使用一个许可证监控全部技术一个许可证

我们的客户友好、基于点的许可让您可以灵活地监控网络、服务器、虚拟机、应用、配置或流量的任何组合。您可以随时按自己需要的频率更改监控混合。不必纠缠于不使用的特定技术许可证。

网络传输流量分析

分析并监控带宽消耗和网络流量

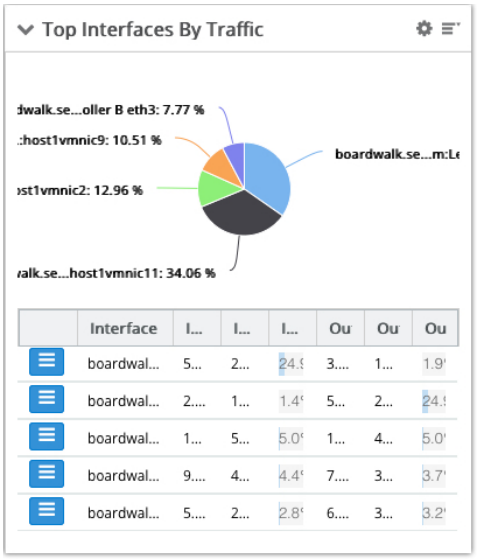
网络流量分析是 WhatsUp Gold 的 Total 和 Total Plus 版包含的功能，可以让用户详细了解带宽使用模式。我们标准版、高级版、MSP 和销售版以流量监视器附件的形式提供拟化监控功能。

我们的网络流量分析模块提供了关于网络流量和带宽消耗的详细且可操作数据，有助于您制定并实施宽带使用策略、控制 ISP 成本、保护网络，以及提供用户、应用程序及业务所需的网络容量。它不仅显示了局域网、广域网及互联网的整体利用率，也表明哪些用户、应用程序及协议正在消耗带宽。

详细了解带宽使用模式

监控您的网络流量

网络流量分析模块从网络上的任何具有流量功能的设备收集网络流量和带宽使用数据，它支持 Cisco NetFlow、NSEL 协议、Juniper Network J-Flow，以及 sFlow 和 IPFIX。它是唯一支持 Cisco NetFlow-Lite 的工具，且无需使用第三方聚合器将流记录从 NetFlow-Lite 转换为网络流格式。



详细了解以下相关的网络流量信息：

- 发送者、接收者及对话
- 发送者和接收者网域
- 发送者和接收者国家
- 应用程序和协议
- 传入和传出接口流量
- 传入和传出接口利用率
- 主机和群组的带宽使用率

为 Cisco CBQoS（基于等级的服务质量）和 NBAR（基于网络的应用识别）收集数据。

接收有关网络流量的警报

网络流量分析模块提供基于阈值的警报，帮助您在用户、应用程序及业务受到影响之前解决网络流量问题。当发送者或接收者超过带宽阈值、接口流量超出利用率阈值，以及当失败连接和伙伴对话阈值超出时，其将发出警报。

利用网络流量分析模块，您可以创建协议流量的自定义警报，比如 UDP 流量的瞬间峰值可能意味着网络中发生拒绝服务攻击 (DoS)。您可以创建应用流量的自定义警报。例如，当用户在 YouTube、Spotify、英雄联盟等非业务应用上消耗大量互联网带宽时，您将收到通知。您甚至可以为主机流量创建自定义警报。例如，当包含敏感数据资产的大文件通过互联网传输时，您将收到警报。当用户超过带宽使用阈值时将会收到警报。