

Resolución de problemas de bloqueo de datos de formularios DLP en tiempo real para todos los destinos

Contenido

[Introducción](#)

[Antecedentes](#)

[Troubleshoot](#)

[Conclusión](#)

Introducción

Este documento describe cómo resolver problemas relacionados con la configuración de una regla de protección de pérdida de datos (DLP) en tiempo real para bloquear todos los datos del formulario.

Antecedentes

Al configurar una regla de DLP en tiempo real para bloquear todos los datos del formulario, existe el riesgo de que tanto los verdaderos positivos como los falsos positivos tengan consecuencias no deseadas para las aplicaciones en la nube. Estas consecuencias pueden afectar al correcto funcionamiento de las aplicaciones en la nube, incluida la posibilidad de que los usuarios no puedan utilizar la página de inicio de sesión. El objetivo de este artículo es destacar estos riesgos y proporcionar pasos de resolución de problemas para abordar cualquier problema que pueda surgir.

Troubleshoot

En caso de que surjan problemas derivados del bloqueo de todos los datos del formulario en reglas de DLP en tiempo real, estos pasos pueden ayudar a solucionar el problema:

1. Refinar los identificadores de datos: este paso ayuda a encontrar el equilibrio entre el bloqueo eficaz de datos confidenciales y la autorización para que los datos de formularios legítimos circulen sin interrupciones.
 - Revise los detalles de los eventos de DLP bloqueados mediante el informe Data Loss Prevention (Reporting > Additional Reports > Data Loss Prevention) para identificar los identificadores de datos específicos que activan la regla de DLP.
 - Considere la posibilidad de perfeccionar los identificadores de datos ajustando los niveles de tolerancia o añadiendo términos de proximidad para reducir los falsos

positivos, al tiempo que se mantiene su capacidad de coincidencia según sea necesario.

2. Excluir URL bloqueadas: al excluir las URL, puede garantizar que las páginas de inicio de sesión y otros componentes esenciales de las aplicaciones no se ven afectados por la regla de bloqueo de DLP.

- Analice el registro de actividades mediante Búsqueda de actividades (Informes > Informes principales > Búsqueda de actividades) y los detalles de los eventos de DLP para identificar las URL que se están bloqueando.
- Agregue estas direcciones URL a una lista de destinos configurada en "Seleccionar listas de destinos y aplicaciones para su exclusión".

3. Modificar el comportamiento de las reglas DLP: si los problemas persisten y las consecuencias no deseadas superan las ventajas de bloquear todos los datos del formulario, debe modificar el comportamiento de DLP para detener el análisis de los datos del formulario. El cambio de comportamiento es posible con solo seleccionar "Cargas de archivos y datos de formularios de aplicaciones analizadas únicamente".

Conclusión

Al configurar una regla de DLP en tiempo real para bloquear todos los datos del formulario, es fundamental ser consciente de los riesgos asociados a las consecuencias no deseadas. Estos riesgos pueden afectar al buen funcionamiento de las aplicaciones en la nube, incluida la capacidad de utilizar la página de inicio de sesión. Utilice los pasos para la resolución de problemas que se describen en esta guía para mitigar estos riesgos y garantizar el correcto funcionamiento de las aplicaciones basadas en la nube al tiempo que mantiene la protección de datos.

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).