Cisco Intersight 平台的安全性

实现安全可靠的软件即服务管理

目录

安全管理，值得信赖

如果您的 IT 基础设施遍布企业数据中心、网络边缘以及远程和分支机构，在每个位置使用单独的工具会给管理带来重重挑战。Cisco Intersight™ 平台可以统一并简化思科统一计算系统™ (Cisco UCS®) 服务器和 Cisco HyperFlex™ 系统的管理工作。无论您是通过基于云的软件即服务门户还是通过托管在数据中心的设备来访问 Intersight 软件，我们都能帮助您轻松安全地部署、运营和管理您的信息技术。

管理环境瞬息万变

传统 IT 基础设施管理工具使用的是具有多个元素管理器的单点产品。而凭借 Cisco UCS，我们彻底改变了 IT 基础设施和系统管理方式。通过将融合基础设施与基于模型的嵌入式管理相结合，Cisco UCS 可简化和自动化计算任务，使日常运维工作变得更简单、更高效。借助 Cisco Intersight 软件即服务 (SaaS) 和本地 Cisco Intersight 虚拟管理设备，我们的管理覆盖范围得以进一步扩展，现已涵盖部署在任何位置的 Cisco UCS 和 Cisco HyperFlex 系统。

Cisco Intersight 简介

无论您使用的是基于云的门户还是本地设备，Cisco Intersight 都能让您同时拥有基于云的管理优势与可媲美本地系统的安全性。而分析和机器学习技术的应用进一步增强了该管理和自动化平台，使其能够在提升效率的同时不断演进，帮助您有效管理日益复杂的 IT 基础设施。

该软件可监控使用 Cisco UCS 或 HyperFlex 管理系统的各类基础设施组件的运行状况和关系。遥测和配置信息的收集和存储严格遵守思科信息安全要求。系统会隔离您的数据，并通过直观的用户界面为您展示相关信息。由于该软件可轻松扩展，并支持在不影响性能的情况下经常更新，因此，这种简化且一致的基础设施管理方法能有效解决支持常用工具和设备面临的难题（图 1）。

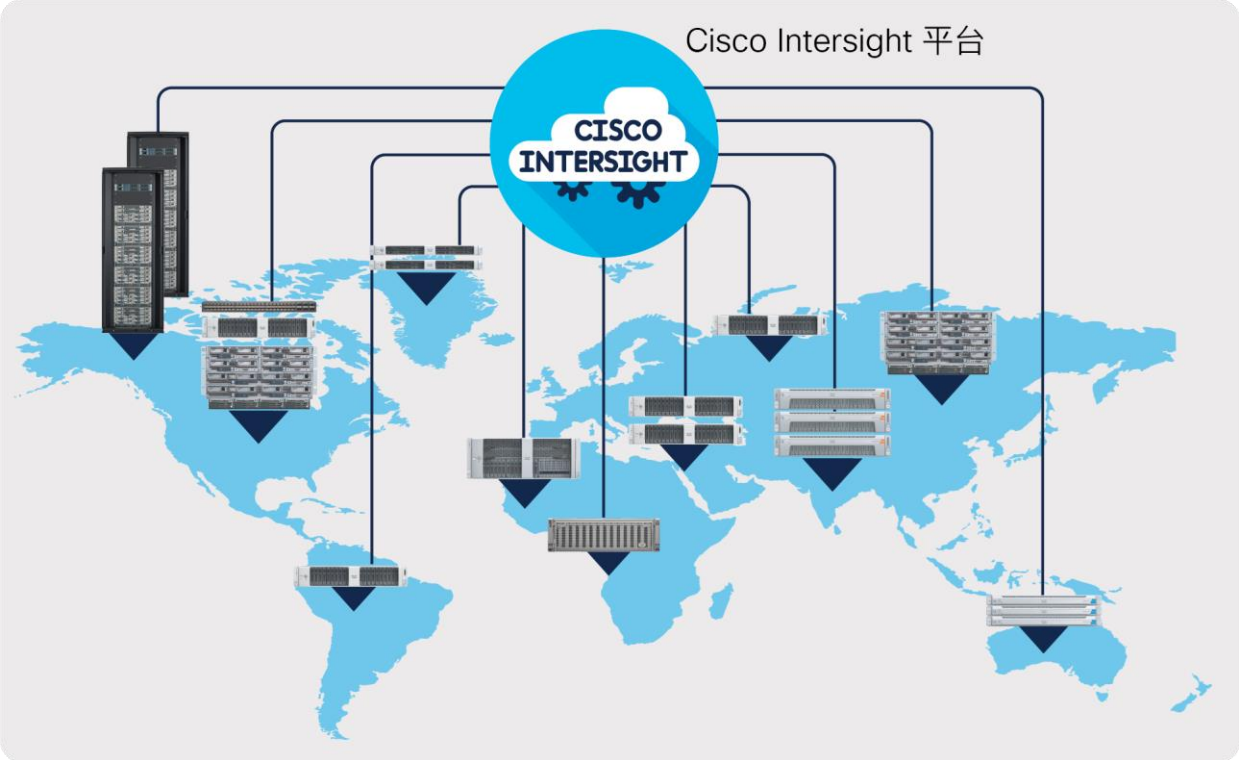

图 1.
无论您的 IT 资源位于何处，Cisco Intersight 都能简化基础设施的管理

Cisco Intersight 平台

Cisco Intersight 软件即服务 (SaaS) 平台可以帮助您将意图（想要实现的目标）转化为基础设施配置，并实现持续管理和主动优化。借助这种基于云的订用模式解决方案，您只需在用户界面中认领服务器、超融合基础设施和交换矩阵互联；激活服务许可；将您的资源分配到逻辑分组中（例如远程或分支机构位置或虚拟集群）；并使用基于角色和策略的界面来配置和管理处于任何位置的资源。

内置安全功能

Cisco Intersight 平台采用基于行业标准安全技术的分层安全架构。此外，该平台还对数据进行加密，遵守严格的思科安全和数据处理标准，并分离管理和 IT 生产网络流量，以实现进一步隔离。因此，基于云的系统管理平台可为您提供所需的强大安全性，让您无任何后顾之忧。

“客户希望使用 API 驱动的集成管理解决方案来持续监控工作负载，优化性能，并协调基础设施运营。这类解决方案应具备可定制的图形用户界面，以及支持大数据的 IT 运营分析功能。”

IDC：全球云系统管理软件预测，2017-2021 年，2017 年 2 月，#US41374417。

安全至上

如今，网络攻击变得日趋复杂和频繁，在这种瞬息万变的网络安全形势下，您的组织必须能够做出迅速响应。在设计 Cisco Intersight 平台之初，我们深知安全至上。为此，我们构建了一个基于云的 SaaS 管理平台，致力于提供满足客户要求的强大安全性。考虑到有些组织更倾向于托管本地管理服务器，我们推出了 Cisco Intersight 虚拟设备，该虚拟设备可提供相同的服务。两者都属于 SaaS，并通过我们的持续集成流程不断更新。

Cisco Intersight 平台的安全性

Intersight 平台的开发、集成和测试严格遵守思科安全开发生命周期准则。这种安全可靠的产品开发和部署实践由多个部分组成，包括固有设计和开发实践、测试实施情况，以及为在充分保障安全的前提下进行部署而提出的一整套建议。思科开发流程已通过 ISO 27001 认证，针对 Intersight 开发的认证目前正在接受审计。

最终，我们在平台中嵌入内置安全保护，保障设备、系统、基础设施和服务的安全。Intersight 建立在互联网商务广泛使用的同一行业标准安全技术之上，采用分层安全架构。Intersight 还对数据进行加密，遵守严格的思科安全和数据处理标准，并分离管理和 IT 生产网络流量，以实现进一步隔离。

单点登录

通过单点登录 (SSO) 身份验证，您可以使用一组凭证登录多个应用。利用 SSO，您可以使用公司凭证而不是思科 ID 来登录 Intersight。Intersight 的 SSO 通过 SAML 2.0 实现，它本身作为服务提供程序 (SP)，可通过与身份提供商 (IdP) 集成来提供 SSO 身份验证。

用户身份验证和基于角色的访问控制

Intersight 账户构成了用户的身份验证域。该账户可以控制所有资源的访问，即使用户已经过身份验证，他们也无权查看账户中未对其授权的任何数据。在 SaaS 平台中，思科登录 ID 可用于对 Cisco.com 的身份提供商进行身份验证，并且支持多因素身份验证。SaaS 和本地 Intersight 的实施都支持与外部身份管理系统集成，以满足现有客户身份验证要求。

Cisco Intersight 框架使用精细访问控制，并按资源管理相应权限。Intersight 软件支持将用户和组配置为多个角色，且每个用户或组都可以是多个角色的成员。实施的角色包括以下权限：

- **账户管理员**：对所管理的 Cisco Intersight 账户和设备具有全面控制和管理权限。
- **只读**：对所管理资源只有查看权限。
- **设备技术人员**：可对设备执行各项管理操作（包括向 Cisco Intersight 账户认领设备）。
- **设备管理员**：可对设备执行各项管理操作（包括从 Cisco Intersight 账户删除设备）。
- **HyperFlex 集群管理员**：具有 HyperFlex 集群生命周期和基于策略的管理权限。
- **服务器管理员**：具有服务器生命周期和基于策略的管理权限。
- **用户访问管理员**：具有用户、组和身份提供商配置权限。

请参阅 Intersight 帮助页面，了解有关管理角色和资源的详细信息。

设备连接

Cisco UCS 和 HyperFlex 系统通过嵌入在每个系统的管理控制器中的设备连接器连接到 Intersight SaaS 平台或本地虚拟设备（图 2）。设备连接器支持对设备向 Intersight 平台发送信息和从中接收控制指令的连接进行加密。

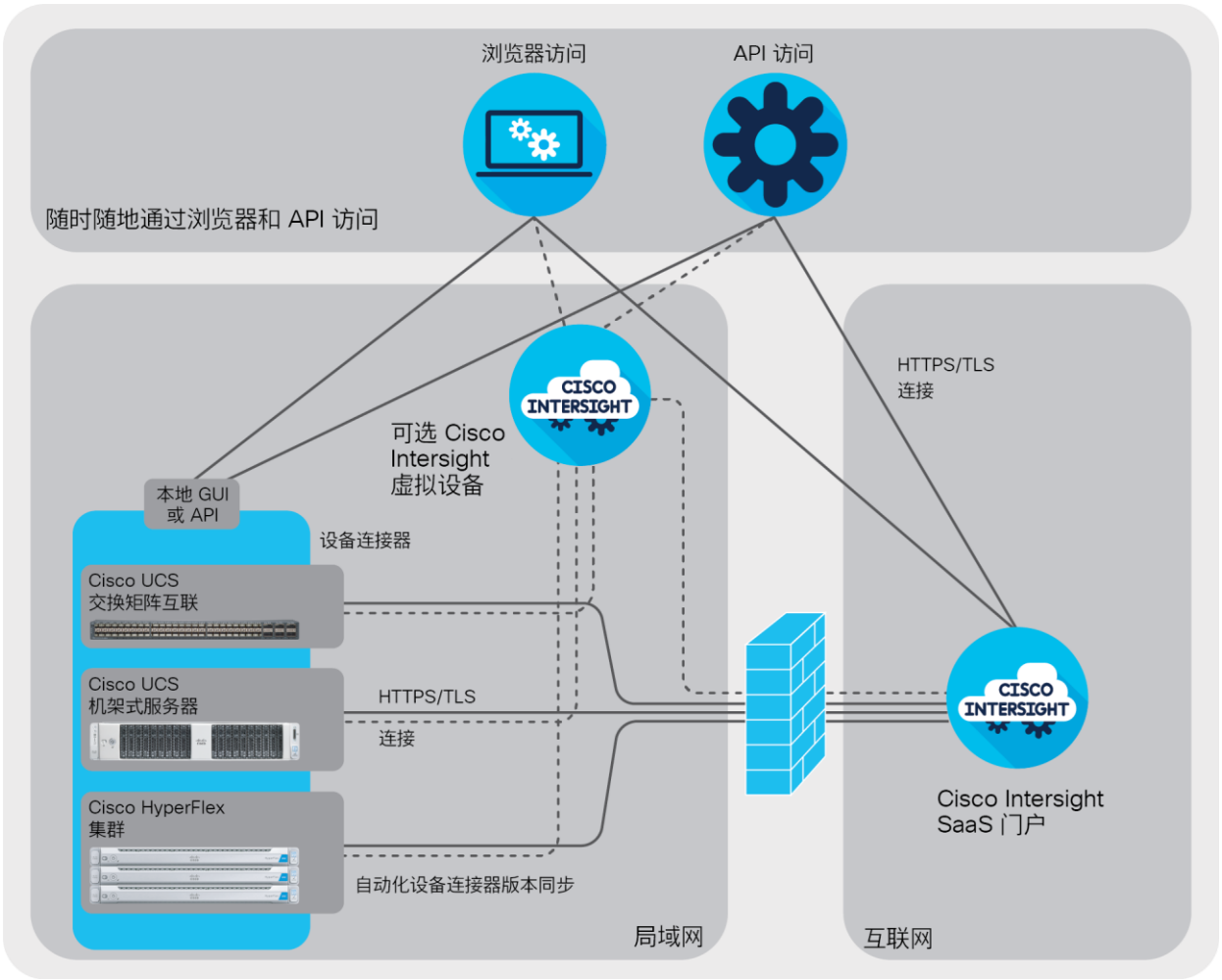

图 2.
Intersight 平台分离用户和设备流量，并使用行业标准 HTTPS 和 TLS 协议进行通信

数据加密和连接安全

设备和 Intersight 平台之间交换的所有数据均使用行业标准加密和安全协议。连接的设备使用传输层安全 (TLS) 协议，该协议对标准 HTTPS 端口 443 应用受限密码和 HTTPS。发送到 Intersight 的所有数据均使用高级加密标准 (AES) 进行加密，其利用 256 位随机生成的密钥，通过公钥机制分发。此外，由于每台连接到门户的设备都使用加密令牌进行身份验证，因此平台只能管理合法设备，这样便消除了潜在的特洛伊木马攻击途径。

由于所有连接均从设备发起，因此防火墙可以阻止所有传入的连接请求；只需为出站连接启用 HTTPS 端口 443。这样一来，用户无需对防火墙进行任何其他特殊配置，即可启用 Intersight 连接。您还可以将设备配置为使用 HTTPS 代理服务器，通过这种间接传输方式增添一层额外安全保护。

为了帮助确保连接安全可靠并防止中间人攻击，直接连接到 Intersight 平台的 Cisco UCS 和 Cisco HyperFlex 设备均使用单目标 HTTPS URL。该平台提供证书颁发机构 (CA) 签名的证书。提交未签名证书的设备将无法连接到门户。Intersight 软件和设备连接器共同创建了一个安全可靠的管理框架，可提供与设备安全相关的实时信息。该方法还允许连接的设备和 Intersight 软件与最新连接安全更新保持同步。

通过双因素身份验证保护设备认领过程

要使用 Intersight 平台监控和管理设备，必须先从 Intersight 账户认领这些设备。可以使用浏览器认领设备，方法是转至 SaaS 或虚拟设备门户，然后点击**认领设备**选项卡。此时系统将从设备中检索设备 ID 和认领代码，两者都是每台设备的独有信息。您可以通过设备的本地管理界面找到设备 ID 和认领代码。认领代码每 10 分钟刷新一次，以进一步确保认领设备的管理员对其具有物理访问权限。

双因素身份验证用于验证要认领的每台设备的身份和真实性。该身份验证机制为设备认领流程增加了一层安全保护。它需要访问设备以及针对您的 Intersight 账户进行验证的设备标识信息。即使有未经授权的用户猜出或获悉设备信息，只要该用户无法对设备进行物理访问，就无法认领相关设备。

认领设备时，用户可以将设备设置为只读模式或允许通过 Intersight 平台进行控制。无论 Intersight 账户中的用户具有何种权限，Intersight 软件都无法修改配置为只读模式的设备。您也可以通过门户，从 Cisco Intersight 账户中取消认领或删除设备。

符合行业安全标准

Intersight 平台满足或超出适用于众多行业标准的信息安全要求：

- **联邦信息处理标准 (FIPS) 140-2：**Intersight 使用符合 FIPS 140-2 的加密模块。相关认证正在计划阶段。

该平台的带外管理架构使其超出某些标准/审核范围：

- **支付卡行业数据安全标准 (PCI DSS)：**客户流量（包括持卡人数据）不流经 Intersight 平台。
- **健康保险转移与责任法案 (HIPAA)：**网络上任何可识别个体身份的健康信息 (IIHI) 都不会发送到 Intersight 门户。

收集的数据和静态加密

与本地 API 访问一样，Intersight 平台对托管的系统具有完全的可视性与可控性。设备连接器在托管系统上收集的数据可能包含以下信息：

- **资产和配置数据：**用于交换矩阵互联以及所有服务器和节点（包括存储控制器、网络适配器、I/O 模块和 CPU）。
- **服务器操作数据**（例如故障）：Intersight 平台可利用该数据提供自动化建议。
- **技术支持文件：**可在思科技术支持中心 (Cisco TAC) 需要时创建。

请注意，设备连接器不会收集可能存储在连接系统中的敏感数据（如密码）。

利用 Cisco Intersight 虚拟设备，您可以控制是否将上述数据传送到基于云的门户。如果选择退出其他数据收集，则上述信息将被保留在本地。Intersight 帮助页面提供有关本地 Cisco Intersight 虚拟设备收集的数据的更多信息。

对收集的所有数据实施以下额外安全实践：

- **客户数据**通过虚拟数据隔离技术实现与其他客户数据的分离。Cisco Intersight 服务发起的数据请求仅返回特定于客户账户的数据，并且在访问时需使用相应客户的加密密钥。
- **长期持久数据**采用静态加密。对所有数据和租户文件启用块存储或类似的卷加密。
- 不允许**第三方访问数据。**

符合思科安全和数据处理标准

保护基础设施和数据需要思科 IT 部门和信息安全 (InfoSec) 组织密切合作。作为思科安全和信任组织 (STO) 的一部分，InfoSec 与思科 IT 部门紧密配合，帮助确保我们构建的产品和运营的基础设施安全可靠。这些团队相互协作，在提升业务效率的同时保护我们的系统和数据免受内部和外部威胁。我们不再只关注硬件和软件层面，而是着眼于整体，采用更广泛的方法加强安全防护，其中包括：

- 使用思科安全开发生命周期准则开发、集成和测试 Intersight。
- 将多个产品开发和部署组件整合到我们的方法中，从固有设计和开发实践、测试实施情况，到最终制定出一套部署建议，力求最大限度确保系统安全性。
- 培养注重安全的文化，缩小受攻击面，打造强健的安全态势。
- 实施以安全为中心的策略和流程。
- 将安全保护融入整个基础设施。

我们对人员和流程给予足够重视，同时针对以下方面实施以安全为中心的策略：

- **访问管理：**我们通过对身份验证、授权和审核采取适当的控制措施，实施对用户和管理员访问信息资产和信息系统的管理要求。
- **审核和风险评估：**我们实施安全和数据完整性策略合规性、调查事件并酌情监控用户和系统活动。
- **云安全：**该服务基于云，而且我们使用的服务必须符合我们的安全要求。

- **加密控制：**我们使用加密控制来保护信息资产的机密性、完整性和可用性。
- **数据保护：**我们规定了对数据进行分类、标记和保护的要求。这些策略定义了信息的相对敏感度，确定了如何处理以及向思科员工和其他各方披露这些信息。
- **信息安全：**我们实施各项策略，这些策略规定了信息资产的机密性、完整性和可用性。
- **网络访问：**我们识别出可以访问我们网络的授权用户和设备。

分离管理网络

Intersight 平台中的带外控制平面将管理数据与 IT 生产和应用数据分离（图 4）。管理数据（如配置、监控信息和统计数据）从设备流向 Intersight 门户（图 3）。IT 生产和应用数据直接发送到生产数据网络上的目标位置。

使用带外架构后，即使设备由于互联网或其他服务中断而无法与 Intersight 软件通信，用户也不会受到任何影响。用户仍可以访问本地管理和生产网络，而且所有 Cisco UCS 和 Cisco HyperFlex 策略和设置仍会继续实施。此外，本地用户身份验证不受任何影响，且 Cisco UCS Manager 等本地配置工具仍然可用。

安全优势

与常用的监控和管理工具相比，Cisco Intersight 平台的管理方法可提供诸多安全优势：

- **高效性：**Intersight 平台减轻了平台管理的责任，使 IT 员工能够专注于其他任务和优先事项。
- **设备连接性：**由 Intersight 管理的设备可自动连接并报告其配置和运行状态，包括其活动固件和软件版本。
- **自主性：**设备建立初始连接后，用户无需在其上进行人机交互。无需安装或者维护代理或其他软件。
- **同步性：**通过自更新设备连接器，每台设备可自动与 Intersight 平台保持同步。可以根据需要将修补程序和安全更新推送到设备连接器，无需用户执行任何操作。
- **分析性：**Cisco Intersight 可根据自动收集的数据，提供必要的基础设施更新建议，以确保您的硬件、固件和软件与思科最新测试组合相兼容。
- **简便性：**Cisco Intersight 提供单一位置，用于跟踪和报告终端安全性和合规性。

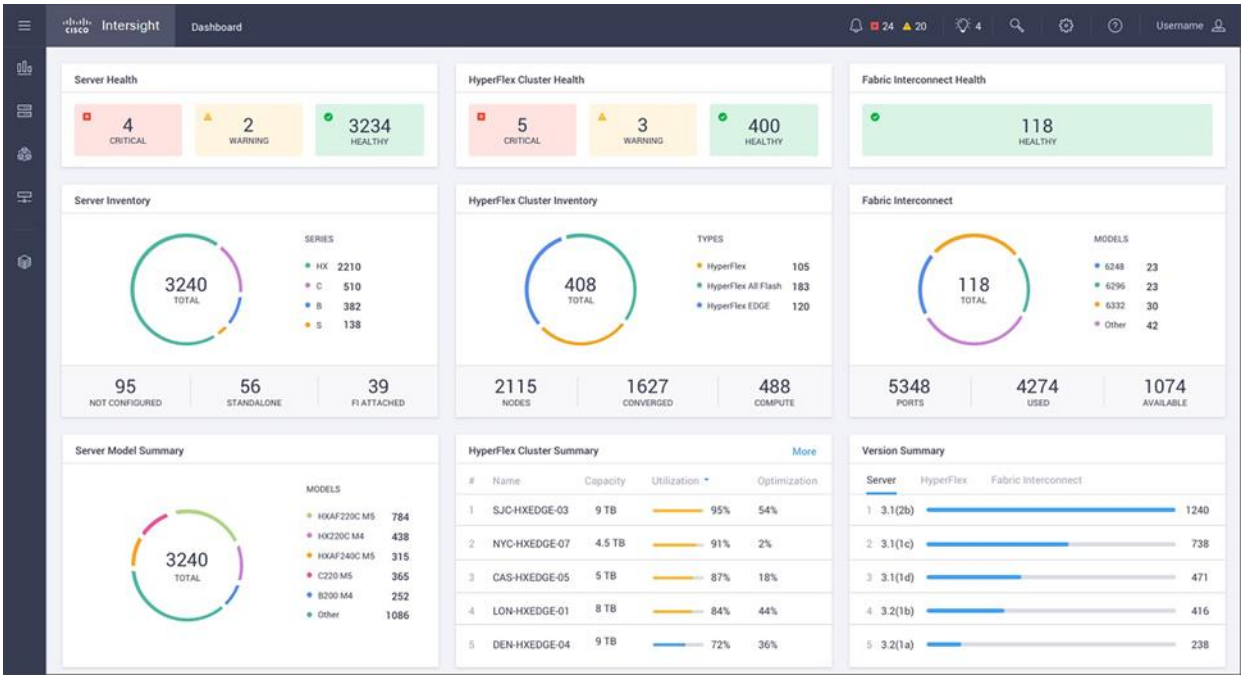

图 3.
Cisco Intersight 控制面板

门户基础设施

您可以通过基于云的门户管理 Intersight。思科工作人员全天候提供后勤安保、运营和变更管理方面的支持。所有服务都会在多个独立数据中心之间进行复制，因此，用户服务能够在数据中心发生故障时快速实现故障切换。

数据中心可靠性和可用性

- 实施跨多个运营团队快速上报问题的规程。
- 采用独立中断警报系统。
- 在数据中心之间复制所有数据（包括指标和设备配置）。
- 在数据中心之间实时复制数据。
- 在出现硬件故障或其他数据中心故障时迅速实现 Intersight 服务的故障切换。
- 利用带外架构，即使在门户连接中断的情况下，最终用户网络功能也能得以保留。
- 定期测试故障切换程序。

安全可靠的带外架构

- 即使连接中断，也不会影响您的 IT 生产或管理网络。
- 仅存储管理网络数据。
- 存储敏感数据时对其进行加密。
- 定期对数据中心进行渗透测试。

数据中心认证与合规性

- 有关数据中心认证与合规性报告的具体问题，请联系 Cisco Intersight 安全和数据隐私团队。

“我们努力做到可靠可信、公开透明、认真负责。因此，我们会不遗余力地探寻基础设施或数据中存在的威胁。”

Michele Guel,
思科杰出工程师
兼首席安全架构师

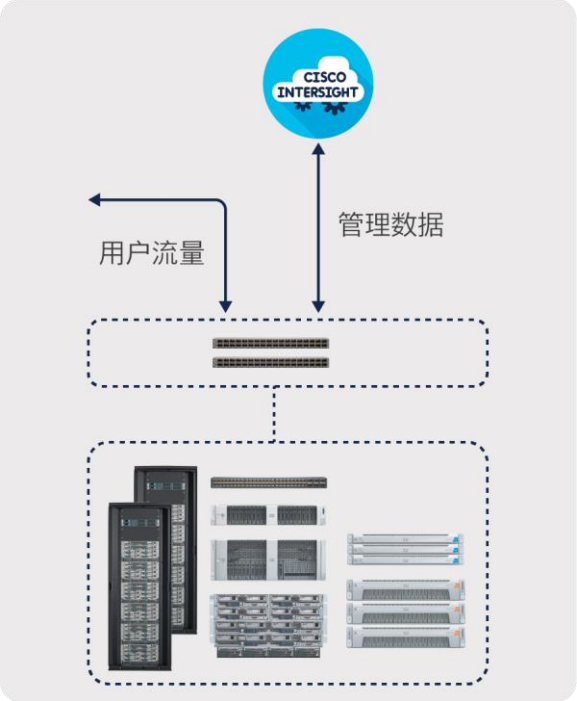

图 4.
流量分离

具备多项安全优势

与本地和基于代理的监控和管理工具相比，Cisco Intersight 平台的 SaaS 管理方法可提供诸多安全优势：

- **高效性：**Cisco Intersight 门户减轻了平台管理的责任，使 IT 员工能够专注于其他任务和优先事项。
- **设备连接性：**由 Cisco Intersight 管理的设备可自动连接并报告其配置和运行状态，包括其活动固件和软件版本。
- **自主性：**设备建立初始连接后，用户无需在其上进行人机交互。无需安装或者维护代理或其他软件。
- **同步性：**通过自更新设备连接器，每台设备均可自动与 Cisco Intersight 保持同步。可以根据需要将修补程序和安全更新推送到设备连接器，无需用户执行任何操作。
- **分析性：**Cisco Intersight 可根据自动收集的数据，提供必要的基础设施更新建议，以确保您的硬件、固件和软件与思科最新测试组合相兼容。
- **简便性：**Cisco Intersight 提供单一位置，用于跟踪和报告终端安全性和合规性。

更多详细信息

要了解有关 Cisco Intersight 平台的更多信息，请访问 https://www.cisco.com/go/intersight。

要了解有关思科运营安全方法的更多信息，请访问 https://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/cs-sec-03232016-operational-security.html。

要了解有关 Cisco UCS 的更多信息，请访问 https://www.cisco.com/go/ucs。

要了解有关 Cisco HyperFlex 系统的更多信息，请访问 https://www.cisco.com/go/hyperflex。

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。

美国印刷 C22-744638-00 01/21