Troubleshoot Real-Time DLP Form Data Blocking for All Destinations

Contents

Introduction

This document describes how to troubleshoot issues related to configuring a real-time Data Loss Protection (DLP) rule to block all form data.

Background Information

When configuring a real-time DLP rule to block all form data, there is a risk of both true positives and false positives leading to unintended consequences for cloud applications. These consequences can impact the successful operation of cloud applications, including the possibility of users being unable to use the login page. This article aims to highlight these risks and provide troubleshooting steps to address any issues that can arise.

Troubleshoot

In the event of any issues arising from blocking all form data in real-time DLP rules, these steps can help troubleshoot and resolve the problem:

1. Refine Data Identifiers - This step helps strike a balance between effectively blocking sensitive data and allowing legitimate form data to pass through without disruption.

    - Review the blocked DLP events details via the *Data Loss Prevention* report (**Reporting** > **Additional Reports** > **Data Loss Prevention**) to identify the specific data identifiers triggering the DLP rule.

    - Consider refining the data identifiers by adjusting the tolerance levels or adding proximity terms to reduce false positives while still maintaining their ability to match as needed.

2. Exclude Blocked URLs - By excluding URLs, you can ensure that login pages and other essential components of your applications are not affected by the blocking DLP rule.

    - Analyze the activity log via *Activity Search* (**Reporting** > **Core Reports** > **Activity Search**) and the DLP event details to identify the URLs that are getting blocked.

    - Add these URLs to a destination list configured under "Select Destination Lists and Applications for Exclusion".

3. Modify DLP Rule Behavior - If the issues persist and the unintended consequences outweigh the

benefits of blocking all form data, you need to modify the behavior of the DLP to stop form data scanning. Changing behavior is possible by simply selecting "File uploads and form data of vetted applications only".

Conclusion

When configuring a Real Time DLP rule to block all form data, it is crucial to be aware of the risks associated with unintended consequences. These risks can impact the smooth operation of cloud applications, including the ability to use the login page. Use the troubleshooting steps outlined in this guide to mitigate these risks and ensure the successful functioning of your cloud applications while maintaining data protection.