

思科 Stealthwatch 代理集成服务



优势

- 将代理服务器上的代理记录集成到大部分数据库（例如 SQL 或 Hadoop 数据库）。通过查询数据库对所需数据进行检索和分析，从而帮助安全团队定位潜在的恶意外部站点。
- 查看从内部主机到代理再到外部 URL 的通信，从而提供对网络上的用户活动的 100% 可视性。
- 查询思科® Stealthwatch 以查看访问潜在的恶意外部 URL 的内部主机数量，并确定用户身份、用户访问网站的时间、已发送或已收到的数据量（如有），以减少数据丢失和不良站点感染。
- 对于不合规的网络使用行为，系统会基于所访问的 URL 或域名向安全团队发出警报，从而避免发生违反公司政策的情况。这有助于保持网络安全性和合规性。
- 对代理服务器上的命令和控制通信进行快速而准确的调查分析，以改善整体安全状态。

代理服务器集成提供精细的可视性和情景信息

使用思科 Stealthwatch 代理集成服务可将几乎任何 Web 代理与思科 Stealthwatch 流量收集器集成，并扩展内部主机之间、代理服务器之间及外至公共互联网和公共 Web 服务的网络可视性。这种端到端网络可视性能够跨越 Web 代理，有助于扩展网络保护范围，增强威胁检测，并通过集成服务提供的精细可视性降低公司风险。代理集成服务使代理服务器深度集成到网络，以对命令和控制活动、潜在的恶意主机和自定义警报进行更为详细的查询。此定制设计的集成服务充分利用代理服务器提供的功能和数据。

借助我们的专家团队，您可以优化 Stealthwatch 的操作并推动与内部业务策略的成功集成。代理集成服务可提供增强的安全情报、优化的网络性能和更高的投资回报。

通过将思科 Stealthwatch 与 Web 代理服务器集成，可为您的整体状态增加额外的情景、保护和安全层。

我们的思科 Stealthwatch 代理集成服务包含 Web 代理与思科 Stealthwatch 流量收集器集成所需的代理适配器组件和相关服务。代理适配器侦听传入的系统日志消息，然后在发送至流量收集器之前将其转换为 NetFlow 记录。适配器通过提供详细的应用信息，为穿越代理的 Web 流量提供可视性。这类信息包括 URL 和域信息，可表明访问的用户、所访问的网络服务，以及访问时间。

适配器在虚拟机或实体服务器上运行，并将代理系统日志消息转换成 NetFlow 记录供流量收集器进行分析。您能够：

- 将 Web 代理与 Stealthwatch 流量收集器集成，将网络可视性扩展至内部客户端和外部 Web 服务器之间的拼接流，从而提高对外部互联网的可视性。
- 通过对访问代理的用户以及所访问的 URL 的可视性，做到心中有数。
- 与支持的代理服务器无缝集成，以获得对流量收集器中数据的可视性。
- 自定义和集成几乎所有可用的代理服务器，以实现最大的灵活性。
- 确保所有流向互联网的流量都按照公司政策的规定使用代理，以防止发生违反政策的情况。

专业服务需要五天的时间与您的团队一起完成集成。该服务可在现场或通过虚拟会话提供，最多为四个代理服务器提供集成帮助。服务完成后，我们会召开知识传达会议，并且会提供有关如何执行该服务的文档，以便安全团队进行未来的集成。

思科安全 Stealthwatch 代理集成服务可助您实现跨 Web 代理的端到端网络可视性。这能够扩展网络保护范围并提高 Stealthwatch 部署的投资回报率，以便您的组织更加了解代理流量。其结果是实现一种更加安全、恢复能力更强的网络。

后续行动

要了解有关思科安全服务的更多信息以及我们的 Stealthwatch 部署服务如何使您的企业受益，请联系您当地的客户代表或经授权的思科分销商。有关思科如何帮助您的组织防护当今不断变化的威胁的更多信息，请访问 www.cisco.com/go/services/security。