NOT USED Data Leak Prevention in ClrStream

Table of Contents

Data leak prevention for the Inbound mail flow

In addition to the mail policies which can control inbound, internal and outbound mail flow, you can configure some additional data leak prevention rules for the Inbound mail flow.

Your domain can be configured to **Intercept, Modify or Monitor** the incoming mail flow.

The **Intercept** actions possible are:

- Deliver now
- Delete message
- Quarantine
- Change recipient

The **Modify** actions possible are:

- Clean cleanable malware, delete those that cannot be cleaned
- Stamp the body with a cautionary message.
- Tag the subject with keywords which alert the recipient that the mail is from an external sender
- Delete matching attachments

The way to **Monitor** such Inbound mail would be to:

- Send an email notification to a predefined email id
- Send a bcc of the inbound mail to a predefined email id.

These actions can be taken for mails which match one or more of these **conditions**

- all inbound mail
- all inbound mail for a selected set of users on your domain
- mail from a selected set of senders to any user on your domain

- mail from a selected set of senders to a select set of recipients on your domain
- all mail with certain attachments

Configure the DLP rules for your domain

Inbound data leak prevention rules and mail policies are configurable via the back-end and we request you fill this spreadsheet (https://skyconnect.mithi.com/res/submit-dlp-requests-for-inbound-and-outbound-mailflow.xls) with the details and raise a ticket to the Mithi Support team (https://docs.mithi.com/home/helpdesk-for-customers#raising-a-ticket). We will configure the same for you.