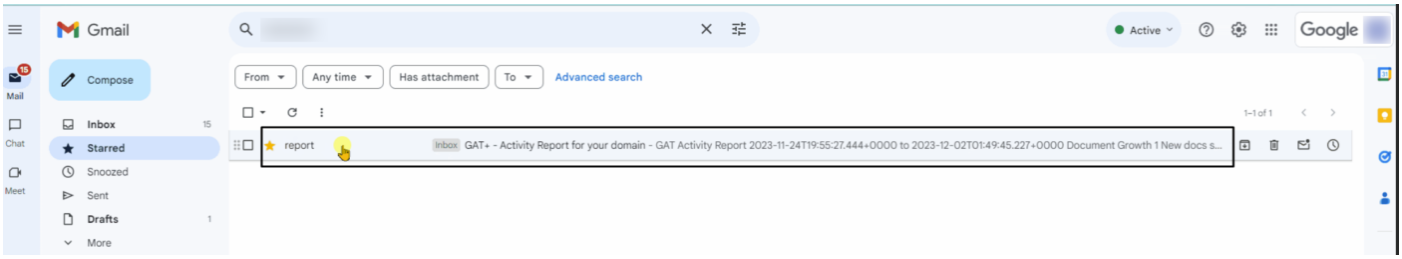
How to Monitor External Email Attachments with GAT+ Activity Report

Email Audit & Management · https://gatlabs.com/knowledge/tech-tips/how-to-monitor-external-email-attachments-with-gat-activity-report/

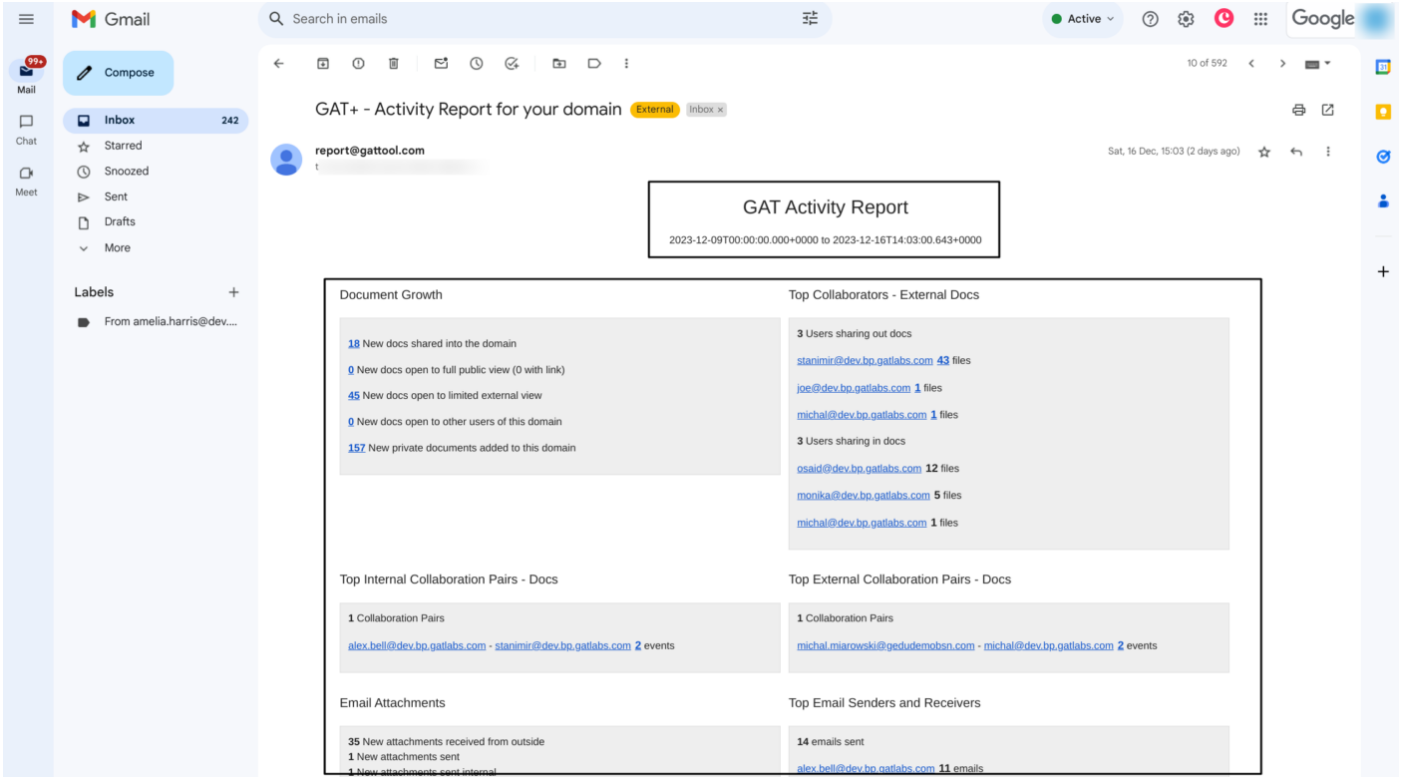
Identify potentially dangerous external attachments sent via email

Learn to monitor email attachments with GAT+ effectively, a vital tool for Google Workspace admins aiming to safeguard their domains against external threats. Effortlessly accessible, this essential feature delivers weekly reports directly to your admin inbox, keeping you consistently informed and vigilant.

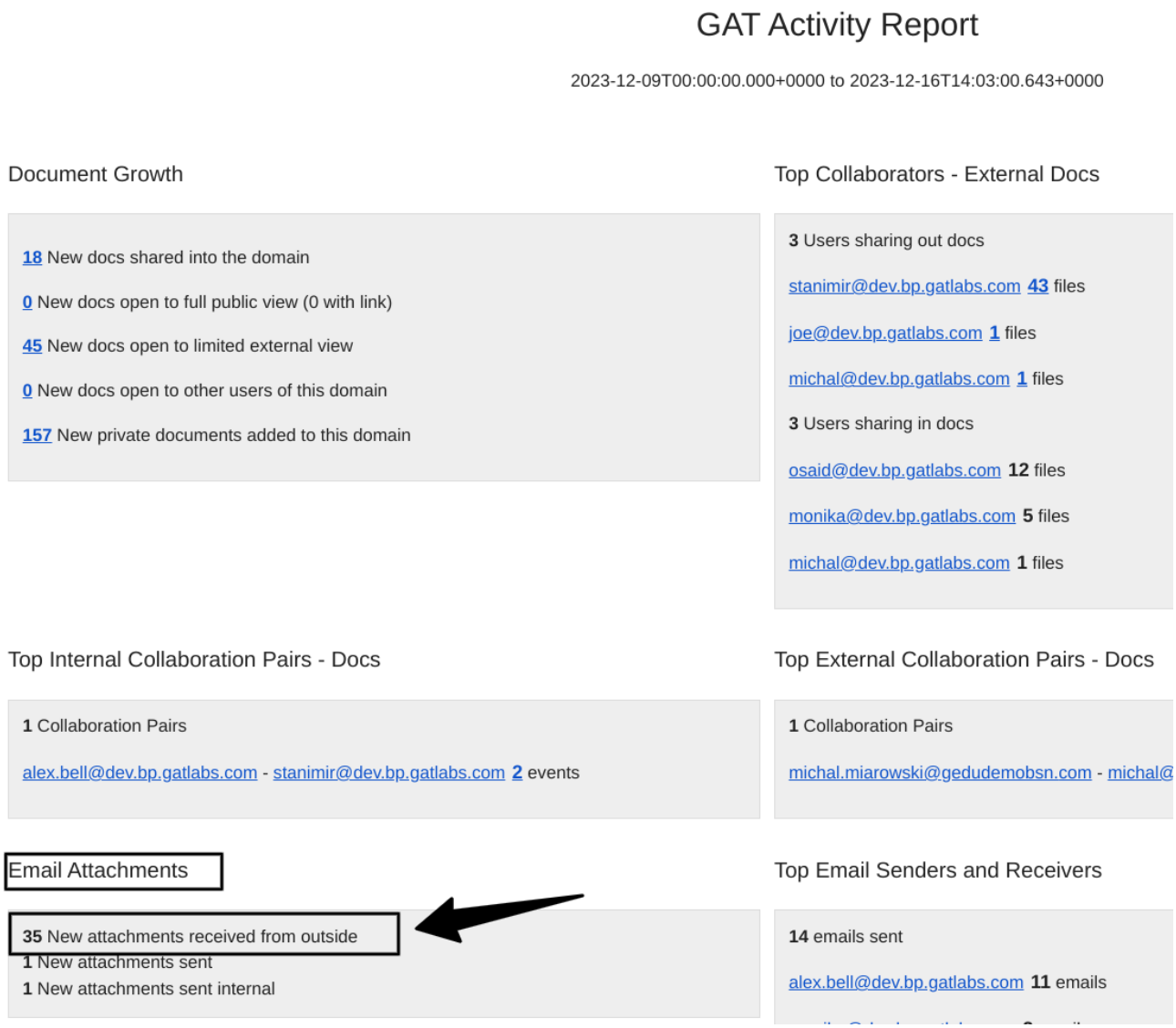
The Administrator can use the GAT+ Activity Report sent weekly, which contains a shortened report on what happened in the domain during the last week.



The Activity Report is sent weekly to Google Workspace domain super administrators and can be the first step in identifying suspicious shares or attachments arriving on your domain and taking appropriate action.



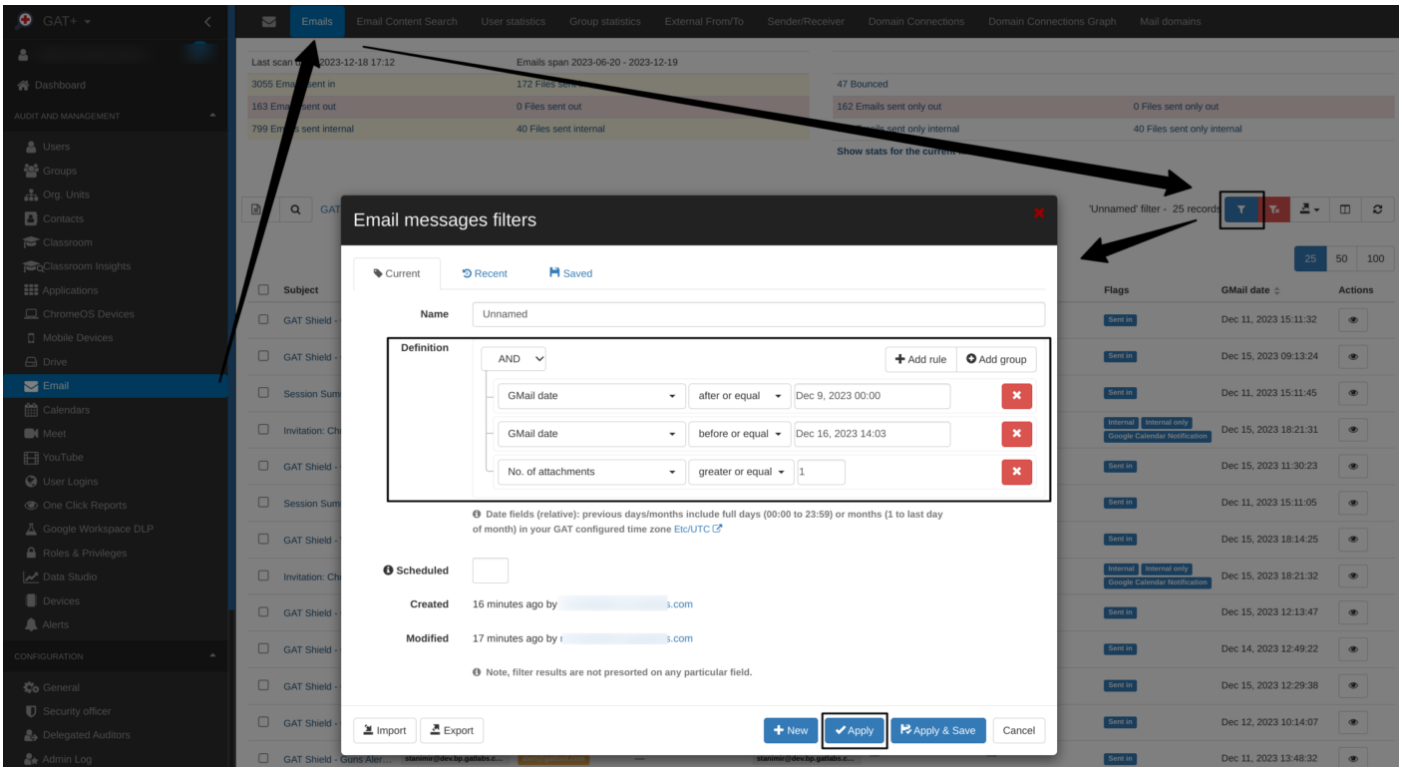
In this article, we focus on how to monitor email attachments with GAT+, particularly ***new attachments received from outside.***



This particular Activity Report shows 35 **New attachments received from outside**. That number is not clickable however the relevant filter can be used to identify those emails with attachments.

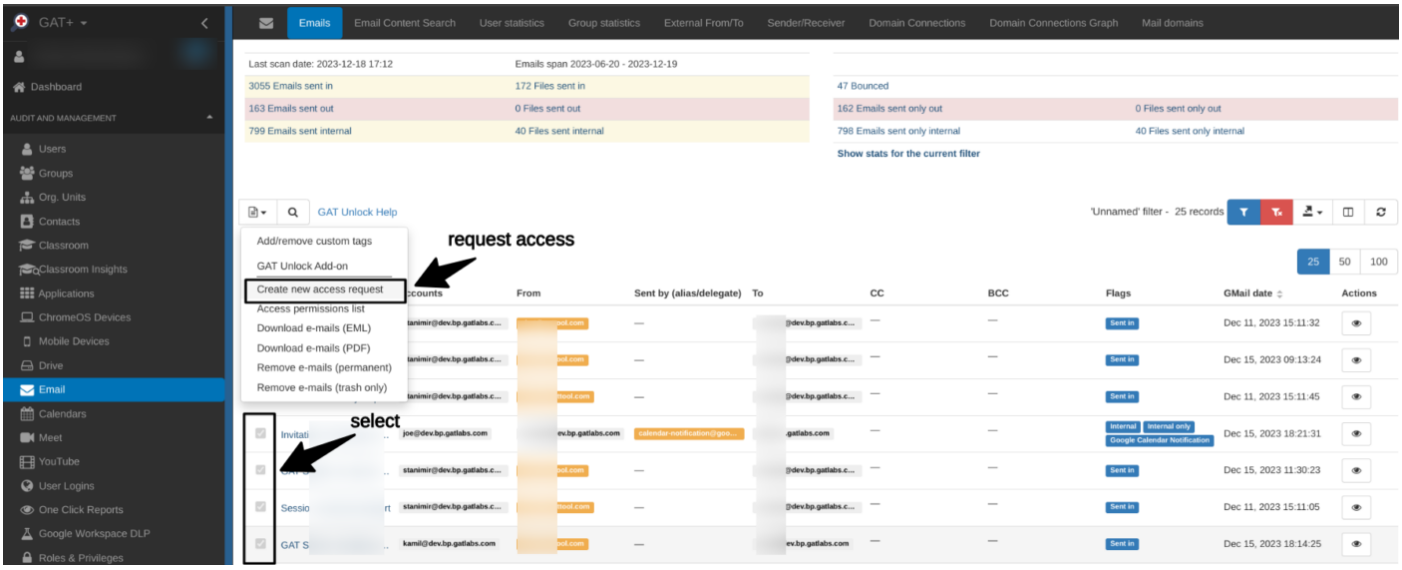
NOTE: *Ultimately, all numbers will be clickable and will redirect to a specific section in the GAT+ console.*

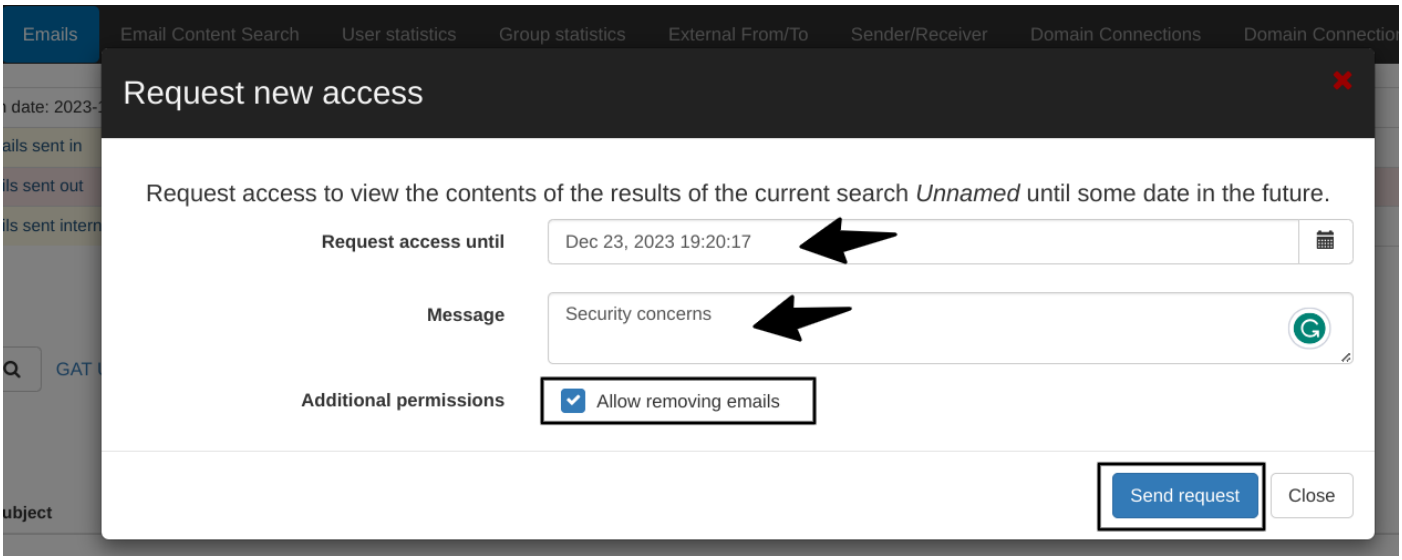
Apply the below filter to thoroughly check each of the 35 attachments sent from outside to your local users' inboxes that week, enhancing your process of monitoring email attachments with GAT+.



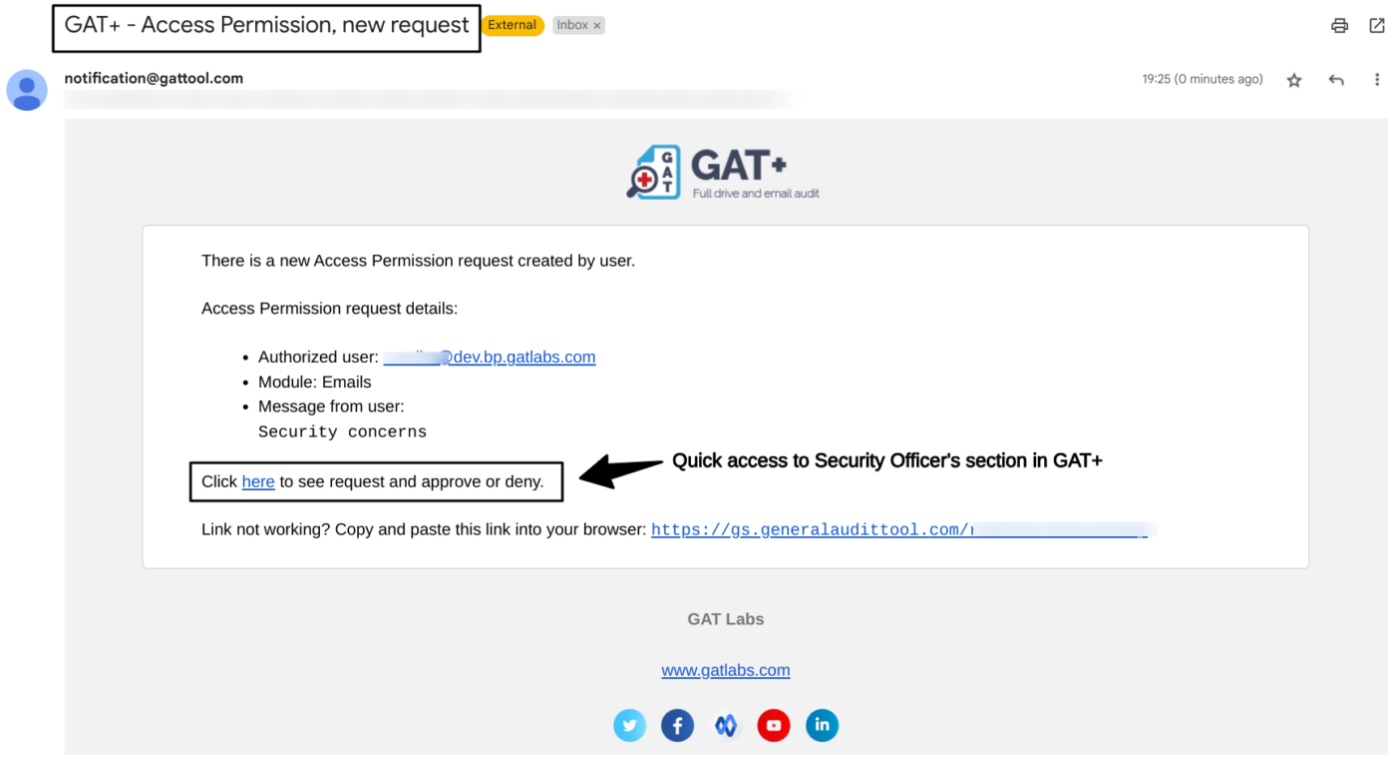
If any of the emails appear to pose a security risk, you can request to access those emails to view and remove them.

Select all the relevant metadata in GAT+, and request access:

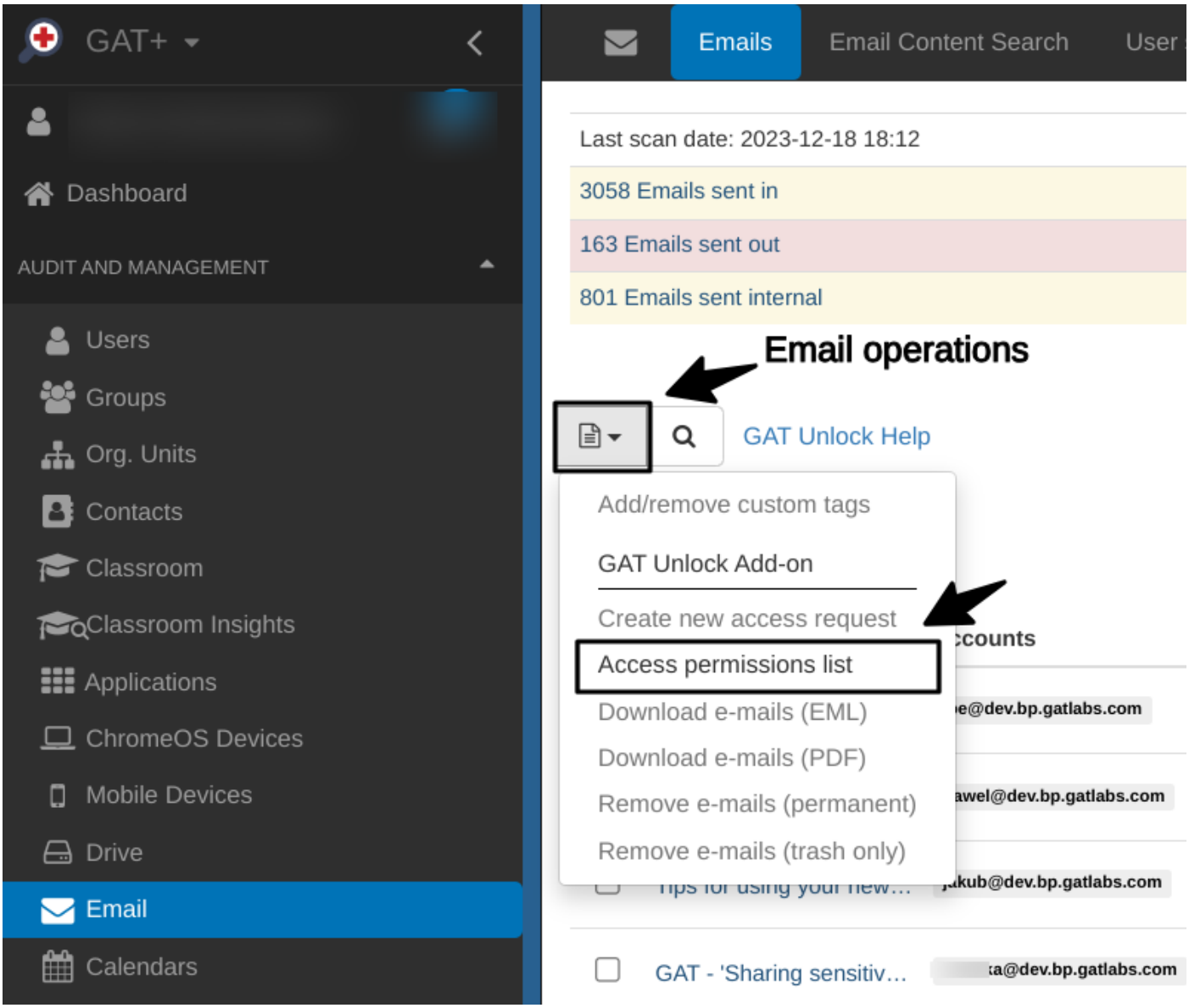




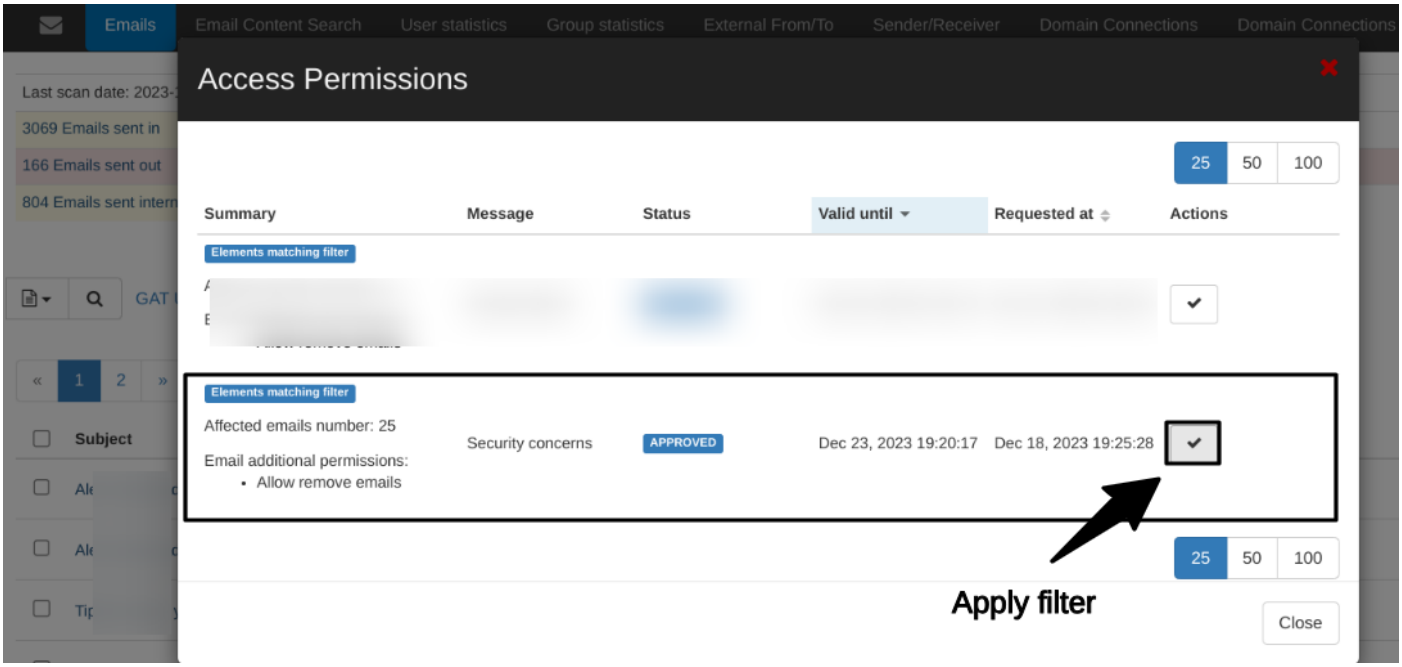
The Security Officer must approve the request.



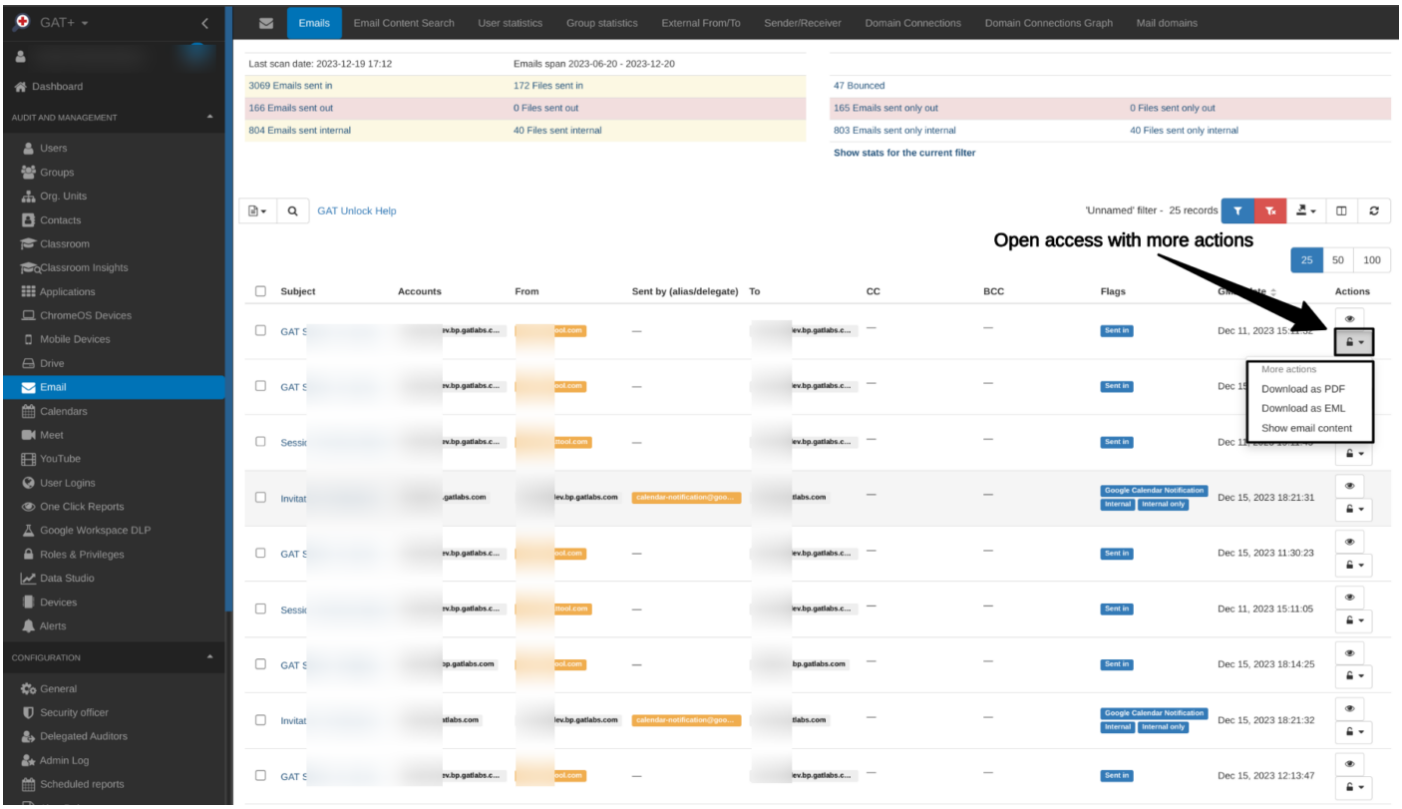
Once approved by the Security Officer, an administrator can bring back the filter and relevant metadata. Clicking on the **Access permissions List** under the **Email operations.**



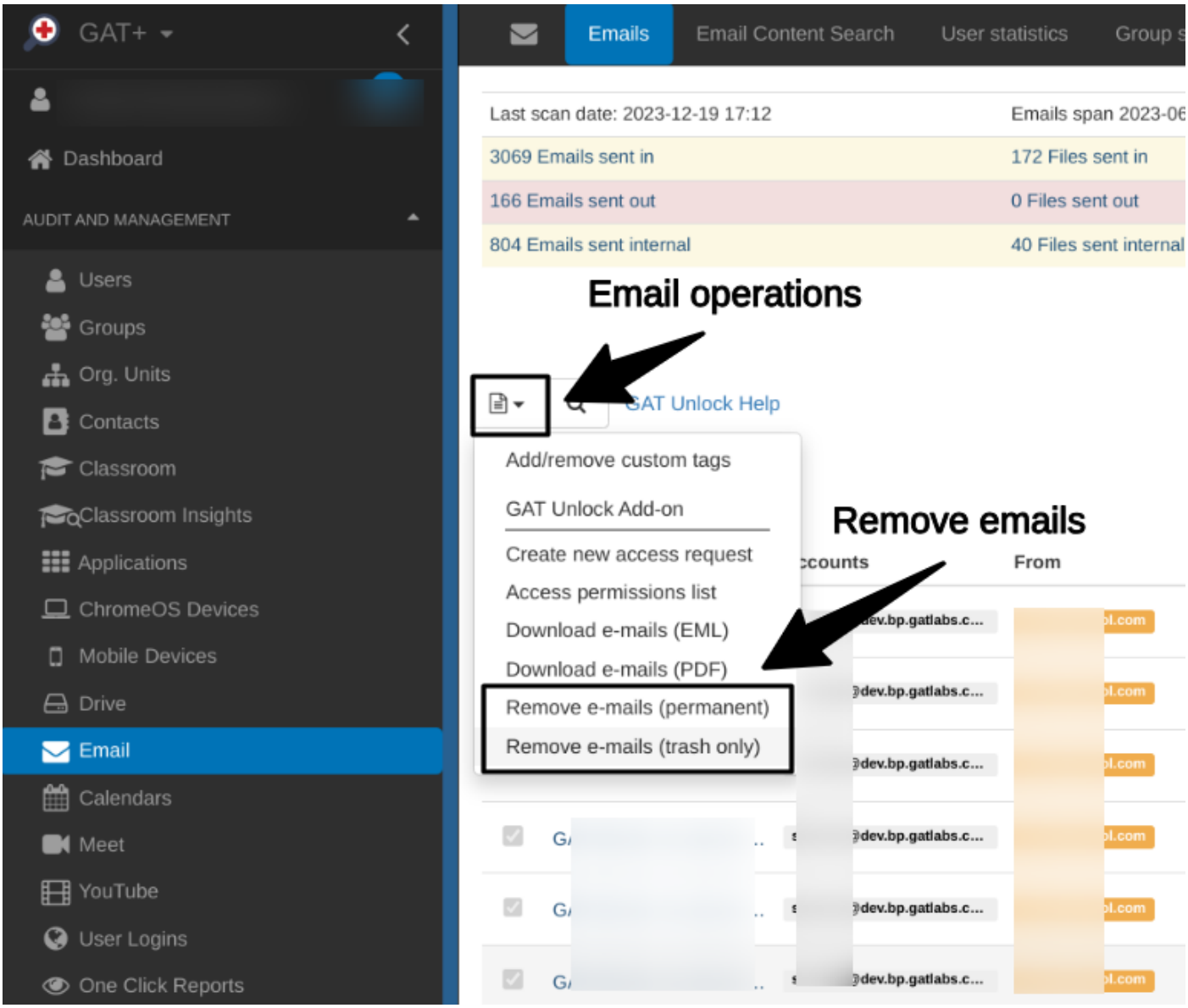
The system will return the relevant metadata with open access.



An Administrator can view or download the content by clicking on the **More Actions** button (the open 'lock' icon)



Additionally, you can remove potentially dangerous emails by clicking on the **Email Operations button** and selecting one of the removal options.



Finally, by learning to monitor email attachments with GAT+, you ensure your domain is always safe and well-protected.

Related posts

Domain Security Monitoring with GAT+ Activity Report

Activity Report for Your Google Workspace Domain

Find and delete Phishing emails

Delete Spam, Inappropriate or Accidental Emails

Delete Domain Users' Emails That Pose Security Risks with GAT+