

Problemen oplossen met real-time DLP-formuliergegevensblokkering voor alle bestemmingen

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Problemen oplossen](#)

[Conclusie](#)

Inleiding

In dit document wordt beschreven hoe u problemen kunt oplossen met betrekking tot het configureren van een DLP-regel (Real-time Data Loss Protection) om alle formuliergegevens te blokkeren.

Achtergrondinformatie

Bij het configureren van een real-time DLP-regel om alle formuliergegevens te blokkeren, bestaat het risico dat zowel echte positieve als valse positieve resultaten leiden tot onbedoelde gevolgen voor cloudtoepassingen. Deze gevolgen kunnen van invloed zijn op de succesvolle werking van cloudapplicaties, waaronder de mogelijkheid dat gebruikers de inlogpagina niet kunnen gebruiken. Dit artikel is bedoeld om deze risico's onder de aandacht te brengen en stappen te bieden voor het oplossen van problemen die zich kunnen voordoen.

Problemen oplossen

In het geval van problemen die voortvloeien uit het blokkeren van alle formuliergegevens in real-time DLP-regels, kunnen deze stappen helpen bij het oplossen van het probleem:

1. Gegevens-ID's verfijnen - Deze stap helpt een evenwicht te vinden tussen het effectief blokkeren van gevoelige gegevens en het toestaan van legitieme formuliergegevens om zonder onderbreking door te geven.
 - Bekijk de details van de geblokkeerde DLP-gebeurtenissen via het rapport Gegevensverliespreventie (Rapportage > Aanvullende rapporten > Gegevensverliespreventie) om de specifieke gegevensidentificatoren te identificeren die de DLP-regel activeren.
 - Overweeg om de data-identifiers te verfijnen door de tolerantieniveaus aan te passen of nabijheidstermen toe te voegen om false positives te verminderen, terwijl ze toch in

staat blijven om te matchen als dat nodig is.

2. Geblokkeerde URL's uitsluiten - Door URL's uit te sluiten, kunt u ervoor zorgen dat aanmeldingspagina's en andere essentiële onderdelen van uw toepassingen niet worden beïnvloed door de DLP-blokkeringsregel.
 - Analyseer het activiteitenlog via Activity Search (Reporting > Core Reports > Activity Search) en de details van de DLP-gebeurtenis om de URL's te identificeren die worden geblokkeerd.
 - Voeg deze URL's toe aan een bestemmingslijst die is geconfigureerd onder "Selecteer bestemmingslijsten en toepassingen voor uitsluiting".
3. DLP-regelgedrag wijzigen - Als de problemen blijven bestaan en de onbedoelde gevolgen zwaarder wegen dan de voordelen van het blokkeren van alle formuliergegevens, moet u het gedrag van de DLP wijzigen om het scannen van formuliergegevens te stoppen. Het wijzigen van gedrag is mogelijk door simpelweg "Bestand uploads en formuliergegevens van doorgelichte toepassingen alleen" te selecteren.

Conclusie

Bij het configureren van een Real Time DLP-regel om alle formuliergegevens te blokkeren, is het van cruciaal belang om zich bewust te zijn van de risico's die gepaard gaan met onbedoelde gevolgen. Deze risico's kunnen van invloed zijn op de goede werking van cloudapplicaties, waaronder de mogelijkheid om de inlogpagina te gebruiken. Gebruik de stappen voor probleemoplossing die in deze handleiding worden beschreven om deze risico's te beperken en de succesvolle werking van uw cloudtoepassingen te garanderen met behoud van gegevensbescherming.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.