地方进行连接，潜在威胁发起者将有更多的机会在不被发现的情况下渗透组织环境。安全组织需要一个能与其安全套件中的其他工具配合使用的解决方案，以便将可视性扩展到其网络和服务的各个角落，并发现潜伏在其日常环境中的潜在威胁发起者。Cisco Secure Cloud Analytics 可提供所需的可视性和威胁检测功能，确保您的组织在从 Amazon Web 服务 (AWS)、Microsoft Azure 和 Google Cloud Platform 等所有主要云环境，到现有本地网络及其连接到这些服务的员工方面的安全性。

Cisco Secure Cloud Analytics 可在不使用代理的情况下，以低干扰提供全面的可视性和高精度警报。Cisco Secure Cloud Analytics 是一种基于云的软件即服务 (SaaS) 交付解决方案。它可检测勒索软件和其他恶意软件、数据渗漏、网络漏洞、系统、事件和配置风险，以及表明受到影响的角色更改，从而提供异常和行为检测，以作为终端检测和云安全解决方案的补充，后者侧重于通过扩展这些资产的可视性来保护个人工作负载和计算机，因此可以更全面地了解状况，更快地捕获威胁，同时缩短响应时间。

为了实现集成和响应，Cisco Secure Cloud Analytics 还配备了具有最广泛且集成度最高的安全平台 Cisco SecureX，以统一可视性、简化威胁响应并实现跨每个入侵载体和无线接入点的自动化功能。

特性和优势

功能	优势
网络和云分析	对设备级的网络流量和通信模式进行完全自动化的实时分析，以获得在公共云和专用网络上运行的所有设备和资源的可视性。
通过高保真的安全警报缩短平均检测时间	提供切实可行的智能建议，同时减少误报，从而实现更智能的安全操作，缩短对威胁进行检测和响应的时间。
内置 SecureX 平台	通过业界最广泛、集成度最高的安全平台来统一可视性，简化威胁响应并实现自动化。
映射到 MITRE 的调查结果	Cisco Secure Cloud Analytics 中的大多数警报都会被映射到 MITRE 策略和技术，从而提供一种了解和响应调查结果的行业标准方式。
软件即服务 (SaaS)	增加了组织大规模部署安全性所需的易用性、部署便利性和灵活性。
实体建模	提供网络上每个设备和实体的行为模型，可用于自动识别表明存在威胁的行为和恶意活动的突然变化。
自动角色分类	根据其行为自动识别每个网络设备和云资源的角色。
无代理部署	使用来自网络和 Amazon Web 服务 (AWS)、Microsoft Azure 和 Google Cloud Platform (GCP) 云实例的本地遥测和日志源，而无需专门的硬件或软件代理。
通过无处不在的可视性缩短平均响应时间	了解网络和公共云中设备的爆炸半径，从而提供一种快速的方法来了解和补救可能已通过安全云分析或其他工具（例如终端安全解决方案或防火墙）发现的活跃事件。

网络可视性至关重要

当今企业正疲于应对安全“盲点”，因为专用网络上的设备数量不断增加，越来越多的工作负载转移到了公共云上。与此同时，安全从业人员面对不断涌入的安全警报也感到束手无策。这就需要重点关注可提供一系列保护的各种安全措施，包括终端、网络和云安全。异常、行为和 IOC 检测都能提供不同级别的可视性，以便在没有哪一种方法可以十拿九稳的情况下捕获攻击者。许多攻击都需要攻击者与网络进行交互才能实现其目标。将这些检测方法和覆盖区域相结合，即可形成更强大的解决方案，用于在攻击者进入组织时对其进行检测，而无论攻击者的攻击手段有多先进。

Cisco Secure Cloud Analytics 可在整个网络和公共云中提供异常、行为威胁和 IOC 检测，从而实现对其他安全产品未覆盖的区域的可视性，同时帮助发现点安全解决方案无法发现的攻击者。Cisco Secure Cloud Analytics 通过使用来自公共云、专用网络的遥测和日志源，然后对行为进行建模以识别威胁活动来实现此目的。

可视性和分析

这些遥测数据会在 Cisco Secure Cloud Analytics 中进行处理，以提供对现代网络（包括专用网络、分支机构和公共云）中所有活动实体的可视性。通过实体建模，该解决方案可以非常精准地检测各种威胁活动。高保真安全警报支持更明智的安全决策，减少错误警报的数量，并缩短进行调查所花费的时间。

灵活性和易用性

Cisco Secure Cloud Analytics 以软件即服务 (SaaS) 的形式交付，易于试用、购买和使用。既无需购买专用硬件，又无需部署软件代理，也不需要任何特殊的专业知识。

从解决方案开始接收数据的那一刻起，就无需进行其他配置或设备分类。所有分析均会自动进行，因此只需很少的管理或安全专业知识即可操作。

用于高级威胁检测的实体建模

在收集遥测数据后，Cisco Secure Cloud Analytics 会创建网络上或受监控公共云中每个活动实体的模型，即一种模拟。使用建模有助于您快速识别早期和隐藏的入侵指标。没有签名列表需要更新，也没有软件代理需要部署。

每个模型都由实体行为的五个关键维度组成：

- **预测：**根据过去的活动来预测实体行为，并根据这些预测来评估观察到的行为。
- **分组：**通过将实体与类似实体进行比较来评估实体的行为一致性。
- **角色：**根据实体的行为来确定其角色，然后检测与该角色不一致的活动。
- **规则：**检测实体何时违反组织策略，包括协议和端口使用、设备和资源配置文件特征以及被列入阻止列表中的通信。
- **一致性：**识别设备在数据传输和访问特征方面严重偏离其过去行为的情况。

实体建模允许解决方案检测与潜在威胁相关的各种行为。例如，Cisco Secure Cloud Analytics 会自动对公共云资源进行分类。这些资源的行为将与类似实体在一段时间内的行为进行比较。这些通信模式可为“正常”行为构建一个基准，如果存在偏离此基准的流量，用户可以通过邮件、其他思科应用来接收自定义警报，甚至还可以通过 Cisco SecureX 平台或其他第三方对威胁采取补救解决方案。Cisco Secure Cloud Analytics 可以识别所有主要公共云提供商的角色。它将近乎实时地检测任何新行为，并会生成包含可疑流量详细信息的警报。

DNS 滥用、地理位置上异常的远程访问、持续的远程控制连接以及潜在的数据库泄露都是 Cisco Secure Cloud Analytics 警报的示例。此外，它还提供包含最常出现的 IP、最常用的端口、具有流量统计信息的活动子网等内容的网络报告。

通过对网络和云的普遍可视性以及利用强大的行为分析，Cisco Secure Cloud Analytics 不仅有助于更轻松快速地发现未知、高级或被遗漏的威胁，而且当威胁被其他安全解决方案（如终端安全性）发现时，这种可见性也能更快地做出反应。

产品/服务

Cisco Secure Cloud Analytics

该解决方案可以在没有软件代理的情况下进行部署，而是依靠本地遥测数据源，例如其虚拟私有云 (VPC) 流日志或 IPFIX 本地部署。Cisco Secure Cloud Analytics 会对组织的资源和功能生成的所有 IP 流量进行建模，而不论这些流量是在 VPC 内部、VPC 之间还是流向外部 IP 地址。它会与 Cloud Trail、云监控、配置、检查器、身份和访问管理 (IAM)、Lambda 等其他云服务提供商 API 集成，以查找网络上的攻击者行为并深入组织云环境。

订购信息

Cisco Secure Cloud Analytics 产品 ID：ST-CL-SUB

许可基于订用，提供 1 个月、12 个月、24 个月、36 个月和 60 个月的期限。此外，还提供 1 个月和 12 个月的自动续约选项。在选择期限选项后，您就能添加公共云监控和/或专用网络监控产品/服务。

若要下单，请联系您的思科客户代表。

面向安全的 Cisco Software Support

面向安全的 Cisco Software Support 的基本在线支持选项适用于 Cisco Secure Cloud Analytics 订用。基本在线支持可在已购软件订用的整个期限内提供基础支持，包括：

通过在线工具获得支持。（不提供电话支持。）

思科将在标准工作时间内不迟于下一个工作日对提交的问题作出回复。

订购 Cisco Secure Cloud Analytics 订用时，基本在线支持将作为该订用的一部分包含在内。它并非一项单独的可订购服务。因此，续订 Cisco Secure Cloud Analytics 订用时，基本在线支持也将续订相同的期限。无需其他产品或费用即可通过 SaaS 订用享受该支持。

有关 Cisco Software Support 的详细信息，请参阅服务说明。

立即着手保护环境

立即免费试用 60 天 Cisco Secure Cloud Analytics，打消您对风险的担忧。要了解更多信息，请访问 https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html，或者联系您当地的思科客户代表。

Cisco Capital

灵活的支付方案，助您顺利实现目标

Cisco Capital 可以帮助您更从容地获得所需技术来实现目标，推动业务转型，并保持竞争力。我们会帮助您降低总拥有成本，以便您保留更多资本用于加速增长。我们灵活的支付方案已覆盖全球 100 多个国家/地区，可确保您以可预测的付款方式轻松购买思科硬件、软件和服务，乃至其他补充性的第三方设备。了解详情。

美洲总部
Cisco Systems, Inc.
San Jose, CA

亚太总部
Cisco Systems (USA) Pte. Ltd.
Singapore

欧洲总部
Cisco Systems International BV Amsterdam,
The Netherlands

思科在全球设有 200 多个办事处。思科网站 https://www.cisco.com/go/offices 中列有各办事处的地址、电话和传真。

990837995 12/22