产品手册

思科公开信息

Cisco Secure Network Analytics (前称 Stealthwatch)

Contents

Cisco Secure 网络分析

本文档介绍 Cisco Secure Network Analytics（前称 Stealthwatch Enterprise）的信息。Cisco Secure Cloud Analytics（前称 Stealthwatch Cloud）产品手册可于此处查看。

有关更多详细信息，请访问： https://cs.co/sna。

解决方案概述

Cisco Secure Network Analytics 提供企业范围的网络可见性，以实时检测和响应威胁。该解决方案持续分析网络活动，以创建正常网络行为的基准。然后，它使用此基准以及非基于签名的高级分析（包括行为建模和机器学习算法）以及全局威胁情报来实时识别异常并检测和响应威胁。Secure Network Analytics 可以快速、准确地检测到威胁（例如网络命令-与-控制 (C&C) 攻击、勒索软件、分布式拒绝服务 (DDoS) 攻击、非法加密货币挖矿、未知恶意软件和内部威胁）。通过使用无代理解决方案，您可以对整个网络流量进行全面的威胁监控，即使流量已加密也是如此。

组织已经在其 IT 基础设施和安全性方面投入了大量资金。然而，威胁仍在不断寻找入侵途径。此外，检测威胁经常需要几个月甚至几年的时间。这种可视性的缺乏是网络复杂性不断增加以及威胁不断演变的结果。而由于资源有限、工具分散，安全团队所能做的工作并不多。实际上，所有组织都有安全解决方案（例如防火墙），但他们如何知道这些工具是否在正常工作、管理和配置？而他们又如何知道这些工具是否执行了需要它们执行的工作？

我们决定解决这个问题 - 为什么不利用您现有的投资（网络）来保护您的组织？网络遥测是丰富的数据资源，可以提供有关连接到组织的用户及其活动的有价值洞察。一切都涉及网络，因此这种可视性从总部扩展到分支机构、数据中心、漫游用户、扩展到私有云和公共云的智能设备。对这些数据进行分析有助于检测可能绕过了现有控制措施的威胁，从而避免它们对您造成重大影响。

解决方案是 Secure Network Analytics，它使网络能够提供本地以及私有云和公共云中流量的端到端可视性。这种可视性包括了解每台主机并查看谁在任何给定点访问了哪些信息。在此基础上，必须了解特定用户或“主机”的正常行为，并建立一个基准，从中可以在用户行为发生任何变化时立即收到警报。

Secure Network Analytics 提供两种不同的部署模式 - 作为硬件设备或虚拟机进行本地部署。Secure Cloud Analytics（前称 Stealthwatch Cloud）是 Secure Network Analytics 的软件即服务 (SaaS) 版本。除了监控专用网络，还可以部署 Secure Cloud Analytics 来检测公共云中的威胁和配置问题。

重要使用案例

实时威胁检测

简而言之，通过提供最全面和情景丰富的网络可视性，再加上经过时间检验的行业领先的安全分析，Secure Network Analytics 可提供最广泛、最高保真的基于行为的威胁检测功能，从而显着改善：

- 未知威胁检测：识别传统的基于签名的工具遗漏的基于行为的可疑网络活动，例如通信和恶意域。
- 内部威胁检测：对数据收集、数据泄露和可疑的横向移动发出警报。
- 加密恶意软件检测：利用多层机器学习，在不解密的情况下扩展对加密 Web 流量的可视性。

- 策略违规：确保实施其他工具中设置的安全和合规性策略。
- 事件响应和调查分析：利用对威胁活动的全面了解、调查分析的网络审计跟踪以及与 SecureX 和其他 Cisco Secure 解决方案的集成，快速有效地做出响应。

远程工作人员监控

Secure Network Analytics 使来自 AnyConnect 网络可视性模块 (NVM) 的终端记录遥测数据成为主要遥测源。这使用户能够捕获各种额外的、特定于终端的用户和设备情景，从而有效地为组织提供对移动远程工作人员终端活动的全面且持续的可视性，无论用户是否使用单个 VPN 会话进行工作，从而优化使用拆分隧道进行远程工作，或者完全断开 VPN 连接。这可以通过对以前不了解的活动的可视性来加强组织的安全状况，例如运行具有需要修补的漏洞的旧操作系统的员工、从事数据收集或数据泄露的员工等。

基于组的策略报告

用户可以利用 Cisco Secure Network Analytics 与 Cisco 身份服务引擎的集成，通过生成基于组的策略报告来加速其基于组的策略采用工作，这些报告提供了可视化组通信的新方法。基于组的策略报告使用户能够轻松地可视化、分析和深入查看任何组间通信，验证策略的有效性，根据其环境需求采用正确的策略，并通过对相关流的见解简化其策略违规调查和关联的 IP。要了解更多信息，请参阅概览。

加密流量分析

迅猛增长的加密流量正不断改变着威胁形势。加密对数据隐私和安全大有裨益，但同时它也为网络犯罪分子隐藏恶意软件和逃避检测提供了机会。如今，大约 95% 的 Web 流量都经过加密，超过 70% 的攻击预计会使用加密。出于性能和资源方面的原因，通过批量解密、分析和重加密进行的传统威胁检测并非始终实用或可行。此外，它还会损害隐私和数据完整性。凭借其在网络基础设施市场的专业知识，Cisco 推出了一项革命性的技术，无需任何解密即可分析加密流量。这使组织能够 1) 检测加密流量中的威胁，2) 确保加密合规性。如需了解更多信息，请访问 https://www.cisco.com/go/eta。

主要优势

- **消除盲点：** Secure Network Analytics 是唯一无需在任何地方部署传感器即可提供整个专用网络和公共云的全面可视性的安全分析解决方案。这是唯一能够在无需解密的情况下检测加密流量中的恶意软件的解决方案。
- **专注于事件，而不是噪音：** 通过使用行为建模、多层机器学习和全局威胁情报，Secure Network Analytics 可显着减少影响环境的关键威胁的误报和警报。
- **即时捕获：** Secure Network Analytics 持续监控网络，实时检测高级威胁。隐身攻击之前通常会执行端口扫描、持续 ping 操作和侦查策略等活动。该解决方案可识别这些早期警告标志和警报，以及早阻止攻击者。识别威胁后，用户还可以进行分解调查，以查明威胁来源并确定威胁可能已传播到何处。
- **充分利用您的投资：** 借助无代理解决方案，您可以使用现有网络基础设施生成的丰富遥测来改善安全状况。
- **随着业务的增长而扩展安全性：** 现在，由于业务需要变化，因此无需牺牲安全性。无论您是要添加新的分支机构或数据中心，将工作负载移至云，还是只是添加更多设备，任何 Secure Network Analytics 部署都可以通过扩展到您的网络需求来轻松提供覆盖范围。它可以部署在本地或云中，可以用作基于 SaaS 或基于许可证的解决方案，并提供自动角色分类功能，以便在新设备添加到网络时自动对其进行分类。

- **将您的安全生态系统与 SecureX 集成：** 该解决方案内置 SecureX 平台，可提供扩展的威胁调查和响应功能。Secure Network Analytics 与 SecureX 平台进行集成，以统一可视性、简化威胁响应并实现跨每个威胁媒介和无线接入点的自动化功能。

解决方案组件

Secure Network Analytics 的核心是所需的组件：管理器、流量收集器和流量许可证。此外，我们还提供流量传感器、Cisco 遥测代理和数据存储等可选组件，这些组件也可用于提供灵活而强大的架构。

系统所需组件

管理器

Secure Network Analytics 管理器可汇聚、组织和提供来自多达 25 个流量收集器、Cisco Secure Network Access（前称 Cisco Identity Services Engine）和其他来源的分析。它通过图形表示网络流量、身份信息、自定义摘要报告以及集成安全与网络情报，供全面分析使用。

管理器的容量决定可以分析和展示的遥测数据量，以及可以部署的流量收集器数量。管理器可通过硬件设备或虚拟机两种形式提供。表 1 列出了管理器的优点。

表 1. 管理器的主要优势

优势	说明
实时更新数据	为同时监控数百个网段上的流量提供数据流，以便您发现可疑的网络行为。此功能在企业层面上尤其重要。
检测安全威胁并确定优先级的功能	通过单一控制中心提供以下能力：快速检测安全威胁并确定优先级、精确查找网络错用行为和性能欠佳之处，以及管理整个企业的事件响应。
管理设备	配置、协调和管理各种 Cisco Network Analytics 设备，包括流量收集器、流量传感器和 UDP 导向器。
使用多种类型的流数据	使用多种类型的流数据，包括 NetFlow、IPFIX 和 sFlow。成果：基于行为的有效网络保护。
可扩展性	支持最苛刻的网络需求。在速度极高的环境中保持出色表现，并且能够保护可通过 IP 访问的每个网络部分（无论大小如何）。
网络事务审计跟踪	提供所有网络事务的完整审计跟踪，提高调查分析研究的效率。
实时可自定义关系流图	提供组织流量当前状态的图形视图。管理员可根据位置、功能或虚拟环境等任何标准轻松构建网络图。通过在两组主机之间创建连接，操作人员能够快速分析在它们之间传输的流量。然后，只需选择有问题的数据点，即可更加深入地洞察在任意时间点发生的情况。
灵活的交付选项	您可以订购物理设备，这是一款可扩展的设备，适合任何规模的组织。 或者，您可以订购虚拟版本，该版本的功能与实体设备版本相同，但在虚拟环境或 KVM 虚拟机管理程序环境中运行。

管理器规格

- Cisco Network Analytics 管理器 2210 – 部件号：ST-SMC2210-K9
- Cisco Network Analytics 管理器 2300 – 部件号：ST-SMC2300-K9
- Cisco Network Analytics 管理器虚拟版 – 部件号：L-ST-SMC-VE-K9

流收集器

流量收集器收集企业遥测技术，例如 NetFlow、IPFIX（互联网协议流量信息导出）、NVM和来自现有基础设施（例如路由器、交换机、防火墙、终端和其他网络基础设施设备）和其他网络基础设施设备的系统日志。流收集器还可以从代理数据源收集遥测，这些数据可由基于云的机器学习引擎进行分析（全局威胁警报）。

对遥测数据进行分析以提供网络活动的全面概况。可以存储数月甚至数年的数据，从而创建审计追踪，用于改进分解调查取证和合规计划。从网络收集的遥测数据量由已部署的流量收集器的总合并容量决定。可以安装多个流量收集器。流量收集器可通过硬件设备或虚拟机两种形式提供。表 2 列出流量收集器的优势。

表 2. 流量收集器的主要优势

优势	说明
威胁检测	采集代理记录并将其与流记录相关联，提供每个流的用户应用和 URL 信息，从而提高情景感知能力。此过程可以增强组织精确找到威胁的能力，缩短平均知道时间 (MTTK)。
流量监控	同时监控数百个网段上的流流量，这样您就能发现可疑的网络行为。此功能在企业层面上尤其重要。
长期数据保留	允许组织和机构长期保留大量的数据。
可扩展性	在速度极高的环境中保持出色表现，并且能够保护可通过 IP 访问的每个网络部分（无论大小如何）。
去重与拼接	执行重复数据删除，任何穿过多个路由器的流仅计数一次。然后，可以将流信息拼接在一起以全面了解网络事务。
交付方法选择	您可以订购 Appliance Edition，这是一款可扩展的设备，适合任何规模的组织。 或者，您可以订购虚拟版本，该版本的功能与实体设备版本相同，但在虚拟环境或 KVM 虚拟机管理程序环境中运行。该解决方案可以根据所分配资源进行动态扩展。

流量收集器规格

- Secure Network Analytics 收集器 4210 – 部件号：ST-FC4210-K9
- Secure Network Analytics 收集器 5210 – 部件号：ST-FC5210-K9
- Secure Network Analytics 收集器 4300 – 部件号：ST-FC4300-K9
- Secure Network Analytics 流量收集器虚拟版 – 部件号：L-ST-FC-VE-K9

Data Store

Data Store 为需要高数据注入容量或超过一个或多个流量收集器容量的长期保留时间的环境提供解决方案。可以在 Secure Network Analytics 管理器和流量收集器之间添加数据存储集群。对于这些更大、更广泛的网络，一个或多个

流收集器会注入流数据并删除重复数据，执行分析，然后将流数据及其结果直接发送到 Data Store。然后，此流数据在 Data Store 中平均分配，Data Store 至少由三个数据节点设备组成。数据存储可促进流数据存储，并将所有网络遥测保存在一个集中位置，而不是将其分布在分布式模型中的多个流量收集器中。与分布式模型相比，这种新的集中式模型可提供更大的存储容量、更大的流量注入和更高的恢复能力。

表 3. Data Store 的主要优势

优势	说明
增加数据注入容量	可以组合数据存储以创建能够监控每秒超过 300 万个流 (FPS) 的单个数据节点集群，以帮助缓解具有高流量的组织的摄取带宽挑战。
企业级数据恢复能力	遥测数据跨节点冗余存储，以便在单节点故障期间实现无缝数据可用性，从而帮助确保不会丢失遥测数据。具有两个或更多数据存储的部署最多可以支持 50% 的数据节点丢失并继续运行。* Data Store 还支持冗余互连交换机，以便在网络升级和意外中断期间保持完全正常运行。 * 取决于您的硬件配置和安装。
显着缩短查询和报告响应时间	Data Store 可显着提高查询性能和报告响应时间，至少比其他标准部署模型快 10 倍。它还可以通过 API 或 Secure Network Analytics 管理器 Web UI 执行更多的并发查询。这些查询改进可显着提高运营效率。通过更快地运行报告和获得答案的能力，Data Store 使从业人员能够更快地查明和响应威胁，以加快分类、调查和补救工作流程。
存储可扩展性	Data Store 通过添加其他数据库集群的能力，为网络不断增长的组织提供了增强的数据存储可扩展性。
长期数据保留	可扩展的长期遥测存储功能可将流量长期保留长达 1 至 2 年，而无需添加额外的流量收集器。这有助于满足监管要求，并降低与购买和集成第三方存储解决方案或额外流量收集器相关的成本和复杂性。

Data Store 规格表

- Cisco Secure Network Analytics Data Store 6200 – 部件号：ST-DS6200-K9
- Cisco Secure Network Analytics Data Store 6300 – 部件号：ST-DS6300-K9
- Cisco Secure Network Analytics Virtual Data Store 6200 – 部件号：L-ST-DS-VE-K9

要了解更多信息，请参阅 Secure Network Analytics Data Store 解决方案概述

美洲总部
Cisco Systems, Inc.
加州圣荷西

亚太地区总部
Cisco Systems (USA) Pte. Ltd.
新加坡

欧洲总部
Cisco Systems International BV Amsterdam,
荷兰阿姆斯特丹

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。

印刷于美国 06/23