Umbrella控制面板：新功能和文件检测

目录

简介

本文档介绍新的Umbrella控制面板。

注意到您的Umbrella控制面板有任何不同之处吗？我们很高兴地宣布，我们正在启动将人员转移到一组新的很棒的Umbrella功能的过程。我们引入的第一个功能是文件检测。文件检测扫描身份下载的文件以查看它们是否包含恶意代码，如果包含恶意代码，则将其阻止。

为了帮助您利用此新功能，我们还发布了新的和更新的安全报告以及新的策略创建体验。这是我们为未来版本规划的几项功能之一，这些版本旨在提升我们的智能代理基础设施，以便为我们的用户提供更多基于云的安全性。

这些功能正在逐步向我们的客户推出。如果您在控制面板中收到有关这些功能的警报，您就会收到这些功能！如果您希望率先采用这些功能，请联系umbrella-support@cisco.com。

文件检查功能仅适用于具有Umbrella Insights或Umbrella平台套件的客户。单击此处阅读有关套件的详细信息，如有问题，请联系您的思科客户代表。

太好了，我怎样才能利用文件检查呢？

策略向导允许您在摘要页面或在创建新策略时启用文件检查。

在报告端，Umbrella控制面板的“报告”(reports)导航部分已更新，以便您可以轻松地找到我们新的和更新的报告。让我们来了解一下如何启用该功能并查看一些报告。

启用文件检查

文件检查是智能代理的一项功能，通过增加扫描文件以查找可疑域中托管的恶意内容来扩展其范围和功能。可疑域既不可信，也不知道是恶意的，它列于我们的“灰色列表”中。

使用Umbrella策略向导，文件检测易于实施。只需导航到策略(Policies)>策略列表(Policy List)，然后展开策略或点击+（添加）图标创建新策略。在策略向导中，确保在摘要页面上启用文件检查，或在启用智能代理后（在“高级设置”下），从新策略中确保选中检查文件。 此功能的完整文档可从以下位置找到：https://docs.umbrella.com/deployment-umbrella/docs/file-inspection

我们建议启用SSL解密以充分利用此功能。

测试文件检查

从已在启用了文件检查的策略中注册的设备：

1. 浏览 http://proxy.opendnstest.com/download/eicar.com。
2. 系统将显示如下所示的阻止页面：

文件检测报告

为了帮助更好地了解被阻止的内容（以及何时、为何和如何），我们在Umbrella中更新了一些报告，包括修改后的安全活动报告：

- 安全概述报告
  通过图表可以轻松读取网络活动的快照。您可以快速查看身份及其流量发生的情况，说明问题可能发生在何处。请点击此处了解有关的更多信息。

- 安全活动报告
  突出显示Umbrella威胁情报已标记但不一定阻止的安全事件。这包括通过智能代理和文件检查过滤的安全事件。此报告在显示被阻止的内容、原因和方法方面尤为重要。请点击此处了解有关的更多信息。

- 活动搜索报告
  帮助您从各种身份中查找每个DNS、URL和IP请求的结果，按降序日期和时间排序。此报告列出所选时间周期内Umbrella中的所有活动，通过使用过滤器，您可以改进搜索以仅查看想要查看的内容。请点击此处了解有关的更多信息。

通过我们最新更新的导航，这些报告也很容易获得！ 只需展开左侧菜单窗格，然后直接从控制面板中的任意位置跳至任何报告。

我怎么能告诉你我的想法？

我们很想听听您对这些新功能的看法。如果您有任何疑问或意见，我们希望收到您的回复！将您的反馈发送至umbrella-support@cisco.com，并尽可能详细地提供您的反馈。例如，屏幕截图、您使用的浏览器、您的操作系统和您使用这些功能的场景。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。