

DLP Policy Limitations with WhatsApp in Secure Access

Contents

Issue

DLP policies in Cisco Secure Access are not detecting or blocking sensitive files when shared via WhatsApp (browser or desktop application), despite HTTPS decryption being enabled. The DLP engine fails to trigger or detect file uploads through these platforms, while the same DLP policies successfully block identical files when uploaded through other online upload tools. When testing basic upload blocking for WhatsApp, the functionality works correctly on both browser and desktop versions, but the issue is specifically isolated to DLP policy enforcement.

Environment

- Cisco Secure Access
- DLP Policies configured
- HTTPS decryption enabled
- WhatsApp Web and WhatsApp Desktop applications

Resolution

The observed behavior is an expected limitation of WhatsApp and similar platforms due to their end-to-end encryption (E2EE) implementation and non-standard traffic handling. The troubleshooting steps outlined in the next sections and workaround can be implemented.

Troubleshooting Verification Steps

Before implementing the workaround, verify these configuration items:

- Ensure correct SWG identity/origin ID is configured.
- Confirm HTTPS inspection/decryption is enabled and not selectively bypassed for the target platforms.
- Verify Isolation/RBI and Allow-Override settings are properly configured.
- Confirm AD group membership if DLP policies are group-based.
- Check Traffic Steering bypass lists for any exclusions.
- Verify QUIC protocol is disabled in browsers.
- Check for IPv6 traffic effects that could bypass inspection.

Recommended Workaround

To enable DLP enforcement for WhatsApp Web traffic, implement Remote Browser Isolation (RBI) for traffic destined to WhatsApp Web. This workaround allows DLP policies to be enforced by isolating the browser session and enabling content inspection within the isolated environment.

Configure RBI enforcement specifically for WhatsApp Web domains to ensure that file uploads and content sharing through the web interface are subject to DLP policy evaluation.

Additional Information

A product enhancement request has been documented for this limitation - CSE-I-1249.

Cause

WhatsApp (including WhatsApp Web) and similar collaboration platforms implement end-to-end encryption (E2EE) that prevents full content inspection and scanning of message text and file uploads. Additionally, WhatsApp traffic does not utilize standard HTTP/HTTPS ports in the same manner as typical web uploads, which means the Secure Web Gateway (SWG) cannot intercept and inspect the traffic through the normal HTTPS inspection path. This encryption and traffic handling method is by design and represents an expected limitation of the current DLP inspection capabilities for these specific platforms.

Related Content

- [Product Enhancement Request CSE-I-1249](#)
- [Cisco Technical Support & Downloads](#)