Regulatory sensitive information

Sensitive data is data that is considered private or protected by law, policy, or contractual obligation. The Coro console discovers sensitive data stored on the emails and cloud drives of your users that may be subject to regulatory or data compliance requirements, such as sharing from OneDrive, Google Drive, Box, or Dropbox.

Note

Each organization is unique and is required to comply with specific sensitive data regulatory requirements. Use the **Coro interactive discovery tool here** to assess your specific data governance needs.

The following table shows the data transactions monitored by Coro. It includes information on the type of monitoring (data access, data exposure, or both):

Transaction	Monitoring	Detection	Component
Content and attachments of internal (inbound and outbound) email between protected users	Access	Ticket	Data
Content and attachments of outbound email	Access and exposure	On Event	Data
Content and attachments of internal email	Access and exposure	On Event	Data
Internal and external sharing of cloud drive files	Access and exposure	On Event	Data

Sensitive data objects which can be exposed and monitored by Coro from the transactions above can be categorized into the following four types:

Personally identifiable information (PII)

PII is any information connected to a specific individual that can be used to uncover that individual's identity This data includes:

- Social security numbers (SSNs)