Cómo configurar una política de DLP para correo electrónico en Cisco Secure Access (SA) y Cisco Email Threat Defence (ETD)

Contenido

Introducción

El correo electrónico sigue siendo uno de los canales más habituales para la exposición involuntaria o no autorizada de datos. Para ayudar a las organizaciones a proteger la información confidencial compartida a través del correo electrónico, Cisco proporciona funciones de prevención de la pérdida de datos de correo electrónico (DLP) mediante la integración de Cisco Secure Access (SA) y Cisco Email Threat Defence (ETD).

En esta arquitectura, todas las acciones de creación, configuración y aplicación de políticas de DLP para correo electrónico se realizan en Cisco Secure Access. Cisco Email Threat Defence proporciona visibilidad del correo electrónico y seguimiento de mensajes, mientras que Cisco Secure Access actúa como el motor de políticas para definir las reglas de DLP y el comportamiento de aplicación.

En este artículo se explica cómo crear una política de DLP para correo electrónico en Cisco Secure Access mediante una plantilla de DLP predefinida o una plantilla de DLP personalizada.

Prerequisites

Antes de comenzar el proceso de configuración, asegúrese de que se cumplen los siguientes requisitos:

- Acceso administrativo:debe tener privilegios de "administrador completo" tanto para la consola en línea de Cisco Email Threat Defence como para la consola de Cisco Secure Access.
- Suscripciones activas: asegúrese de que tanto los arrendatarios de Email Threat Defence como de Secure Access están activos y aprovisionados.
- Conectividad:la integración de API entre Email Threat Defence y Secure Access debe establecerse correctamente.
- Configuración de flujo de correo: Email Threat Defence debe implementarse correctamente en el modo en línea para garantizar que está inspeccionando activamente el tráfico de correo electrónico.

Importante: Aunque esta solución utiliza tanto Cisco Secure Access como Cisco Email Threat Defence, todos los pasos de configuración de reglas de DLP para correo electrónico descritos en este artículo se realizan únicamente en Cisco Secure Access.

Requisitos y componentes utilizados

Para implementar correctamente una política de DLP de correo electrónico, se utilizan los siguientes componentes:

- Cisco Email Threat Defence (ETD):actúa como punto de inspección de correo electrónico. Captura el tráfico de correo electrónico saliente y facilita el flujo de comunicación necesario para que el motor de DLP realice su análisis.
- Cisco Secure Access (SA): el motor DLP:es el componente principal en el que residen todas las configuraciones DLP. Utilizará la consola de Secure Access para definir:
    - Identificadores de datos: patrones específicos o tipos de datos confidenciales (por ejemplo, PII, números de tarjetas de crédito o códigos de proyecto internos) que el sistema debe supervisar.
    - Políticas DLP:reglas que establecen cómo debe reaccionar el sistema cuando se detectan datos confidenciales (por ejemplo, bloquear, cifrar o notificar).
    - Acciones de política:respuestas automatizadas activadas por el motor de DLP, como evitar que se envíe el correo electrónico o aplicar el cifrado obligatorio.
- Integration Framework:La conectividad backend que permite a ETD entregar metadatos de correo electrónico al motor DLP de Secure Access para la evaluación de políticas y su posterior aplicación.

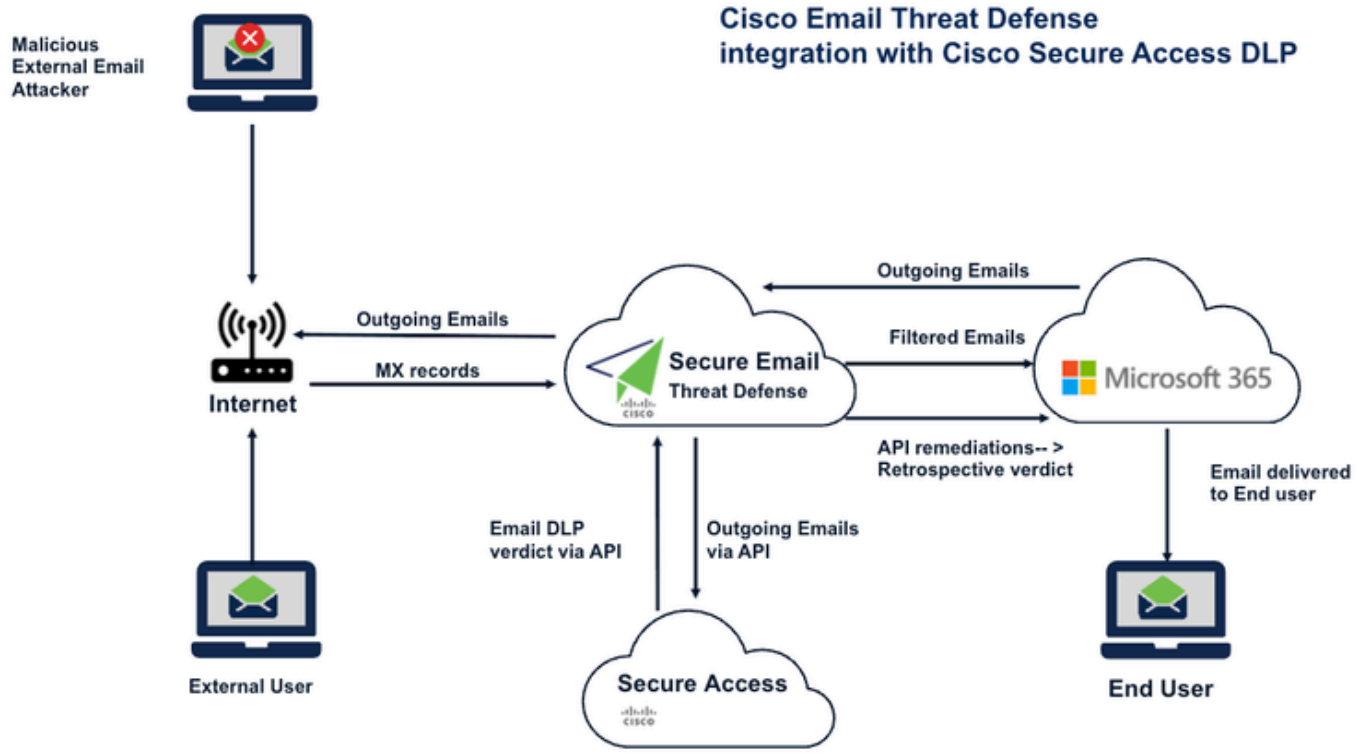
Funciones de políticas de DLP por correo electrónico

Al crear una política de DLP para correo electrónico en Cisco Secure Access, puede configurar:

- Nombre y descripción de la regla
- Nivel de gravedad
- Clasificaciones de datos
- Alcance de la inspección, incluido:
    - Asunto del correo electrónico
    - Cuerpo del mensaje
    - Nombre de archivo adjunto
    - Contenido del adjunto
- Controles de archivo, incluidos:
    - Etiquetas MIP
    - Etiquetas Titus
- Condiciones de remitente
- Condiciones de destinatario
- Acciones de política:
    - Monitor
    - Bloqueo
- Notificaciones de usuario opcionales

Diagrama de la red

A continuación encontrará el diagrama de red que ilustra la integración de la defensa frente a amenazas de Cisco Secure Email con Cisco Secure Access junto con el diagrama de flujo de tráfico.



NOTE: En la imagen anterior, el servidor de Exchange es O365, pero esta configuración de DLP se puede realizar en cualquier servidor de Exchange que admita SMTP.

NOTE: Consulte el artículo "Pasos para integrar Cisco Email Threat Defence (ETD) con Cisco Secure Access:" para integrar Cisco Email Threat Defence y Cisco Secure Access mediante API.

Configurar

Configuración de una política de DLP de correo electrónico en Cisco Secure Access

Paso 1: Inicie sesión en Cisco Secure Access

Inicie sesión en la consola de Cisco Secure Access (SA) con una cuenta de administrador con los

permisos necesarios.

Paso 2: Navegar hasta Creación de reglas de DLP por correo electrónico

En el panel de acceso seguro, vaya a:

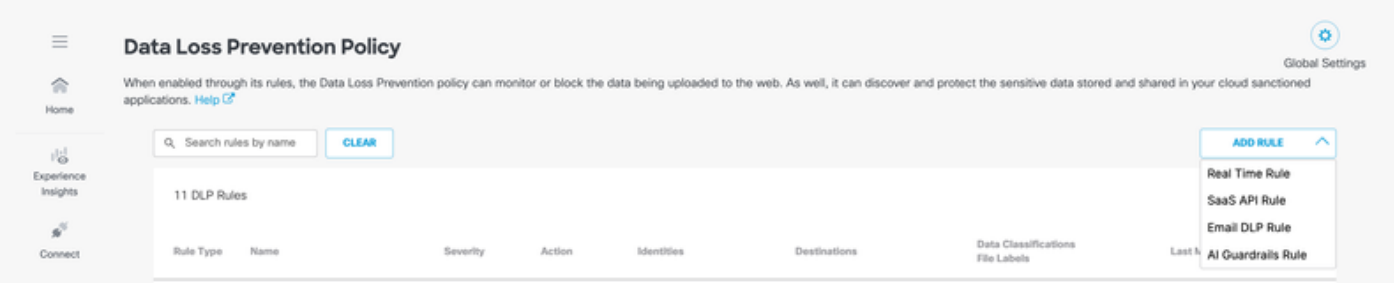
Segura > Política > Política de prevención de pérdida de datos > Agregar regla > Enviar regla DLP por correo electrónico

Se abrirá la página Agregar nueva regla de correo electrónico.

Cisco Secure Access proporciona dos métodos para crear una regla de DLP para correo electrónico:

- Creación de una regla de DLP por correo electrónico mediante una plantilla de DLP predefinida
- Creación de una regla de DLP por correo electrónico mediante una plantilla de DLP personalizada

Figura 1. Acceda a Creación de reglas de DLP por correo electrónico



Opción 1: Creación de una regla DLP de correo electrónico mediante una plantilla DLP predefinida

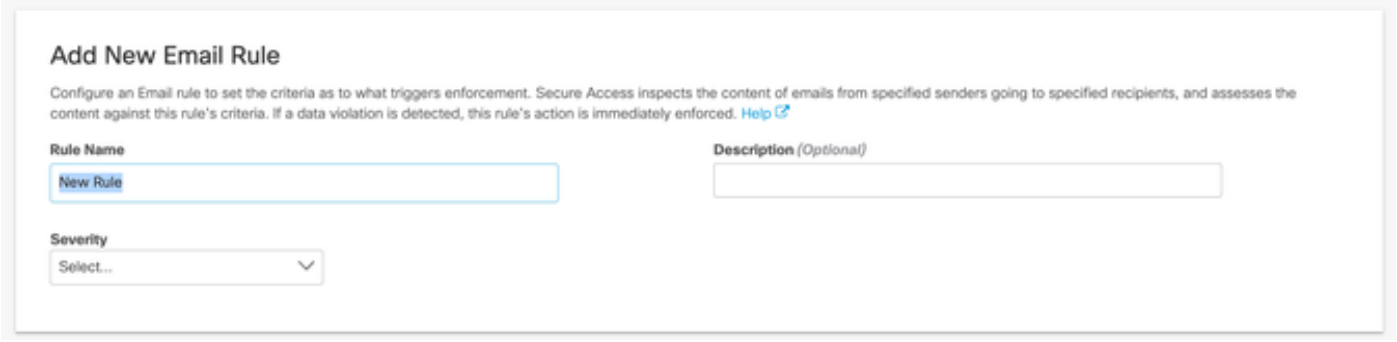
Paso 3: Configurar información básica de reglas

Acceda a la ventana ADD RULE > Email DLP Rule.

En la ventana Add New Email Rule, ingrese los siguientes detalles:

- Nombre de regla
  Introduzca un nombre descriptivo para la regla de DLP de correo electrónico.
- Descripción
  Proporcione un breve resumen del propósito de la regla.
- Gravedad
  Seleccione el nivel de gravedad adecuado para la política:
  - Bajo
  - Medio
  - Alto
  - Crítico

Estos campos ayudan a clasificar la regla de administración, generación de informes y visibilidad operativa.



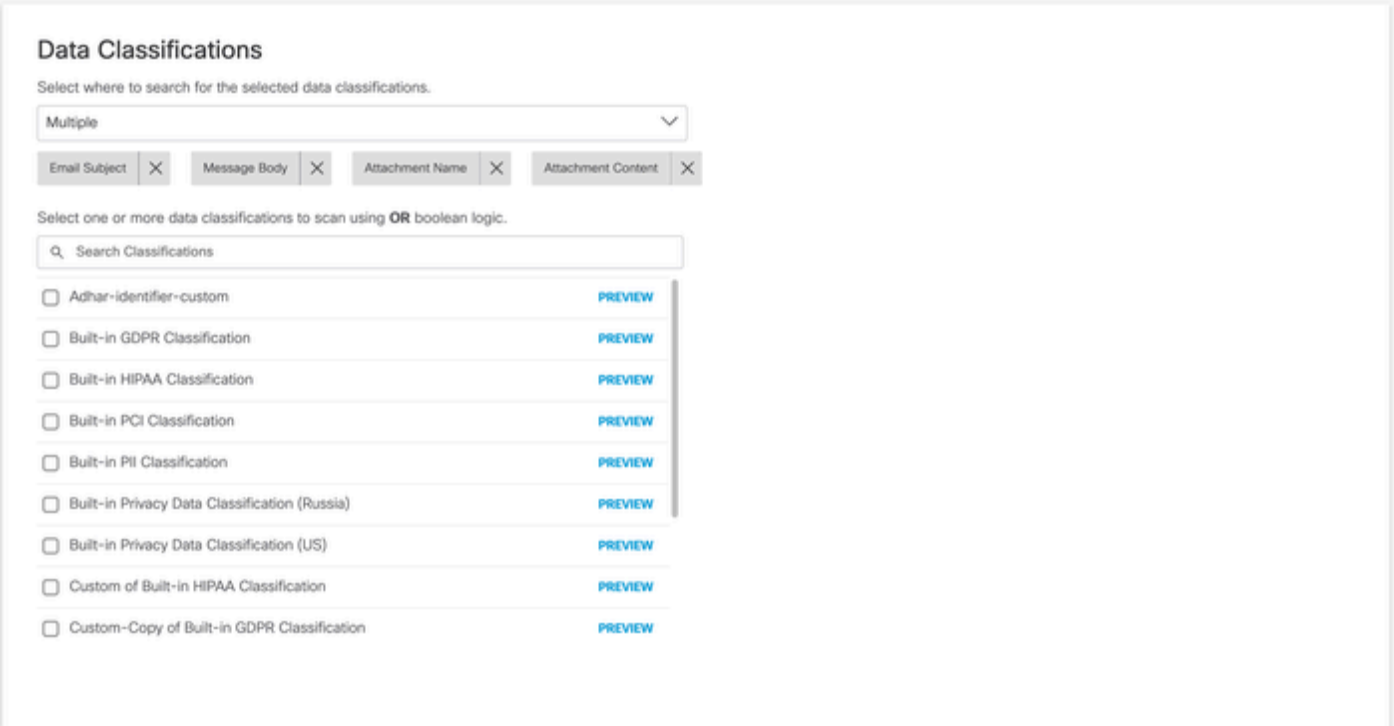
Paso 4: Seleccionar clasificaciones de datos

En Clasificaciones de datos, seleccione la plantilla de DLP predefinida que se utilizará para examinar el contenido del correo electrónico en busca de posibles infracciones de DLP.

A continuación, elija dónde deben coincidir las clasificaciones seleccionadas. Las ubicaciones de inspección compatibles incluyen:

- Asunto del correo electrónico
- Cuerpo del mensaje
- Nombre de archivo adjunto
- Contenido del adjunto

Esto permite a la directiva inspeccionar el contenido de los mensajes y los archivos adjuntos en busca de información confidencial.



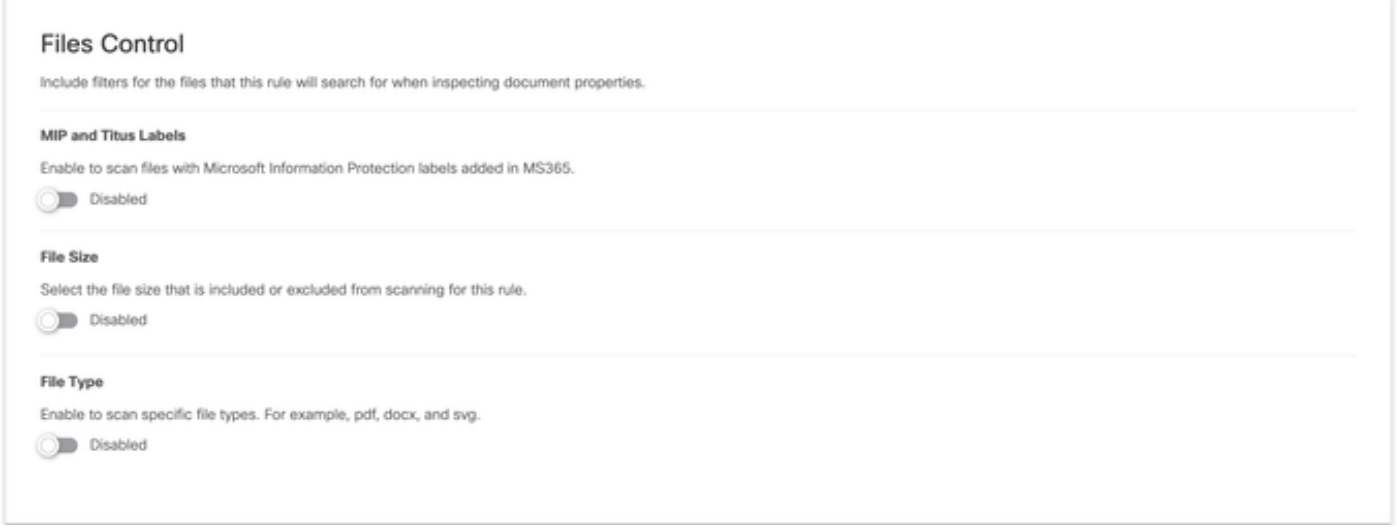
Paso 5: Configurar controles de archivos

En Control de archivos, configure los criterios de inspección basados en archivos para la regla.

Esto incluye soporte para:

- Etiquetas MIP
- Etiquetas Titus

Esta configuración resulta útil cuando la aplicación de DLP debe tener en cuenta las etiquetas de sensibilidad o los metadatos asociados a los archivos adjuntos.



Paso 6: Definir ámbito de remitente

En la sección Remitentes, especifique a qué remitentes se aplica la política.

Entre las opciones disponibles se incluyen:

- Todos los remitentes
- Remitentes específicos
- Excluir remitentes específicos

Esto permite aplicar la regla de forma amplia o restringirla a los usuarios o grupos seleccionados.

Paso 7: Definir ámbito de destinatario

En la sección Destinatarios, elija los usuarios o grupos que deben incluirse o excluirse de la evaluación de políticas.

Entre las opciones disponibles se incluyen:

- Incluir todos los usuarios
- Incluir usuarios específicos
- Excluir usuarios específicos

Esto ayuda a adaptar la aplicación de políticas en función de los destinatarios deseados.

Paso 8: Seleccione la acción de directiva

En la sección Acción, elija cómo Cisco Secure Access debe manejar los correos electrónicos que se identifican positivamente como que violan la regla DLP.

Las acciones disponibles son:

- Monitor
  Se permite el correo electrónico y se registra el evento para obtener visibilidad e informes.
- Bloqueo
  El correo electrónico se descarta para evitar la transmisión de datos confidenciales.

Nota: En la actualidad, los correos electrónicos identificados positivamente se pueden permitir a través de la acción Monitor o se pueden descartar a través de la acción Block.

Importante: Las acciones de DLP por correo electrónico solo se configuran en Cisco Secure Access. Si un correo electrónico está bloqueado por Secure Access, el evento también está visible en el seguimiento de mensajes de Cisco ETD.

Paso 9: Configurar notificaciones de usuario

La opción de notificación solo está disponible para los destinatarios.

En Notificaciones de usuario, configure si se debe notificar a los usuarios cuando un correo electrónico coincide con la política DLP.
Existe la opción de notificar al "Administrador del actor" o a un "Destinatario personalizado". Un "destinatario personalizado" puede ser cualquier persona.

Configure la plantilla de mensaje de correo electrónico de Notificación predeterminada a Notificación personalizada según sus necesidades.

Si están habilitadas, las notificaciones pueden ayudar a mejorar el conocimiento del usuario y reducir las violaciones de políticas repetidas. Configure este parámetro de acuerdo con los requisitos operativos y de cumplimiento de su organización.

Paso 9: Configurar notificaciones de usuario

Las notificaciones de usuario son una herramienta eficaz para promover el reconocimiento de la seguridad y garantizar el cumplimiento. Al avisar a los usuarios o administradores cuando un correo electrónico activa una política DLP, puede proporcionar información inmediata y contexto sobre la infracción.

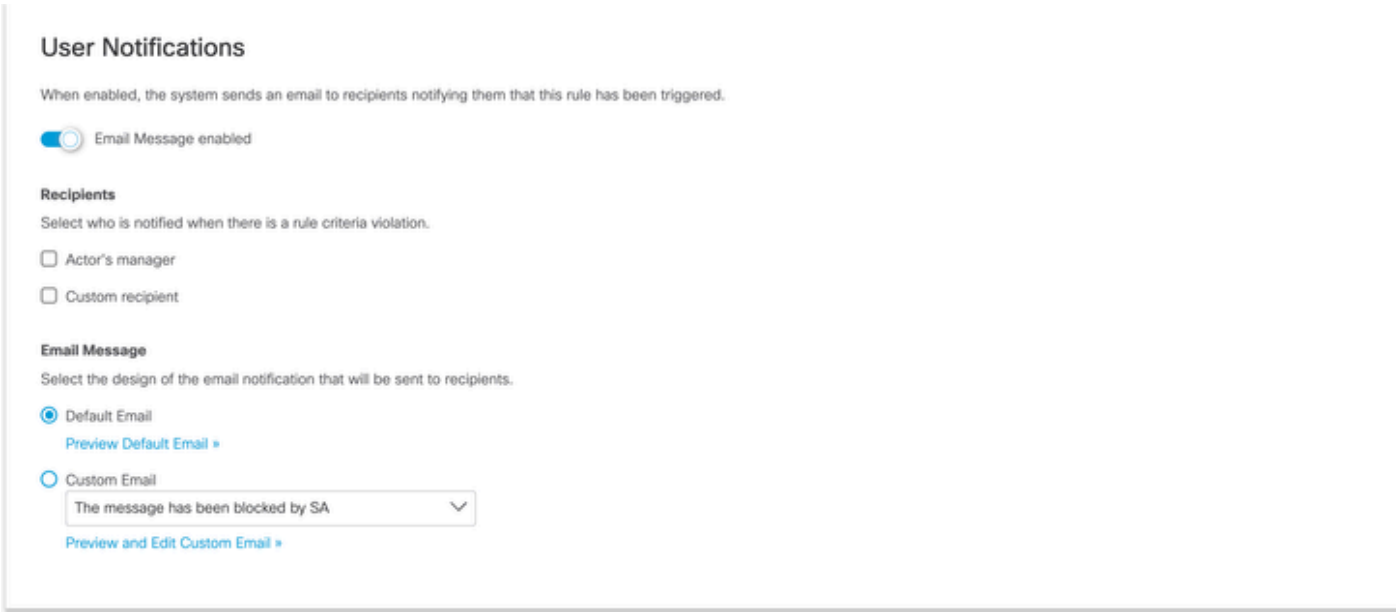
Nota: La configuración de notificación está pensada principalmente para los destinatarios de correo electrónico y las partes interesadas designadas.

Para configurar notificaciones:

1. Definir destinatarios de notificación: En la sección Notificaciones de usuario, especifique quién debe recibir la alerta. Tiene dos opciones principales:
    - Gerente del actor: Envía la notificación directamente al administrador del usuario que desencadenó la infracción de directiva.
    - Destinatario personalizado: Permite especificar cualquier dirección de correo electrónico (por ejemplo, un centro de operaciones de seguridad o un jefe de departamento específico).

2. Seleccionar plantilla de mensaje: Puede elegir entre la plantilla de notificación Predeterminada o una notificación Personalizada.
    - Recomendación: Si su organización tiene requisitos de marca interna o mensajes de conformidad específicos, utilice la opción Personalizado para adaptar el cuerpo del correo electrónico y proporcionar instrucciones claras y prácticas al destinatario.
3. Revisar y guardar: Una vez configurados, asegúrese de que los parámetros se corresponden con las políticas operativas y de cumplimiento de su organización.

Práctica recomendada: Habilitar estas notificaciones es una forma eficaz de reducir las infracciones de políticas repetidas mediante la formación de los usuarios en tiempo real acerca de los procedimientos de gestión de datos confidenciales.



Nota: Las opciones de notificación pueden variar en función de la configuración del arrendatario y la configuración de la política.

Paso 10: Revisar y guardar la regla

Después de completar la configuración de la regla:

1. Revise todos los parámetros configurados.
2. Verifique que las clasificaciones de datos, el alcance de inspección, las condiciones de remitente y destinatario y la acción seleccionados coincidan con el comportamiento de política deseado.
3. Haga clic en Guardar para crear la regla DLP de correo electrónico.

La política de DLP de correo electrónico está ahora activa en Cisco Secure Access.

Opción 2: Creación de una regla DLP de correo electrónico mediante una plantilla DLP personalizada

La creación de una plantilla de DLP personalizada implica dos fases principales: definición de un identificador personalizado y configuración de la clasificación de datos.

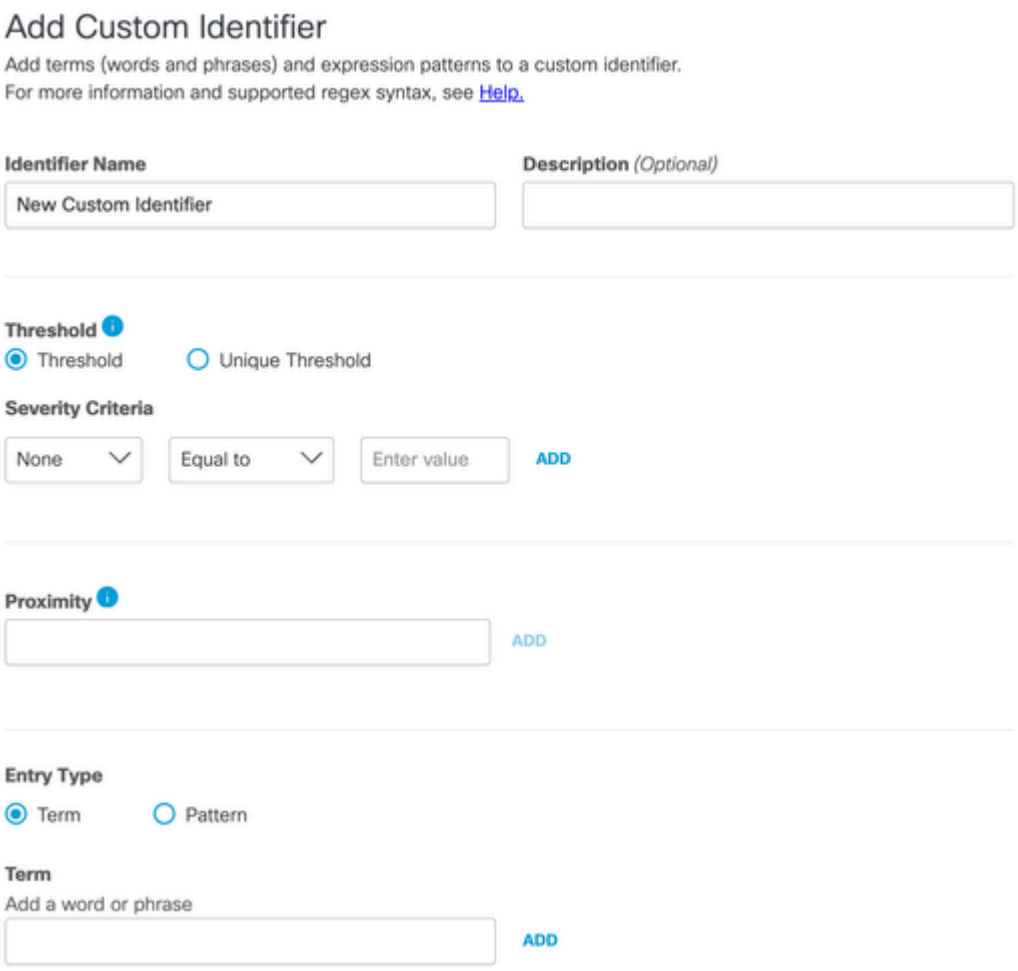
Nota: El motor de clasificación de datos es muy flexible, lo que permite crear directivas mediante un único identificador personalizado o una combinación de identificadores personalizados e predefinidos vinculados por operadores booleanos AND/OR.

Paso 11: Crear un identificador personalizado

Para definir un nuevo patrón de datos para la detección, siga estos pasos:

1. Inicie sesión en elpanel de acceso seguro.
2. Vaya aSeguro > Clasificación de datos.
3. Haga clic en Agregar identificador personalizado.
4. Configure los siguientes parámetros en la ventanaAgregar identificador personalizado:

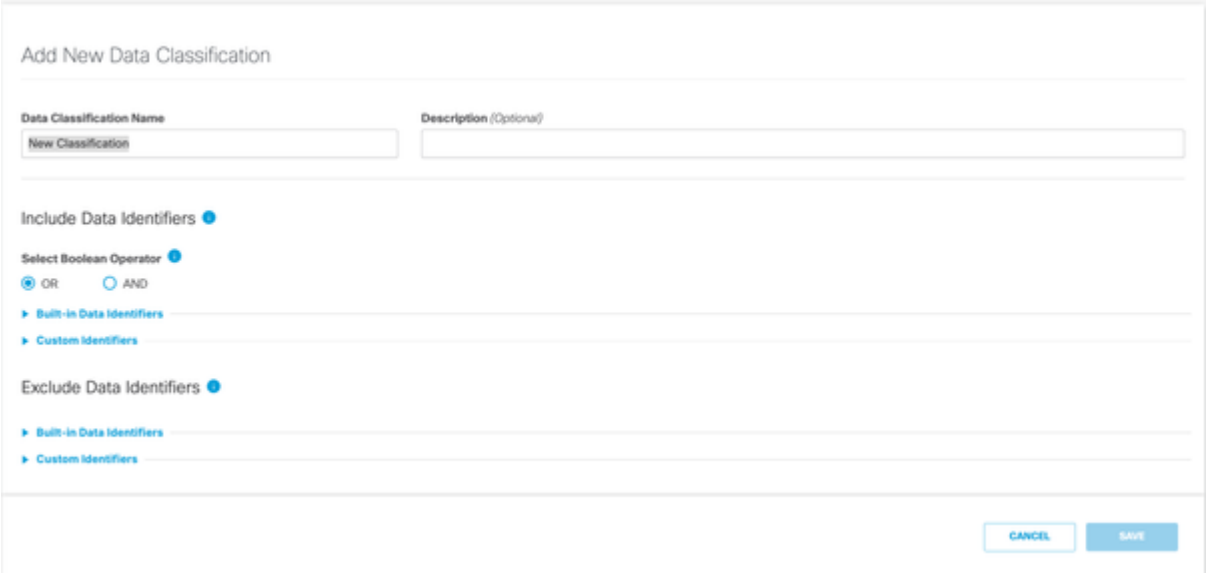
- Nombre y descripción: Proporcione un nombre único y una breve descripción del tipo de datos que desea detectar.
- Umbral:
    - Umbral: Supervisa la frecuencia total de los datos detectados.
    - Umbral único: Supervisa sólo el número deapariciones únicas de los datos, omitiendo los duplicados.
- Criterios de gravedad: Asigne niveles de gravedad (Muy bajo, Bajo, Medio, Alto) en función de la frecuencia de detección. Puede definirlos mediante operadores de comparación como EqualTo, Greater Than, Less Than o Range.
- Proximidad: Establezca el umbral de proximidad. Esto se aplica a todos los términos y patrones definidos dentro de este identificador de forma conjunta, en lugar de por término individual.
- Tipo de entrada: Defina cómo identifica el sistema los datos:
    - Término: Una palabra o frase específica.
    - Patrón: Expresión regular (regex) utilizada para detectar formatos de datos específicos (por ejemplo, números de tarjetas de crédito o códigos de proyecto internos).



Paso 12: Configurar clasificación de datos

Una vez guardado el identificador personalizado, puede integrarlo en un objeto de clasificación de datos:

1. Vaya aSeguro > Clasificación de datos > Agregar (utilice el botón de la esquina superior derecha)
2. Seleccione el identificador personalizado recién creado en la lista disponible.
3. (Opcional) Combine el identificador personalizado con identificadores predefinidos mediante la lógica AND/ORpara refinar el ámbito de detección.
4. Guarde la configuración para que esté disponible para su uso en las políticas de DLP de correo electrónico.
5. Consulte la captura de pantalla siguiente para obtener más información.
6. Ahora siga los mismos pasos del Paso 4 al Paso 10 para crear una política utilizando la clasificación de datos personalizada.



Esta configuración garantiza que su organización pueda detectar información confidencial adaptada específicamente a sus estructuras de datos internos y a los requisitos de conformidad.

Troubleshoot

Si la regla de DLP de correo electrónico no se comporta como se esperaba, revise lo siguiente:

La regla no coincide con los correos electrónicos

- Confirme que la plantilla de clasificación de datos correctoestá seleccionada.
- Verifique que las ubicaciones de inspección relevantes estén habilitadas:
  - Asunto del correo electrónico
  - Cuerpo del mensaje
  - Nombre de archivo adjunto
  - Contenido del adjunto
- Asegúrese de que los filtros de remitente y destinatario no excluyen involuntariamente el correo electrónico de prueba.

Los correos electrónicos no están bloqueados

- Compruebe que la acción de la regla está establecida en Bloquear y noSupervisar.
- Confirme que la regla está guardada y habilitada.
- Asegúrese de que el contenido del correo electrónico coincide positivamente con los criterios de DLP configurados.

Los eventos DLP no son visibles en ETD

- Confirme que Cisco ETD y Cisco Secure Access están integrados correctamente.
- Verifique que ETD esté procesando activamente el tráfico de correo electrónico relevante.
- Compruebe si el evento de política está presente primero en Cisco Secure Access.

No se detectan coincidencias basadas en datos adjuntos

- Confirme queNombre y/oContenido del adjunto están seleccionados en el ámbito de inspección.
- Compruebe la configuración del control de archivo si las etiquetas como MIPorTitle forman parte de la lógica de la regla.

Mejores medidas

Tenga en cuenta las siguientes prácticas recomendadas a la hora de implementar políticas de DLP por correo electrónico:

- Comience conModoSupervisión para validar el comportamiento de la política antes de aplicarBloque.
- Utilice nombres de reglas claros y descriptivos para facilitar la administración.
- Aplique cuidadosamente las condiciones de remitente y destinatario para reducir las coincidencias no deseadas.
- Pruebe con datos representativos antes de realizar una implementación amplia.
- Revise el seguimiento de mensajes ETD con regularidad para validar la actividad de correo electrónico bloqueado o supervisado.
- Utilice plantillas personalizadas en las que se requieran identificadores de datos específicos de la empresa.

Summary

Cisco Secure Access es la plataforma central para configurar las políticas de DLP para correo electrónico en una implementación integrada de Cisco Secure Access y Cisco Email Threat Defence. Mientras que ETD proporciona visibilidad y seguimiento de mensajes, toda la creación de reglas DLP, selección de clasificación, acción de aplicación y notificaciones se configuran en Secure Access.

Mediante el uso de plantillas de DLP predefinidas o personalizadas, los administradores pueden inspeccionar el contenido y los archivos adjuntos de los correos electrónicos, definir el alcance del remitente y del destinatario, y aplicar las acciones Supervisar o Bloquear para ayudar a evitar la pérdida de datos confidenciales a través del correo electrónico.

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).