为生成AI和ChatGPT配置DLP和CASB支持

目录

简介

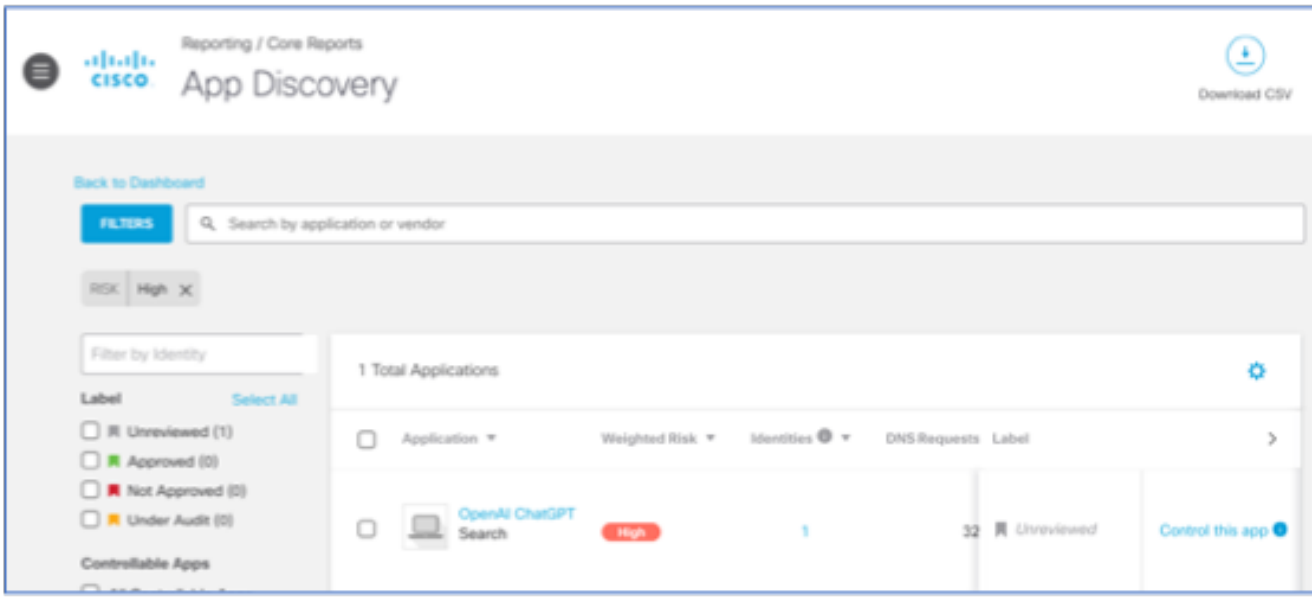
本文档介绍对生成AI和ChatGPT的云访问安全代理(CASB)和数据丢失防护(DLP)支持。

概述

Umbrella 产品套件中发布了全新的云访问安全代理(CASB)和数据丢失防护(DLP)增强功能，旨在帮助客户更有效地管理其组织内的ChatGPT使用。
这些增强功能使我们的客户能够确保他们的员工负责任且安全地使用ChatGPT，同时保护敏感信息免受潜在风险的侵害。

以下是主要功能：

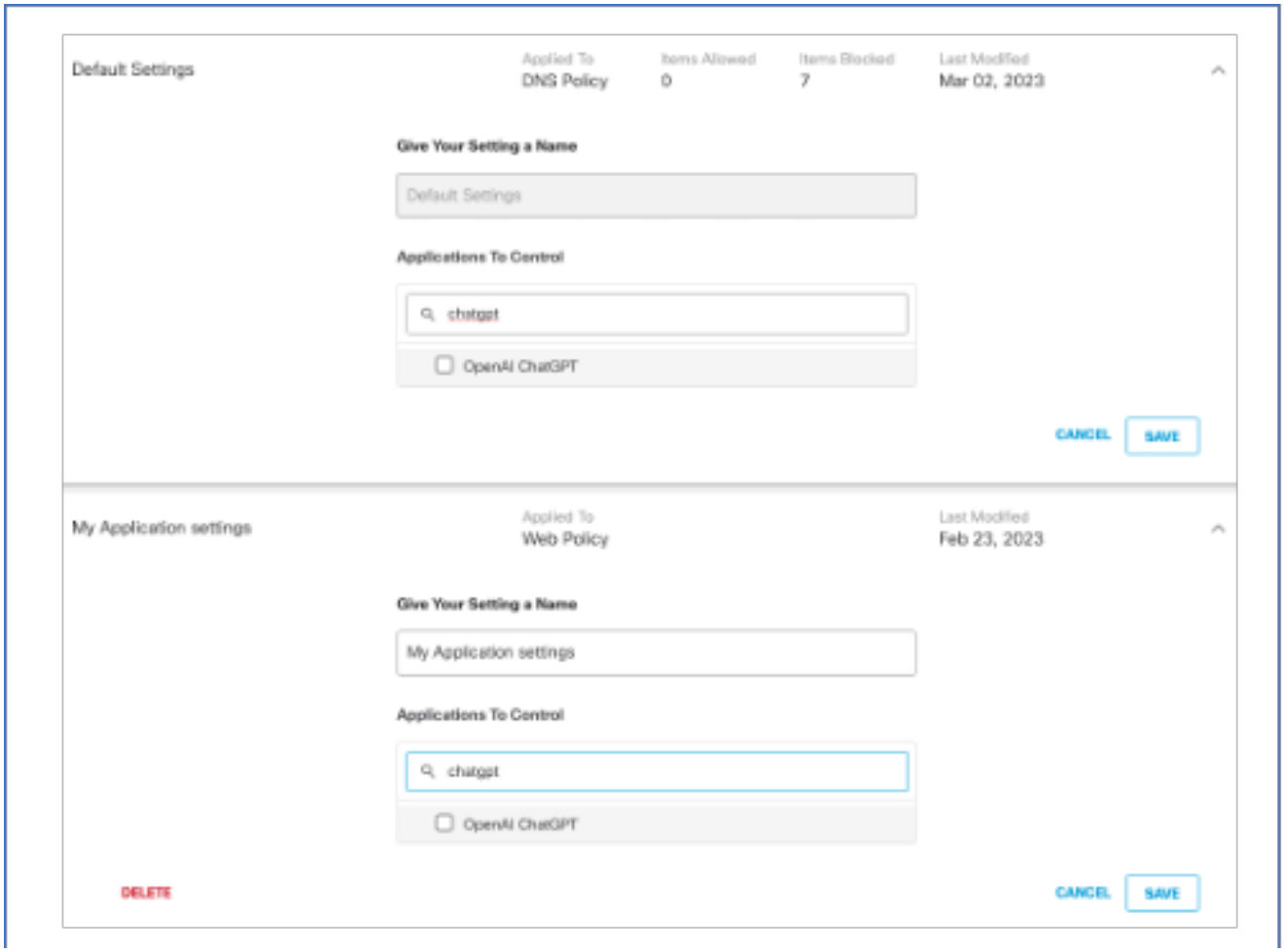
1. 发现组织中的ChatGPT使用情况：
   使用应用发现报告(Reports -> Core Reports)，客户可以识别和监控其组织中的ChatGPT使用情况。
   这让他们能够深入了解员工如何使用工具，使他们能够优化工具的使用并确保符合其内部策略。



16221272854164

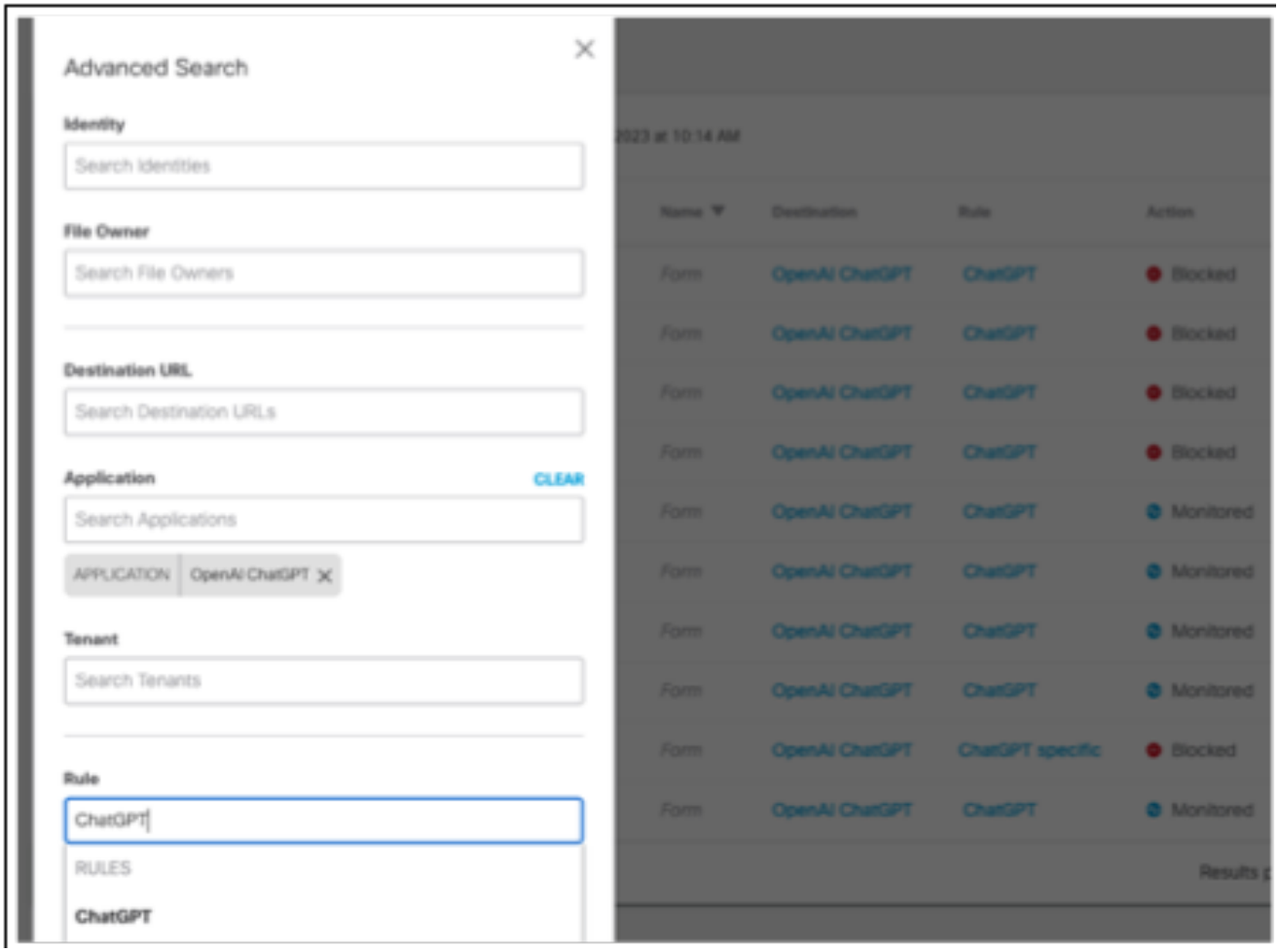
16221291406100

2. 对ChatGPT访问的精细控制：
现在，客户可以阻止每个人访问ChatGPT，或只允许特定用户或用户组访问。
此精细控制有助于根据安全和合规性要求管理ChatGPT的使用。 通过在Application Settings中选择openAI ChatGPT，可以通过DNS和Web策略进行阻止。



16221268217748

3. 使用DLP评估ChatGPT使用风险：
现在，实时DLP使客户能够监控与ChatGPT发送和共享的敏感信息的类型。这有助于评估与ChatGPT使用相关的风险，并采取适当的措施来减少潜在的数据泄露或泄露.
要启用ChatGPT的DLP监控，客户可以利用目标设置为All Destinations的实时规则，或者专门从可用应用程序列表中选择openAI ChatGPT。



16221283948052

4. 允许使用DLP安全使用ChatGPT:
   通过使用我们的DLP解决方案，客户现在可以阻止包含敏感信息的ChatGPT提示。这可确保员工继续安全安全地使用ChatGPT，而不会将组织暴露在潜在风险中。
   要对ChatGPT启用DLP阻止，客户可以利用目标设置为All Destinations的实时规则，或者专门从可用应用程序列表中选择openAI ChatGPT。

16221311959572

5. 防止源代码泄漏到带有DLP的ChatGPT:
   通过新的源代码数据标识符，客户可以使用DLP监视并停止与ChatGPT共享源代码，从而保护他们的宝贵知识产权(IP)。

6. 新的创成AI应用类别：
   引入了一个新的创成式AI应用类别，以解决更广泛工具的使用发现和防御问题。

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）。