Cisco Tetration Analytics

Cisco Tetration Analytics™ 平台可提供全面的可视性、基于行为的应用见解和零信任模式迁移，实现了高效的数据中心运营。

产品概述

借助需要快速部署应用的虚拟化、容器化和工作负载移动技术以及支持应用组件之间不断变化的通信模式，现代数据中心实现了动态化运营。得益于这些技术进步，东 - 西流量占数据中心流量的比例达到 76%。此外，当今的数据中心还要求网络具备高可用性，并可以消除计划停机。这种动态环境带来了三项主要挑战：

- 提供对数据中心基础设施中的流量的全面可视性并实现长期保留数据，以便进行调查和分析
- 了解数据中心内部所有应用的通信和依赖性
- 建立白名单策略模型，实时识别行为偏差，并执行调查分析操作

全新的 Cisco Tetration Analytics 平台可使用算法方法收集丰富的流量遥感勘测数据并执行高级分析，从而成功应对这些挑战。此平台可在数据中心扩展时以线速收集这种丰富的遥感勘测数据。该算法方法包括无人管理式机器学习技术和行为分析，可提供全面解决方案。此平台具备以下优势：

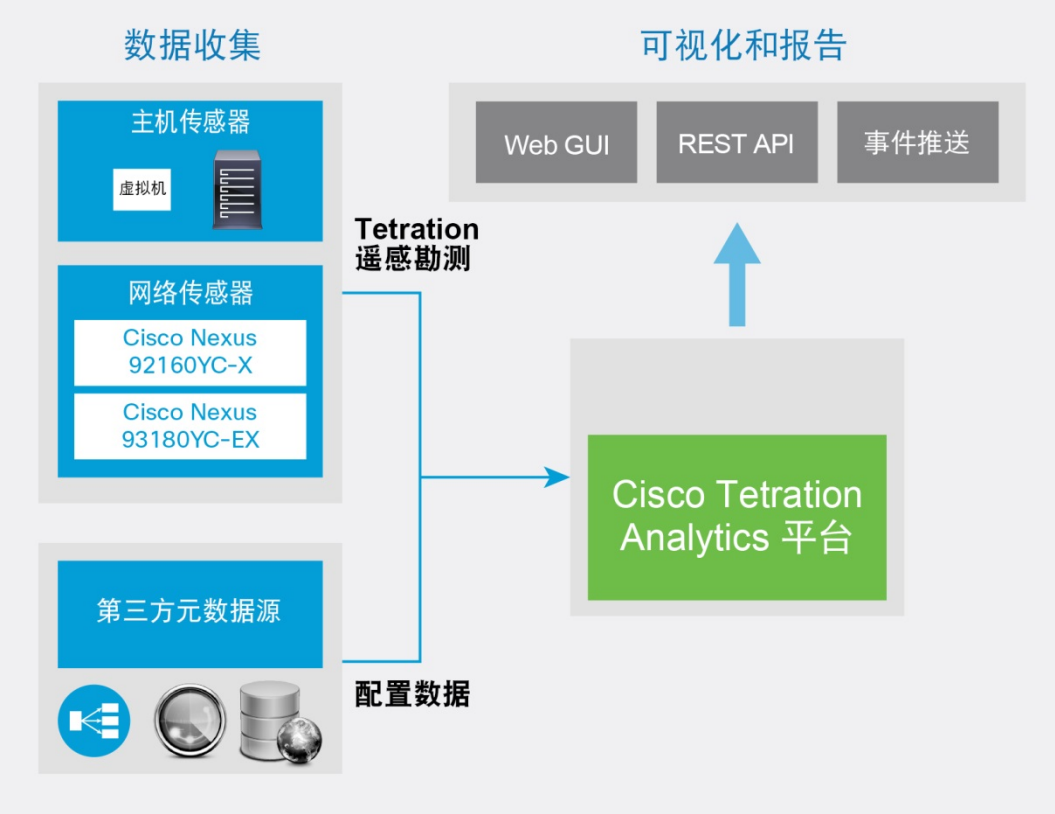
- 每秒能够处理数百万数据流，在几分钟内即可应用智能算法并提供切实可行的见解
- 无需汇聚即可捕捉并存储数千亿条遥感勘测记录，从而支持长期调查分析
- 提供对应用组件及其通信和依赖性的全面可视性，实现网络内部零信任模式

使用传感器收集丰富的 Cisco Tetration 遥感勘测数据。第一版中包含两种类型的传感器：硬件和软件（主机）传感器。借助这两种传感器，该解决方案可同时支持现有（棕地）和新增（绿地）数据中心基础设施。

© 2016 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

图 1 显示 Cisco Tetration Analytics 平台的高级架构。

图 1. Cisco Tetration Analytics 平台架构



Cisco Tetration Analytics 平台包含三个主要功能层：

- **数据收集层：**该层主要由轻型传感器组成，它们可作为分析平台的“眼睛”和“耳朵”。使用两种类型的传感器：
  - 软件传感器或主机传感器：这些传感器可安装在任何终端主机（虚拟化或裸机）服务器中。
  - 硬件传感器：这些传感器嵌入 Cisco Nexus® 92160YC-X、Cisco Nexus 93180YC-EX 和 Cisco Nexus 93108TC-EX 交换机中。

  这些传感器所收集的丰富的 Tetration 遥感勘测数据包括三种类型的信息：
  - **流信息：**该信息包含终端、协议、端口、流开始时间以及流活动时间等。
  - **数据包间变化：**该信息捕捉流内数据包间变化信息。示例包括：TTL 变动、IP/TCP 标记和负载长度变动等。
  - **情景详细信息：**情景信息从数据包信头外部生成。对于软件传感器，该信息包括进程详细信息、生成流的进程、进程 ID、进程相关用户等。

© 2016 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

传感器不处理任何负载信息，且不执行采样。传感器用于监控每个数据包和每个流。除了传感器，该层还包括第三方来源（例如负载均衡器、DNS 服务器映射等），用于收集配置信息。此配置数据用于丰富分析平台所提供的信息。

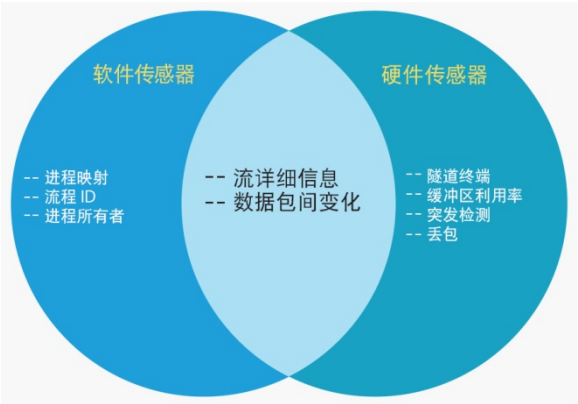
- **分析层：**传感器的数据会发送至 Cisco Tetration Analytics 平台，该平台是执行所有分析的“大脑”。该多服务器大数据平台会处理这些传感器的信息并利用无人管理式导向型机器学习、行为分析和智能算法，为以下使用案例提供全方位体验：
  - 在整个数据中心基础设施中实时提供全面的可视性
  - 根据其行为准确洞察应用组件通信
  - 自动将相似的终端（例如，WebServer 集群、数据库集群等）集中在一起
  - 对应用的白名单策略建议保持一致，及时监控合规性偏差
  - 执行策略影响分析，对其进行测试，然后再将其应用于网络中
  - 长期保留数据以进行历史记录分析，而不损失粒度
  - 利用自然语言搜索和可视性查询进行深入调查分析
- **可视化层：**Cisco Tetration Analytics 平台支持通过易于导航的 Web GUI 界面以及代表性状态传输 (REST) API 消耗此数据。此外，它还提供北向系统可订阅的通知界面，以接收有关流量、策略合规性等通知。

传感器部署和管理

Cisco Tetration Analytics 平台仅可与软件传感器或硬件传感器配合使用。建议尽可能同时启用硬件和软件传感器，因为

- 软件传感器提供与进程相关的情景详细信息
- 硬件传感器提供缓冲区详细信息、隧道终端映射以及检测流量突发的能力
- 准确衡量网络延迟和应用延迟
- 确定流中的丢包及其原因

图 2. Cisco Tetration 遥感勘测 – 硬件传感器对比软件传感器



通过您可能使用的现有自动化方法（Ansible、Puppet、Chef 等），可以进行初始传感器部署。传感器安装并连接到 Cisco Tetration Analytics 平台后，即可使用 Cisco Tetration Analytics GUI 执行包括升级在内的所有后续管理操作。

© 2016 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

特性和优势

表 1 列出 Cisco Tetration Analytics 平台的主要特性和优势。

表 1. 主要特性和优势

特性	优势
轻型传感器	• 硬件传感器和软件传感器组合在一起，可捕捉所有东 - 西流量，从而消除盲点。 • 软件和硬件传感器均位于数据路径范围之外，不会影响应用性能。 • 传感器流量会使带宽开销增加不到 1%。
全面的遥感勘测信息	• 丰富的遥感勘测信息可实现基于应用行为的分析并产生行为偏差。 • 不依赖加密或未加密负载。 • 除了数据包信头数据之外，还提供流情景信息，从而获得更好的见解。
实时流可视性	• 只需不到一秒即可搜索上百亿条流记录，并获得切实可行的见解。 • 加快故障排除和异常检测，以更高效地实现数据中心运营。 • 有效识别应用行为偏差并更好地管理网络策略合规性。
支持数据中心扩展	• 从数据中心的每个数据包收集遥感勘测数据，无需任何采样。 • 平台每秒可以处理数百万条独特流。 • 长期保留数据可实现调查分析及分析操作。
易于部署和使用	• 该设备的工作方式是全方位支持关键运营使用案例。 • 无人管理式机器学习可降低人工交互的需求。
平台安全性	• 通过角色型访问控制 (RBAC) 可对 GUI 和 REST API 进行用户访问控制。 • 使用内置的防火墙全面保护不同平台组件之间的通信安全。
平台自监控	• 自监控使内部不再需要广泛的大数据专业知识，即可操作此平台。 • 监控一直扩展至传感器，可使操作更轻松。 • 使用选项启用 Cisco® Call Home 功能，可报告已知错误状态。
开放式接口	• 将开放式 REST API 用于北向系统集成。 • 使用通知机制，可更轻松地监控基于合规性的活动并检测异常。

数据中心使用案例

Cisco Tetration Analytics 特性和功能支持以下数据中心安全和运营的关键使用案例：

- 对应用组件通信的应用可视性和见解
- 自动化白名单策略建议及影响分析
- 策略合规性及可审核性
- 全面流可视化、探索及调查分析

Cisco Tetration AppInsight

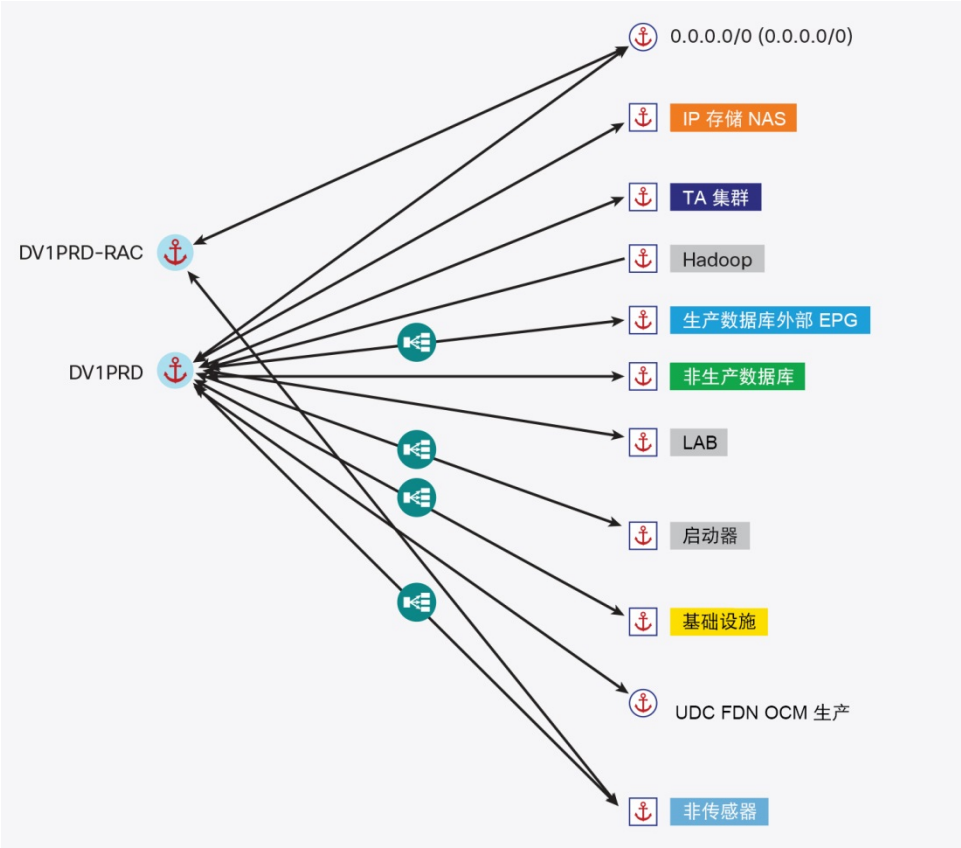
您需要了解数据中心内部的应用组件及其依赖性，以成功运行和迁移应用、执行灾难恢复计划和实施数据中心策略。Cisco Tetration AppInsight 特性可在应用组件之间使用实时数据进行通信，使用行为分析算法来确定应用组及其通信模式和服务依赖性（图 2）。此应用见解功能允许用户和管理员执行以下操作：

- 将终端主机和应用集群集中在一起，以创建应用视图
- 根据通信模式准确地了解消费者和提供商的关系
- 了解每个组件的服务依赖性
- 将标签和标记与终端联系在一起，可便于理解

组织还可以智能地集成第三方设备（例如负载均衡器等）的信息，从而维护应用通信的端到端视图。

© 2016 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

图 3. Web GUI 中的 Cisco Tetration AppInsight 映射



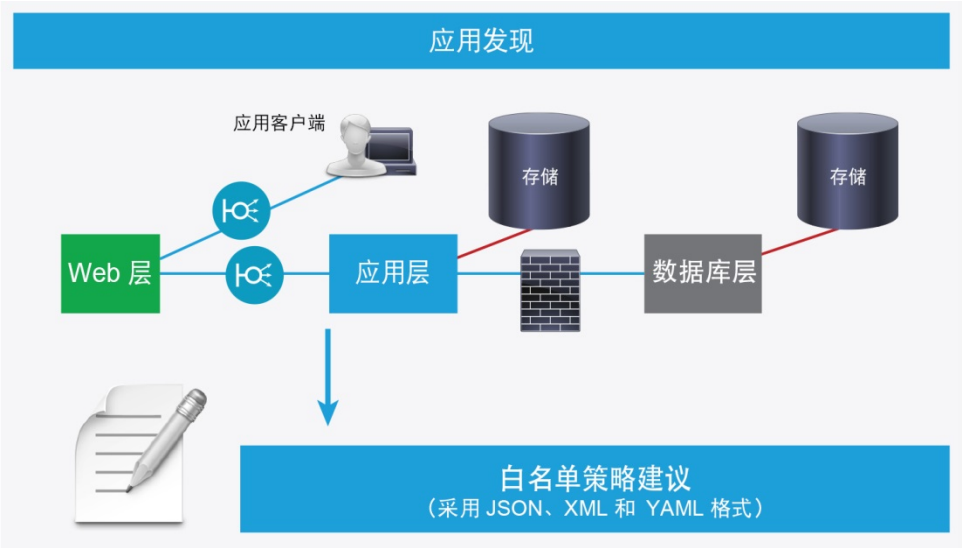
自动化白名单策略生成及合规性

组织需要能够自动生成可靠的白名单策略模型，并随应用发展几乎实现实时更新。此功能可增强安全性，有助于在不同的环境中执行一致的策略，包括在云中运行的工作负载以及更轻松地确定异常。

借助 Cisco Tetration Analytics 平台，您可以根据终端之间的实际通信自动生成白名单策略建议。策略建议能够以三种程序化格式导出：JSON、XML 和 YAML。可将策略导入策略型控制器（例如，思科应用策略基础设施控制器（APIC）），用于策略执行和合规性用途（图 3）。

© 2016 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

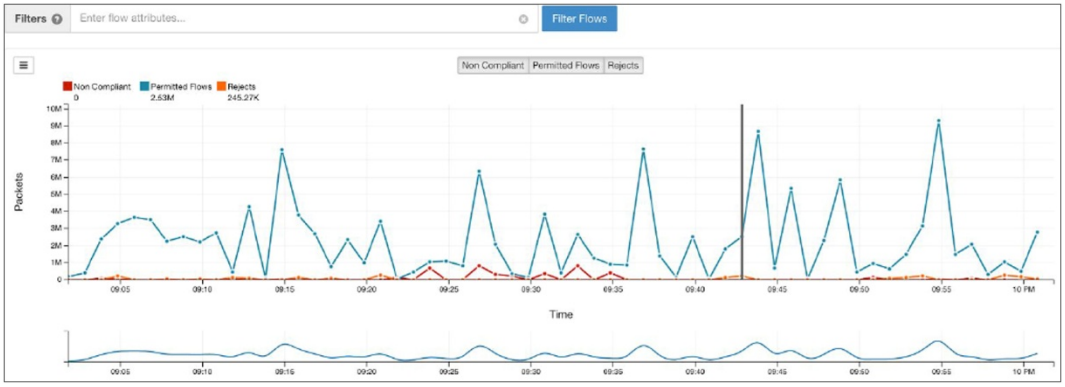
图 4. 自动化白名单策略导出



策略模拟及影响分析

借助 Cisco Tetration Analytics 平台，管理员可以模拟白名单策略并评估其影响，然后再将其应用于生产网络。可使用历史数据或实时数据执行此影响分析，而不会影响生产流量。此功能使管理员能够查看此白名单策略如何影响流经网络的实际流量。此外，管理员还可以立即查看归类为兼容、不兼容或被丢弃的流（图 4）。管理员可使用此模拟和分析功能微调应用映射，并重新生成白名单策略，从而准确反映应用行为。

图 5. Cisco Tetration Analytics 平台上的策略合规性视图

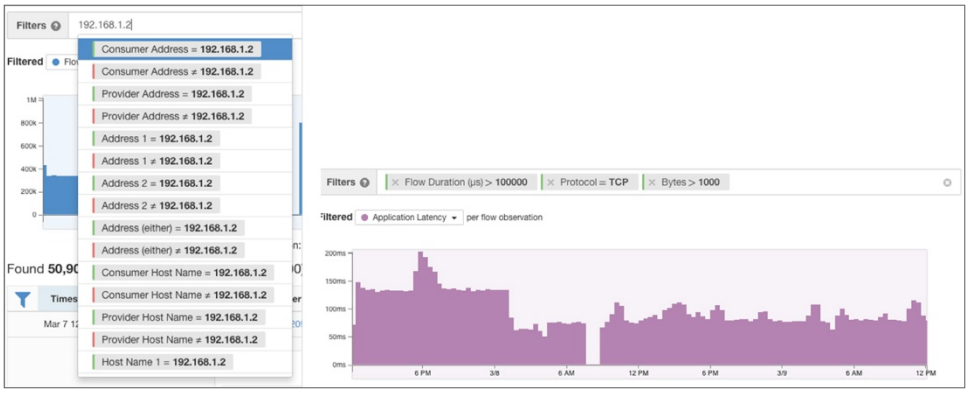


流可视化和探索

Cisco Tetration Analytics 平台可作为数据中心中所有流的搜索引擎。此平台提供的搜索功能非常强大，可使用户在不到一秒之内搜索到上百亿条流记录，并允许通过丰富的自然语言和视觉式搜索查询来查找关键的数据中心运营详细信息。该搜索功能使您不仅能够找到已知问题，还可发现那些通常不被注意的异常行为（图 5）。

© 2016 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

图 6. Cisco Tetration Analytics Web GUI 的调查分析和流搜索



平台自监控

Cisco Tetration Analytics 自监控功能使您能够轻松地管理和操作此平台，而无需任何大数据专业知识。此功能一直扩展至传感器，有助于确保 SLA。平台自监控功能包括：

- 监控平台渠道的流和延迟
- 监控各个平台组件的状态和健康状况
- 传感器健康状况、CPU 和带宽监控
- 可选 Call Home 特性可用于发现已知错误

平台支持和兼容性

表 2 和 3 提供 Cisco Tetration Analytics 平台的软件和硬件支持以及兼容性信息。

表 2. 支持的软件传感器和操作系统

服务器模式	操作系统	分布和发布
虚拟机和裸机服务器	Linux	• Red Hat Enterprise Server 5.3 版及更高版本 • Red Hat Enterprise Server 6.0 版 • CentOS 5.11 版及更高版本 • CentOS 6.0 版 • Ubuntu 12.04、14.04 和 14.10 版
	Microsoft Windows Server	• Microsoft Windows Server 2008 标准版、企业版、基本版和数据中心版 • Microsoft Windows Server 2008 R2 标准版、企业版、基本版和数据中心版 • Microsoft Windows Server 2012 标准版、企业版、基本版和数据中心版 • Microsoft Windows Server 2012 R2 标准版、企业版、基本版和数据中心版

表 3. 支持的硬件传感器

产品线	平台	思科 NX-OS 软件版本
Cisco Nexus 9000 系列交换机	Cisco Nexus 92160YC-X	NX-OS 7.0(3)I3(1) 版及更高版本
	Cisco Nexus 93180YC-EX 和 Cisco Nexus 93108TC-EX	NX-OS 7.0(3)I4(2) 版及更高版本

© 2016 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

产品规格

表 4 列出了标准 Cisco Tetration Analytics 平台的组件规格。表 5 列出了电源规格。

表 4. Cisco Tetration Analytics 平台

标准 Cisco Tetration Analytics 平台包括 36 台服务器和 3 台交换机。Thress 交换机为服务器提供全面的 CLOS 网络。

平台硬件	数量
Cisco Tetration Analytics 计算节点（服务器）	16
Cisco Tetration Analytics 基本节点（服务器）	12
Cisco Tetration Analytics 服务节点（服务器）	8
Cisco Nexus 9372PX 交换机	3

表 5. 电源规格

属性	Cisco Tetration Analytics 平台
Cisco Tetration Analytics 平台的峰值功率（39 RU 单机架选项）	22.5 kW
Cisco Tetration Analytics 平台的峰值功率（39 RU 双机架选项）	每个机架 11.25 kW（总共 22.5 KW）

订购信息

表 6 列出了大型和入门级 Cisco Tetration Analytics 平台的硬件及软件捆绑包 SKU。

表 6. 订购信息：硬件捆绑包

部件号	说明
TA-CL-G1-39-K9	Cisco Tetration Analytics 标准平台，包含 36 台服务器和 3 台交换机，将支持最多处理 5,000 个独特终端（虚拟机或裸机服务器）或每秒一百万个独特流活动（较低的速率）的 Tetration 遥感勘测收集。

表 7 列出了各个终端的软件许可证 SKU。

表 7. 订购信息：独特终端的软件许可证

部件号	说明
TA-BASE-5K-K9=	Tetration Analytics 软件许可证 PID，用于最多 5000 个独特终端（虚拟机或裸机服务器）或每秒一百万个独特流活动（较低的速率）的 Tetration 遥感勘测收集。

借助思科专业知识更快取得成功

思科提供各种专业服务和支持服务，帮助企业从 Cisco Tetration Analytics 平台中获取最大价值。思科服务专家可以提供的支持包括：将 Cisco Tetration Analytics 平台集成到生产数据中心环境；定义与业务目标相关的使用案例；调整机器学习；验证策略和合规性，以提高应用性能和操作效率。适用于 Cisco Tetration Analytics 的思科解决方案支持包括硬件、软件和解决方案级别的支持。只需签订一年合同，即可满足所有支持需求。借助 Cisco Tetration Analytics 服务所提供的专业知识，您将能够更快实现价值，将该平台应用到您的整个环境，实现策略和应用性能的优化，并获得涵盖整个解决方案的全面支持。

© 2016 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

Cisco Capital：提供融资服务，助您实现目标

Cisco Capital® 融资有助于您获得所需的技术来实现目标和保持竞争力。我们可以帮助您减少资本支出，加快增长速度并优化您的投资和投资回报。借助 Cisco Capital 融资服务，您在购买硬件、软件、服务和第三方补充设备时将拥有更多灵活性。Cisco Capital 可以为您提供一种可预测的支付方式。Cisco Capital 融资现已在 100 多个国家/地区推出。了解详情。

更多详情

有关 Cisco Tetration Analytics 平台的详细信息，请访问 http://www.cisco.com/go/tetration 或与您当地的思科客户代表联系。

美洲总部
Cisco Systems, Inc.
加州圣何西

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

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

思科在全球设有 200 多个办事处。 地址、电话号码和传真号码均列在思科网站 www.cisco.com/go/offices 中。

思科和思科徽标是思科和/或其附属公司在美国和其他国家或地区的商标或注册商标。有关思科商标的列表，请访问此 URL： www.cisco.com/go/trademarks 。本文提及的第三方商标均归属其各自所有者。使用"合作伙伴"一词并不暗示思科和任何其他公司存在合伙关系。(1110R)

美国印刷 C78-737256-00 06/16

© 2016 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。