排除所有目标的实时DLP表单数据阻止故障

目录

简介

本文档介绍如何解决与配置实时数据丢失保护(DLP)规则以阻止所有表单数据相关的问题。

背景信息

当配置实时DLP规则以阻止所有表单数据时，存在同时产生正误和误报的风险，从而导致对云应用产生意想不到的后果。这些后果可能会影响云应用的成功运行，包括用户无法使用登录页的可能性。本文旨在强调这些风险并提供故障排除步骤以解决可能出现的问题。

故障排除

如果在实时DLP规则中阻止所有表单数据时出现任何问题，这些步骤可帮助排查和解决问题：

1. 改进数据标识符 — 此步骤有助于在有效阻止敏感数据和允许合法表单数据无中断地通过之间取得平衡。
    - 通过防数据丢失报告(Reporting > Additional Reports > Data Loss Prevention)查看阻止的DLP事件详细信息，以确定触发DLP规则的特定数据标识符。
    - 请考虑通过调整容差级别或添加邻近术语来精简数据标识符，以减少误报，同时仍保持其按需匹配的能力。
2. 排除阻止的URL(Exclude Blocked URLs) — 通过排除URL，您可以确保登录页面和应用程序的其他基本组件不受阻止DLP规则的影响。
    - 通过Activity Search(Reporting > Core Reports > Activity Search)和DLP事件详细信息分析活动日志，以确定被阻止的URL。
    - 将这些URL添加到在“选择排除的目标列表和应用”(Select Destination Lists and Applications for Exclusion)下配置的目标列表。
3. 修改DLP规则行为 — 如果问题仍然存在，且意外结果超过了阻止所有表单数据的好处，则需要修改DLP的行为以停止表单数据扫描。只需选择“仅上传文件并形成经过审核的应用程序的数据”即可更改行为。

结论

将实时DLP规则配置为阻止所有表单数据时，必须了解与意外后果相关的风险。这些风险可能会影响云应用的顺利运行，包括使用登录页面的能力。使用本指南中概述的故障排除步骤来降低这些风险，并确保您的云应用程序在维护数据保护的同时成功运行。

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）。