

Limitaciones de la política DLP con WhatsApp en Secure Access

Contenido

Problema

Las políticas de DLP de Cisco Secure Access no detectan ni bloquean los archivos confidenciales cuando se comparten a través de WhatsApp (navegador o aplicación de escritorio), a pesar de que el descifrado HTTPS está habilitado. El motor de DLP no puede activar o detectar las cargas de archivos a través de estas plataformas, mientras que las mismas políticas de DLP bloquean correctamente los archivos idénticos cuando se cargan a través de otras herramientas de carga online. Al probar el bloqueo básico de carga para WhatsApp, la funcionalidad funciona correctamente tanto en la versión del navegador como en la del escritorio, pero el problema se aísla específicamente en la aplicación de políticas de DLP.

Entorno

- Acceso seguro de Cisco
- Políticas DLP configuradas
- Descifrado HTTPS habilitado
- Aplicaciones web y de escritorio de WhatsApp

Resolución

El comportamiento observado es una limitación esperada de WhatsApp y plataformas similares debido a su implementación de cifrado de extremo a extremo (E2EE) y el manejo de tráfico no estándar. Se pueden implementar los pasos de solución de problemas descritos en las siguientes secciones y soluciones alternativas.

Pasos de verificación de Troubleshooting

Antes de implementar la solución alternativa, verifique estos elementos de configuración:

- Asegúrese de que se ha configurado la ID de origen/identidad de SWG correcta.
- Confirme que la inspección/descifrado HTTPS esté habilitado y que no se omita selectivamente para las plataformas de destino.
- Verifique que las configuraciones de Aislamiento/RBI y Permitir reemplazo estén configuradas correctamente.
- Confirme la pertenencia al grupo de AD si las políticas de DLP están basadas en grupos.
- Verifique las listas de desvío de Traffic Steering para ver si hay exclusiones.
- Verifique que el protocolo QUIC esté inhabilitado en los navegadores.
- Compruebe los efectos del tráfico IPv6 que podrían omitir la inspección.

Solución alternativa recomendada

Para habilitar la aplicación de DLP para el tráfico web de WhatsApp, implemente Remote Browser Isolation (RBI) para el tráfico destinado a WhatsApp Web. Esta solución alternativa permite que las políticas de DLP se apliquen aislando la sesión del navegador y habilitando la inspección de contenido dentro del entorno aislado.

Configure la aplicación de RBI específicamente para los dominios web de WhatsApp para garantizar que las cargas de archivos y el uso compartido de contenido a través de la interfaz web estén sujetos a la evaluación de políticas de DLP.

Additional Information

Se ha documentado una solicitud de mejora del producto para esta limitación: CSE-I-1249.

Causa

WhatsApp (incluido WhatsApp Web) y plataformas de colaboración similares implementan cifrado de extremo a extremo (E2EE) que impide la inspección de contenido completo y el análisis del texto del mensaje y las cargas de archivos. Además, el tráfico de WhatsApp no utiliza los puertos HTTP/HTTPS estándar de la misma manera que las cargas web habituales, lo que significa que Secure Web Gateway (SWG) no puede interceptar e inspeccionar el tráfico a través de la ruta de inspección HTTPS normal. Este método de cifrado y gestión del tráfico está diseñado y representa una limitación esperada de las capacidades de inspección de DLP actuales para estas plataformas específicas.

Contenido relacionado

- [Solicitud de mejora del producto CSE-I-1249](#)
- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).