安全訪問中WhatsApp的DLP策略限制

目錄

問題

Cisco Secure Access中的DLP策略在通過WhatsApp（瀏覽器或案頭應用程式）共用時不會檢測或阻止敏感檔案，儘管啟用了HTTPS解密。DLP引擎無法觸發或檢測通過這些平台的檔案上傳，而相同的DLP策略在通過其他線上上傳工具上傳時成功阻止相同的檔案。當測試WhatsApp的基本上傳阻止時，該功能在瀏覽器和案頭版本上均正常工作，但問題明確獨立於DLP策略實施。

環境

- Cisco Secure Access
- 已配置DLP策略
- 已啟用HTTPS解密
- WhatsApp Web和WhatsApp Desktop應用程式

解析

觀察到的行為是WhatsApp和類似平台由於實施端到端加密(E2EE)和非標準流量處理而預計會受到的限制。可以實施下一節和解決方法中概述的故障排除步驟。

故障排除驗證步驟

實施解決方法之前，請驗證以下配置專案：

- 確保配置了正確的SWG標識/源ID。
- 確認已啟用目標平台的HTTPS檢查/解密，且沒有選擇性地繞過。
- 驗證是否已正確配置隔離/RBI和Allow-Override設定。
- 如果DLP策略是基於組，請確認AD組成員身份。
- 檢查Traffic Steering bypass lists以瞭解所有例外情況。
- 驗證瀏覽器中是否禁用了QUIC協定。
- 檢查可繞過檢測的IPv6流量影響。

建議的解決方法

要為WhatsApp Web流量啟用DLP實施，請為發往WhatsApp Web的流量實施遠端瀏覽器隔離(RBI)。此解決方法允許通過隔離瀏覽器會話並在隔離環境中啟用內容檢查來實施DLP策略。

針對WhatsApp Web域專門配置RBI實施，以確保通過Web介面進行檔案上傳和內容共用時需進行DLP策略評估。

其他資訊

已針對此限制 — CSE-I-1249記錄了產品增強請求。

原因

WhatsApp（包括WhatsApp Web）和類似的合作平台實施端到端加密(E2EE)，防止對郵件文本和檔案上傳進行完整內容檢測和掃描。此外，WhatsApp流量不以與典型Web上傳相同的方式使用標準HTTP/HTTPS埠，這表示安全Web網關(SWG)無法攔截和檢查通過常規HTTPS檢查路徑的流量。此加密和流量處理方法設計為加密方法，代表這些特定平台當前DLP檢測功能的預期限制。

相關內容

- 產品增強請求CSE-I-1249
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。