Een DLP-beleid voor e-mail configureren in Cisco Secure Access (SA) en Cisco Email Threat Defense (ETD)

Inhoud

Inleiding

E-mail blijft een van de meest voorkomende kanalen voor onbedoelde of ongeoorloofde blootstelling van gegevens. Om organisaties te helpen gevoelige informatie te beschermen die via e-mail wordt gedeeld, biedt Cisco mogelijkheden voor het voorkomen van verlies van e-mailgegevens (DLP) via de integratie van Cisco Secure Access (SA) en Cisco Email Threat Defense (ETD).

In deze architectuur worden alle acties voor het maken, configureren en handhaven van DLP-beleid voor e-mail uitgevoerd in Cisco Secure Access. Cisco Email Threat Defense biedt zichtbaarheid van e-mail en het bijhouden van berichten, terwijl Cisco Secure Access fungeert als de beleidsengine voor het definiëren van DLP-regels en handhavingsgedrag.

In dit artikel wordt uitgelegd hoe u een DLP-beleid voor e-mail maakt in Cisco Secure Access, met behulp van een vooraf gedefinieerde DLP-sjabloon of een aangepaste DLP-sjabloon.

Voorwaarden

Voordat u begint met het configuratieproces, moet u ervoor zorgen dat aan de volgende vereisten wordt voldaan:

- Beheerderstoegang: u moet "Volledige beheerdersrechten" hebben voor zowel de Cisco Email Threat Defense Inline-console als de Cisco Secure Access-console.
- Actieve abonnementen: Zorg ervoor dat zowel uw e-mailbedreigingsverdediging als beveiligde toegangshenants actief zijn en worden geleverd.
- Connectiviteit: de API-integratie tussen Email Threat Defense en Secure Access moet met succes tot stand zijn gebracht.
- E-mailstroomconfiguratie: E-mailbedreigingsbeveiliging moet correct worden geïmplementeerd in de inline-modus om ervoor te zorgen dat het e-mailverkeer actief wordt geïnspecteerd.

Belangrijk: hoewel deze oplossing zowel Cisco Secure Access als Cisco Email Threat Defense gebruikt, worden alle configuratiestappen voor de DLP-regel voor e-mail die in dit artikel worden beschreven, alleen uitgevoerd in Cisco Secure Access.

Gebruikte vereisten en componenten

Voor het succesvol implementeren van een e-mail DLP-beleid worden de volgende componenten gebruikt:

- Cisco Email Threat Defense (ETD): fungeert als het e-mailinspectiepunt. Het registreert het uitgaande e-mailverkeer en vergemakkelijkt de communicatiestroom die nodig is voor de DLP-engine om zijn analyse uit te voeren.
- Cisco Secure Access (SA) - De DLP Engine: dit is het primaire onderdeel waar alle DLP-configuraties zich bevinden. U gebruikt de Secure Access-console om het volgende te definiëren:
    - Data Identifiers: De specifieke patronen of gevoelige gegevenstypen (bijv. PII, creditcardnummers of interne projectcodes) die het systeem moet controleren.
    - DLP-beleid: de regels die bepalen hoe het systeem moet reageren wanneer gevoelige gegevens worden gedetecteerd (bijvoorbeeld blokkeren, versleutelen of melden).
    - Beleidsacties: de geautomatiseerde reacties die worden geactiveerd door de DLP-engine, zoals voorkomen dat de e-mail wordt verzonden of verplichte codering toepassen.
- Integratiekader: de back-endconnectiviteit waarmee ETD e-mailmetagegevens kan afgeven aan de DLP-engine voor beveiligde toegang voor beleidsevaluatie en daaropvolgende handhaving.

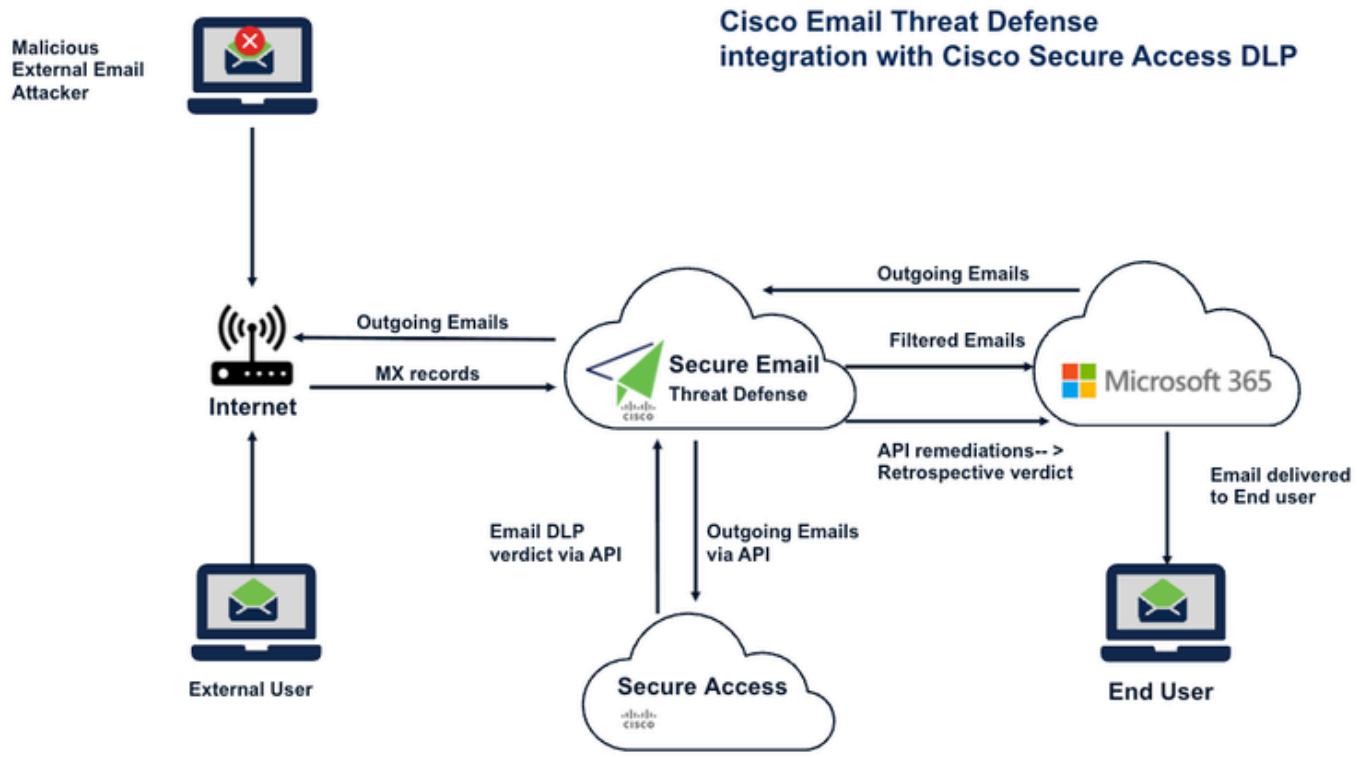
Mogelijkheden voor e-mailDLP-beleid

Wanneer u een DLP-beleid voor e-mail maakt in Cisco Secure Access, kunt u het volgende configureren:

- Naam en beschrijving van regel
- Prioriteitsniveau
- Gegevensclassificaties
- De reikwijdte van de inspectie, waaronder:
    - Onderwerp e-mail
    - berichttekst
    - Naam bijlage
    - Bijlage-inhoud
- Bestandsbesturingselementen, waaronder:
    - PMO-etiketten
    - Titus-etiketten
- Zendervoorwaarden
- Voorwaarden van ontvanger
- Beleidsmaatregelen:
    - Monitor (bewaken)
    - Block (blokkeren)
- Optionele meldingen van gebruikers

Netwerkdiagram

Hieronder vindt u het netwerkdiagram dat de integratie van Cisco Secure Email Threat Defense met Cisco Secure Access illustreert, samen met het verkeersstroomdiagram.



OPMERKING: In de bovenstaande afbeelding is de Exchange-server O365, maar deze DLP-configuratie kan worden uitgevoerd op elke Exchange-server die SMTP ondersteunt.

OPMERKING: Raadpleeg het artikel "Stappen om Cisco Email Threat Defense (ETD) te integreren met Cisco Secure Access:" om Cisco Email Threat Defense en Cisco Secure Access te integreren via API.

Configureren

Een DLP-beleid voor e-mail configureren in Cisco Secure Access

Stap 1: Meld u aan bij Cisco Secure Access

Meld u aan bij de Cisco Secure Access (SA)-console met een beheerdersaccount met de vereiste machtigingen.

Stap 2: Navigeer naar het maken van DLP-regels voor e-mail

Navigeer vanuit het dashboard voor beveiligde toegang naar:

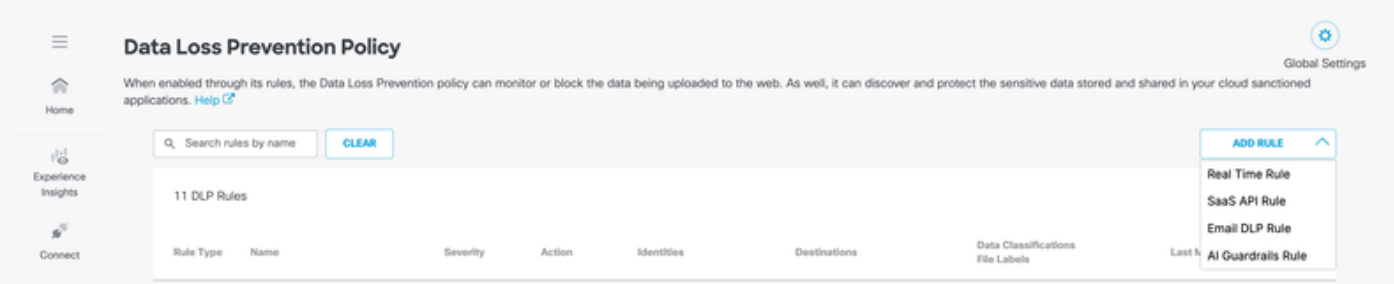
Veilig > Beleid > Beleid ter voorkoming van gegevensverlies > Regel toevoegen > Regel voor e-mail DLP

Hiermee wordt de pagina Nieuwe e-mailregel toevoegen geopend.

Cisco Secure Access biedt twee methoden om een DLP-regel voor e-mail te maken:

- Een e-mail-DLP-regel maken met een vooraf gedefinieerde DLP-sjabloon
- Een DLP-regel voor e-mail maken met een aangepaste DLP-sjabloon

Afbeelding 1. Navigeer naar Aanmaken van DLP-regel voor e-mail



Optie 1: Maak een e-mail DLP regel met behulp van een vooraf gedefinieerde DLP template

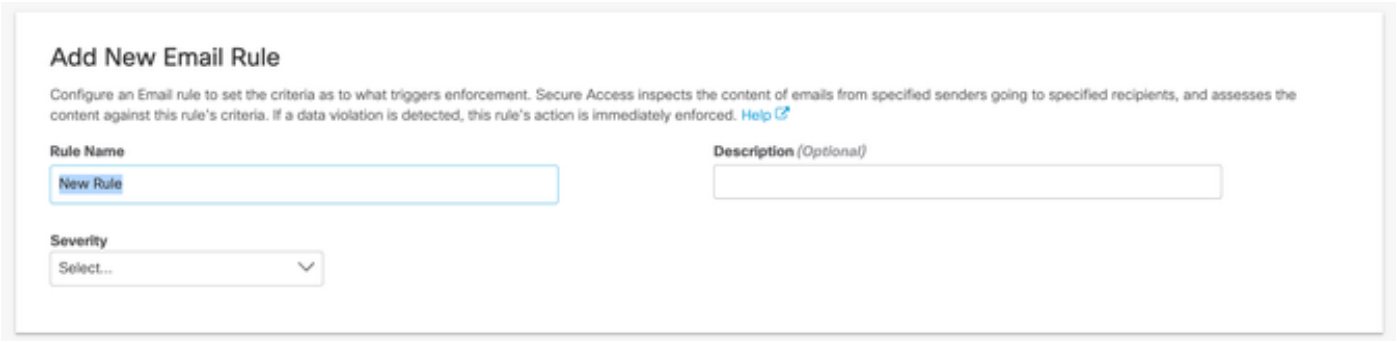
Stap 3: Informatie over basisregels configureren

Navigeer naar REGEL TOEVOEGEN > venster regel voor DLP e-mail,

Voer in het venster Nieuwe e-mailregel toevoegen de volgende gegevens in:

- Naam regel
  Voer een beschrijvende naam in voor de regel DLP e-mail.
- Beschrijving
  Geef een korte samenvatting van het doel van de regel.
- Ernst
  Selecteer het juiste prioriteitsniveau voor het beleid:
    - Laag
    - Gemiddeld
    - Hoog
    - Critical (Kritiek)

Deze velden helpen bij het categoriseren van de regel voor administratie, rapportage en operationele zichtbaarheid.



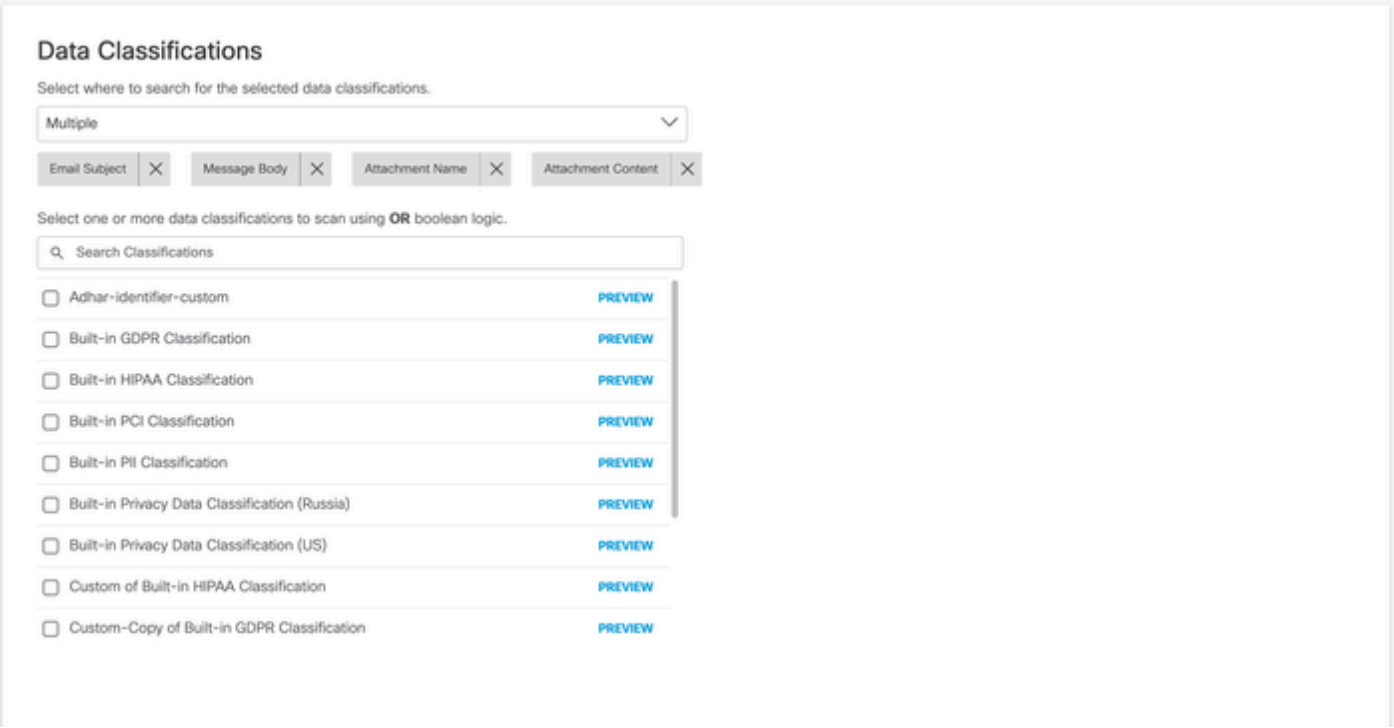
Stap 4: Gegevensclassificaties selecteren

Selecteer onder Gegevensclassificaties de vooraf gedefinieerde DLP-sjabloon die wordt gebruikt om e-mailinhoud te inspecteren op mogelijke DLP-overtredingen.

Kies vervolgens waar de geselecteerde classificaties moeten worden aangepast. Ondersteunde inspectielocaties zijn onder meer:

- Onderwerp e-mail
- berichttekst
- Naam bijlage
- Bijlage-inhoud

Hierdoor kan het beleid zowel de inhoud van het bericht als de bijlagen op gevoelige informatie controleren.



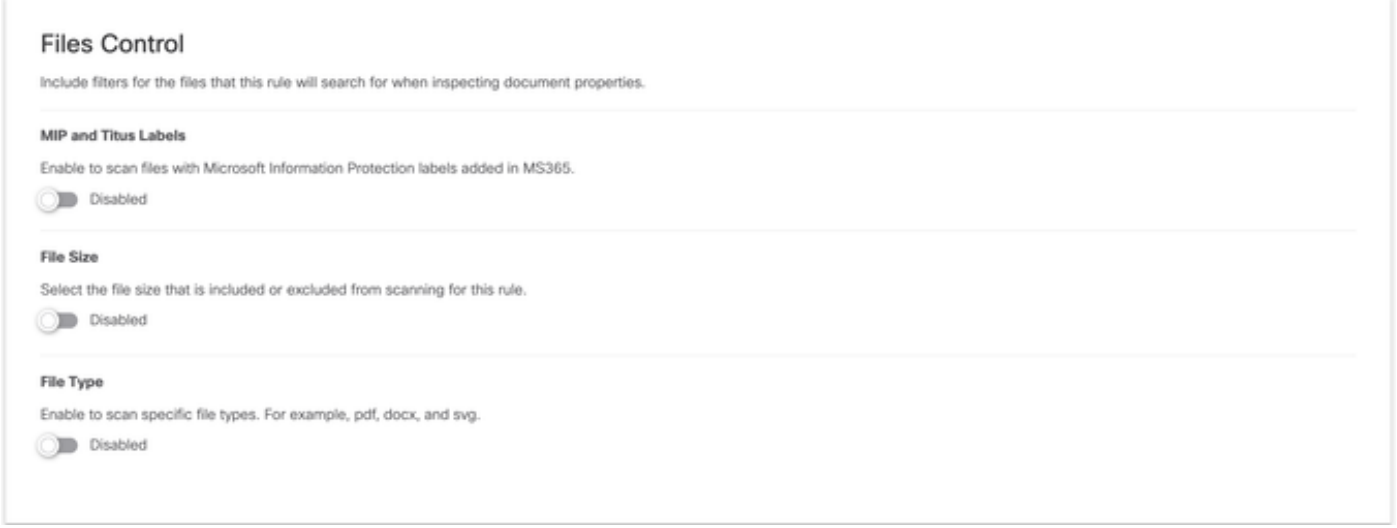
Stap 5: Bestandsbesturingselementen configureren

Configureer onder Bestandsbeheer de bestandsinspectiecriteria voor de regel.

Dit omvat ondersteuning voor:

- PMO-etiketten
- Titus-etiketten

Deze instellingen zijn handig wanneer DLP-handhaving rekening moet houden met gevoeligheidslabels of metagegevens die zijn gekoppeld aan gekoppelde bestanden.



Stap 6: Omvang afzender definiëren

Geef in het gedeelte Afzenders op op welke afzenders het beleid van toepassing is.

Beschikbare opties zijn onder meer:

- Alle afzenders
- Specifieke afzenders
- Specifieke afzenders uitsluiten

Hiermee kunt u de regel breed toepassen of beperken tot geselecteerde gebruikers of groepen.

Stap 7: Begunstigde scope definiëren

Kies in de sectie Ontvangers de gebruikers of groepen die moeten worden opgenomen of uitgesloten van beleidsevaluatie.

Beschikbare opties zijn onder meer:

- Inclusief alle gebruikers
- Inclusief specifieke gebruikers
- Specifieke gebruikers uitsluiten

Dit helpt bij het afstemmen van beleidshandhaving op basis van beoogde ontvangers.

Stap 8: Selecteer de beleidsactie

Kies in het gedeelte Actie hoe Cisco Secure Access moet omgaan met e-mails waarvan is vastgesteld dat ze de DLP-regel overtreden.

Beschikbare acties zijn:

- Monitor (bewaken)
  De e-mail is toegestaan en het evenement is geregistreerd voor zichtbaarheid en rapportage.
- Block (blokkeren)
  De e-mail wordt verwijderd om de overdracht van gevoelige gegevens te voorkomen.

Opmerking: momenteel kunnen positief geïdentificeerde e-mails worden toegestaan via de actie

Monitor of worden verwijderd via de actie Blokkeren.

Belangrijk: DLP-acties voor e-mail worden alleen geconfigureerd in Cisco Secure Access. Als een e-mail wordt geblokkeerd door Secure Access, is de gebeurtenis ook zichtbaar in Cisco ETD-berichttracering.

Stap 9: Gebruikersmeldingen configureren

De meldingsoptie is alleen beschikbaar voor de ontvangers.

Configureer onder Gebruikersmeldingen of gebruikers een melding moeten ontvangen wanneer een e-mail overeenkomt met het DLP-beleid.
Er is een optie om "Actor's Manager" of een "Aangepaste ontvanger" te melden. Een "Custom Recipient" kan iedereen zijn.

Configureer de e-mailberichtsjabloon van Standaard naar Aangepaste melding volgens uw behoefte.

Als deze functie is ingeschakeld, kunnen meldingen de bekendheid van gebruikers verbeteren en herhaaldelijke beleidsovertredingen verminderen. Configureer deze instelling volgens de operationele en nalevingsvereisten van uw organisatie.

Stap 9: Gebruikersmeldingen configureren

Gebruikersmeldingen zijn een krachtig hulpmiddel voor het bevorderen van beveiligingsbewustzijn en het waarborgen van naleving. Door gebruikers of beheerders te waarschuwen wanneer een e-mail een DLP-beleid activeert, kunt u onmiddellijk feedback en context geven met betrekking tot de overtreding.

Opmerking: meldingsinstellingen zijn voornamelijk bedoeld voor de ontvangers van e-mail en aangewezen belanghebbenden.

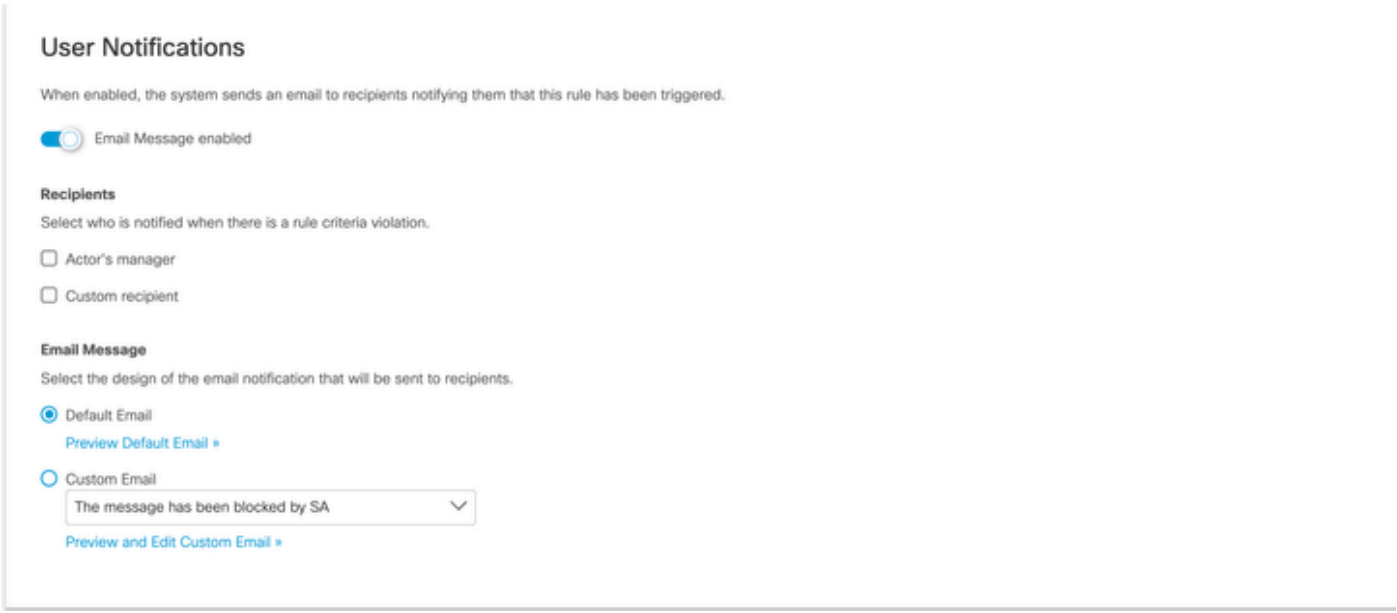
Meldingen configureren:

1. Ontvangers voor meldingen definiëren: Geef in het gedeelte Gebruikersmeldingen op wie de waarschuwing moet ontvangen. Je hebt twee primaire opties:
    - Actor's Manager: verzendt de melding rechtstreeks naar de manager van de gebruiker die de beleidsovertreding heeft veroorzaakt.
    - Aangepaste ontvanger: hiermee kunt u elk e-mailadres opgeven (bijvoorbeeld een

beveiligingscentrum of een specifiek afdelingshoofd).

2. Selecteer Berichtsjabloon: u kunt kiezen tussen de standaardmeldingsjabloon of een aangepaste melding.
    - Aanbeveling: Als uw organisatie specifieke vereisten voor compliance messaging of interne branding heeft, gebruikt u de optie Aangepast om de e-mailstructuur aan te passen om duidelijke, uitvoerbare instructies aan de ontvanger te geven.
3. Controleren en opslaan: zorg ervoor dat de instellingen na configuratie aansluiten op het operationele en nalevingsbeleid van uw organisatie.

Best Practice: Het inschakelen van deze meldingen is een effectieve manier om herhaalde beleidsovertredingen te verminderen door gebruikers in realtime te informeren over procedures voor de verwerking van gevoelige gegevens.



Opmerking: meldingsopties kunnen variëren op basis van de configuratie van de tenant en de beleidsinstellingen.

Stap 10: De regel bekijken en opslaan

Na het voltooien van de regelconfiguratie:

1. Controleer alle geconfigureerde instellingen.
2. Controleer of de geselecteerde gegevensclassificaties, de reikwijdte van de inspectie, de voorwaarden voor afzender en ontvanger en de actie overeenkomen met uw beoogde beleidsgedrag.
3. Klik op Opslaan om de DLP-regel voor e-mail te maken.

Het DLP-beleid voor e-mail is nu actief in Cisco Secure Access.

Optie 2: Een DLP-regel voor e-mail maken met een aangepaste DLP-sjabloon

Het maken van een aangepaste DLP-sjabloon omvat twee primaire fasen: het definiëren van een aangepaste ID en het configureren van de gegevensclassificatie.

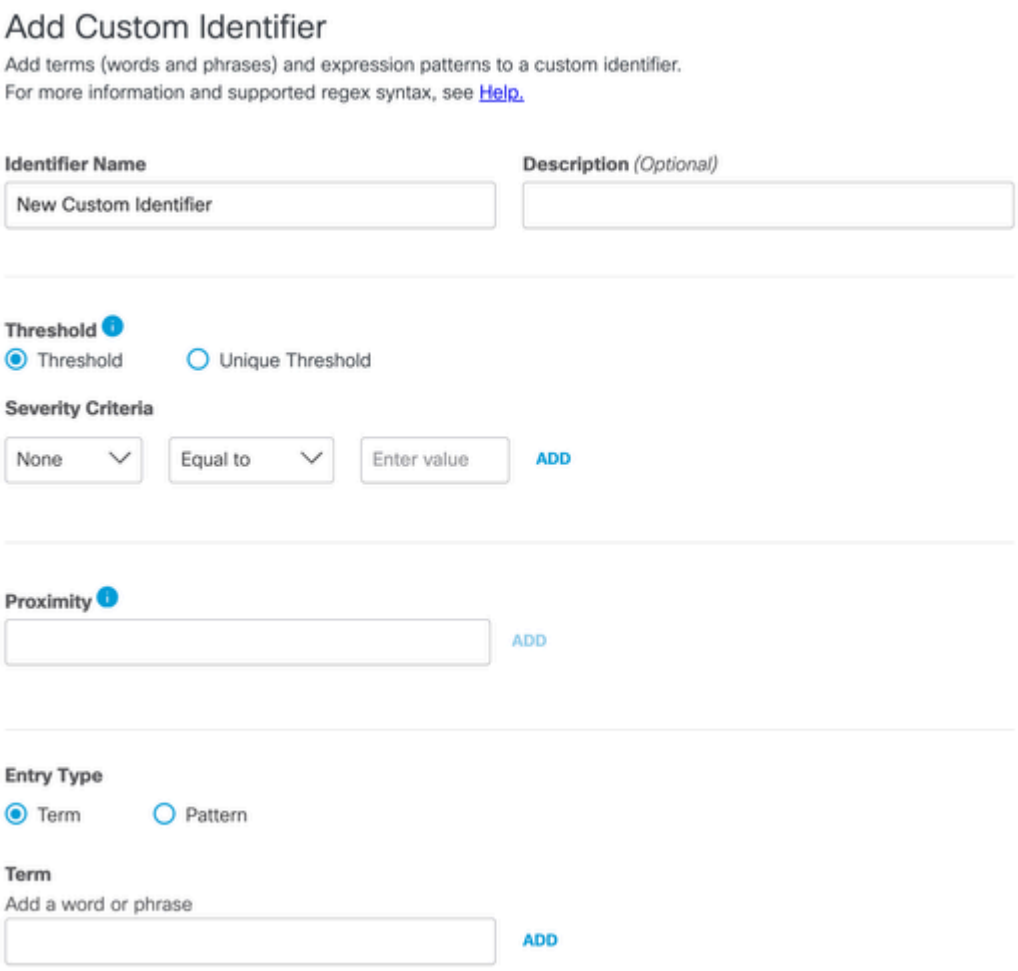
Opmerking: de engine voor gegevensclassificatie is zeer flexibel, zodat u beleidsregels kunt maken met één aangepaste ID of een combinatie van aangepaste en vooraf gedefinieerde ID's die zijn gekoppeld door AND/OR-booleaanse operatoren.

Stap 11: Een aangepaste ID maken

Voer de volgende stappen uit om een nieuw gegevenspatroon voor detectie te definiëren:

1. Log in op het Secure Access dashboard.
2. Navigeer naar Beveiligen > Gegevensclassificatie.
3. Klik op Aangepaste ID toevoegen.
4. Configureer de volgende parameters in het venster Aangepaste ID toevoegen:

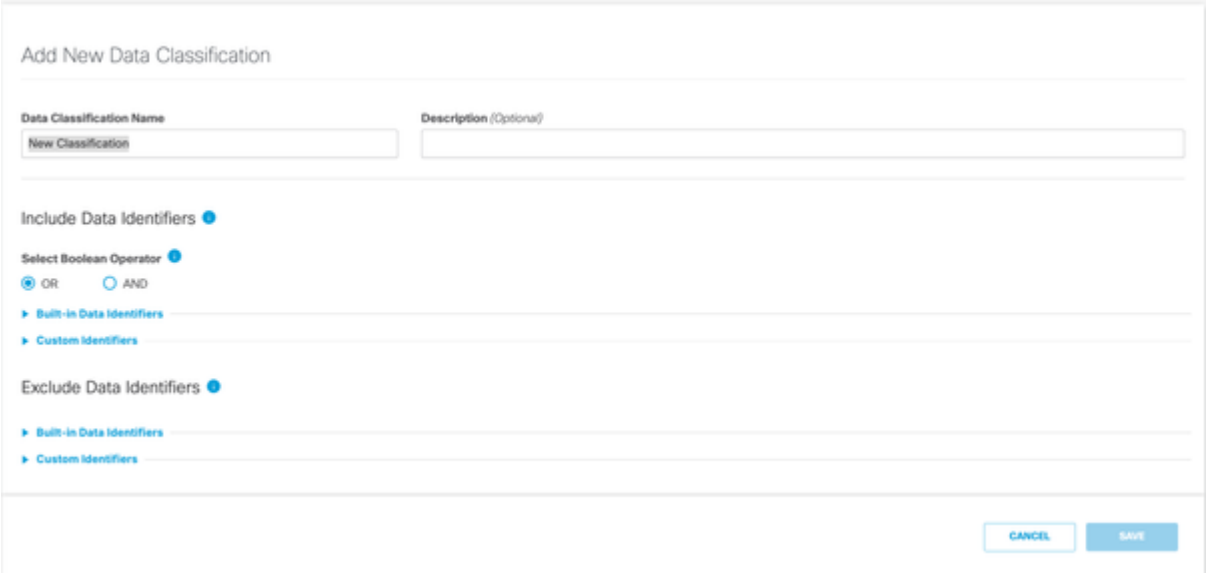
- Naam en beschrijving: Geef een unieke naam en een korte beschrijving van het gegevenstype dat u wilt detecteren.
- Drempelwaarde:
    - Drempelwaarde: hiermee wordt de totale frequentie van de gedetecteerde gegevens bewaakt.
    - Unieke drempelwaarde: bewaakt alleen het aantal unieke voorvallen van de gegevens, waarbij duplicaten worden genegeerd.
- Prioriteitscriteria: wijs prioriteitsniveaus toe (zeer laag, laag, gemiddeld, hoog) op basis van de detectiefrequentie. U kunt deze definiëren met behulp van vergelijkingsoperatoren zoalsGelijk aan, Groter dan, Minder dan of Bereik.
- Nabijheid: Stel de nabijheidsdrempel in. Dit geldt voor alle termen en patronen die binnen deze identifier gezamenlijk worden gedefinieerd, in plaats van per individuele term.
- Type invoer: Bepaal hoe het systeem de gegevens identificeert:
    - Term: een specifiek woord of woordgroep.
    - Patroon: een reguliere expressie (regex) die wordt gebruikt om specifieke gegevensformaten te detecteren (bijvoorbeeld creditcardnummers of interne projectcodes).



Stap 12: Gegevensclassificatie configureren

Zodra uw aangepaste ID is opgeslagen, kunt u deze integreren in een gegevensclassificatieobject:

1. Navigeer naar Beveiligen > Gegevensclassificatie > Toevoegen (gebruik de knop rechtsboven)
2. Selecteer uw nieuw gemaakte aangepaste ID in de beschikbare lijst.
3. (Optioneel) Combineer uw aangepaste identificatiecode met vooraf gedefinieerde identificatiecodes met de AND/ORlogic om het detectiebereik te verfijnen.
4. Sla de configuratie op om deze beschikbaar te maken voor gebruik in uw DLP-beleid voor e-mail.
5. Zie onderstaande screenshot voor meer informatie.
6. Volg nu dezelfde stappen van stap 4 tot stap 10 om een beleid te maken met aangepaste gegevensclassificatie.



Deze configuratie zorgt ervoor dat uw organisatie gevoelige informatie kan detecteren die specifiek is afgestemd op uw interne gegevensstructuren en nalevingsvereisten.

Problemen oplossen

Als de DLP-regel voor e-mail zich niet gedraagt zoals verwacht, controleert u het volgende:

Regel komt niet overeen met e-mails

- Bevestig dat de juiste sjabloon voor gegevensclassificatie is geselecteerd.
- Controleer of de relevante inspectielocaties zijn ingeschakeld:
  - Onderwerp e-mail
  - berichttekst
  - Naam bijlage
  - Bijlage-inhoud
- Zorg ervoor dat de filters voor afzender en ontvanger de teste-mail niet onbedoeld uitsluiten.

E-mails worden niet geblokkeerd

- Controleer of de actie regel is ingesteld op Blokkeren en niet op Bewaken.
- Bevestig dat de regel is opgeslagen en ingeschakeld.
- Zorg ervoor dat de e-mailinhoud positief overeenkomt met de geconfigureerde DLP-criteria.

DLP-gebeurtenissen zijn niet zichtbaar in ETD

- Controleer of Cisco ETD en Cisco Secure Access goed zijn geïntegreerd.
- Controleer of ETD het relevante e-mailverkeer actief verwerkt.
- Controleer eerst of de gebeurtenis policy aanwezig is in Cisco Secure Access.

Overeenkomsten op basis van bijlagen worden niet gedetecteerd

- Bevestig dat de naam en/of inhoud van de bijlage zijn geselecteerd in het inspectiebereik.
- Controleer de instellingen voor bestandsbeheer als labels als MIPorTitus deel uitmaken van de logica van de regel.

---

beste praktijken

Houd rekening met de volgende best practices bij het implementeren van e-mail DLP-beleid:

- Begin met Monitormode om beleidsgedrag te valideren voordat u Block afdwingt.
- Gebruik duidelijke en beschrijvende regelnamen voor eenvoudiger beheer.
- Scope afzender en ontvanger voorwaarden zorgvuldig om onbedoelde wedstrijden te verminderen.
- Test met representatieve gegevens voordat deze op grote schaal worden geïmplementeerd.
- Controleer regelmatig het bijhouden van ETD-berichten om geblokkeerde of gecontroleerde e-mailactiviteiten te valideren.
- Gebruik aangepaste sjablonen waar bedrijfsspecifieke gegevensidentificatoren vereist zijn.

Samenvatting

Cisco Secure Access is het centrale platform voor het configureren van het DLP-beleid voor e-mail in een geïntegreerde implementatie van Cisco Secure Access en Cisco Email Threat Defense. Terwijl ETD zichtbaarheid en berichttracering biedt, worden alle DLP-regelcreatie, classificatieselectie, handhavingsacties en meldingen geconfigureerd in Secure Access.

Door vooraf gedefinieerde of aangepaste DLP-sjablonen te gebruiken, kunnen beheerders e-mailinhoud en bijlagen inspecteren, het bereik van afzender en ontvanger definiëren en acties voor controleren of blokkeren toepassen om te voorkomen dat gevoelige gegevens via e-mail verloren gaan.

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.