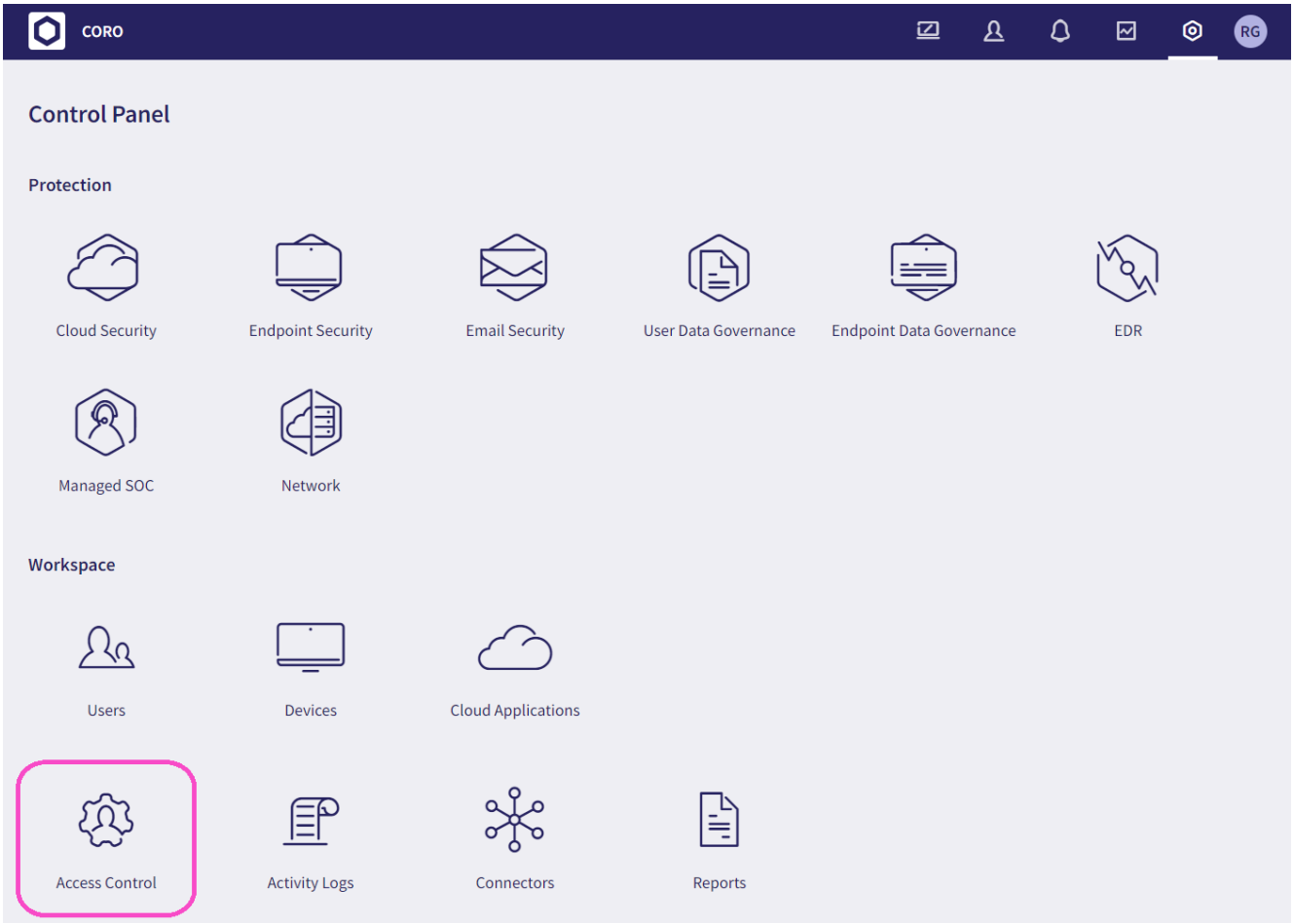
Content inspection permissions

Content inspection for cloud applications allows admin users to view sensitive data in the email content and findings sections of tickets related to **User Data Governance**. Sensitive data is data considered private or protected by law, policy, or contractual obligation. When disabled, these sections display a message stating *Access to sensitive data is restricted* if they contain sensitive data.

Coro enables content inspection by default. You can enable or disable content inspection from **Content inspection permissions**.

To access **Content inspection permissions**:

1. **Sign into the Coro console**.
2. Select **Access Control**:



3. Select the **Admin users** tab: