安全访问中WhatsApp的DLP策略限制

目录

问题

思科安全访问中的DLP策略在通过WhatsApp（浏览器或桌面应用）共享时不会检测或阻止敏感文件，尽管已启用HTTPS解密。DLP引擎无法通过这些平台触发或检测文件上传，而相同的DLP策略在通过其他在线上传工具上传时成功阻止相同的文件。当测试WhatsApp的基本上传阻止时，该功能在浏览器和桌面版本上均正常工作，但这个问题与DLP策略实施密切相关。

环境

- 思科安全访问
- 已配置DLP策略
- HTTPS解密已启用
- WhatsApp Web和WhatsApp Desktop应用程序

分辨率

观察到的行为是WhatsApp和类似平台由于实施端到端加密(E2EE)和非标准流量处理而产生的预期限制。可以实施以下各节中概述的故障排除步骤和解决方法。

故障排除验证步骤

在实施解决方法之前，请验证以下配置项：

- 确保配置了正确的SWG身份/源ID。
- 确认已为目标平台启用HTTPS检测/解密，并且没有选择性地绕过。
- 验证隔离/RBI和Allow-Override设置是否已正确配置。
- 如果DLP策略是基于组，请确认AD组成员。
- 检查Traffic Steering bypass lists以查找任何排除项。
- 验证浏览器中是否禁用了QUIC协议。
- 检查可以绕过检测的IPv6流量影响。

建议的解决方法

要对WhatsApp Web流量启用DLP实施，请对发往WhatsApp Web的流量实施远程浏览器隔离(RBI)。此解决方法允许通过隔离浏览器会话并在隔离环境中启用内容检查来实施DLP策略。

专门为WhatsApp Web域配置RBI实施，以确保通过Web界面上传和共享内容时遵守DLP策略评估。

Additional Information

已针对此限制记录产品增强请求 — CSE-I-1249。

原因

WhatsApp（包括WhatsApp Web）和类似的协作平台实施端到端加密(E2EE)，可防止消息文本和文件上传的全面内容检测和扫描。此外，WhatsApp流量使用标准HTTP/HTTPS端口的方式与典型的Web上传不同，这意味着安全Web网关(SWG)无法拦截和检查通过正常HTTPS检查路径的流量。这种加密和流量处理方法经过设计，代表了对这些特定平台的当前DLP检测功能的预期限制。

相关内容

- 产品增强请求CSE-I-1249
- 思科技术支持和下载

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）。