Google Workspace Admin Best Practices in GAT Suite

Getting Started · https://gatlabs.com/knowledge/tech-tips/best-practices-gat/

There are many different ways Google Workspace admin can set up Google domain to efficiently protect against possible threats and prevent data loss.

The GAT Suite of tools specializes in Security Management and Data Loss Prevention.

GAT requires very little setup on installation, but here are a list of some popular actions and best practices you can take as the administrator, to better optimize your domain for DLP.

Best Practices List

- Generate a monthly report on the extensions your employees are installing
  Chrome extensions audit
- Restrict users from downloading potentially malicious file types
  Report and remove file downloads
- Setting up alerts for when racial/homophobic language is used (and take a screenshot)
  Configuring settings for Alert Rules
- Categorize sites with tags so you can see at-a-glance if employees are working
  Auditing sites with browsing tags
- Set up an alert for when Two Factor Authentication is disabled
  Alert when 2FA is disabled for any reason
- Set up document tracking for docs containing sensitive data
  Track visitors and editors of specific documents
- Set up policies for applications allowed on the domain
  Policies for Google Workspace apps
- Create copies of externally owned files
  List all externally owned files
- Remove public access to files (automatically after being shared)
  Remove public and public-with-link permissions from Google Drive Files

- Remove files shares to personal accounts

  Find all files shared to Gmail accounts and remove them
- Monitoring User Logins

  Monitoring Google Cloud login behaviour
- Find out who's missing their meetings

  Report when the Google Meet organiser is not present
- Set up alerts for Email Delegation

  Email delegation alert rule
- Set up alerts for new email filters

  Alert for new Gmail filter added
- Automate actions that will be taken when a user violates an alert

  Set up event workflows based on GAT+ alerts via GAT Flow
- Force users to change their passwords every 3 months (set as a recurring workflow to run automatically)

  Change users passwords at the next login in bulk
- Allow users access to shared drives and sensitive folders automatically, only when 2FA has been enabled (and remove access if 2FA is disabled)

  Run workflows based on 2FA change
- Remove email filters regularly (automatically)

  Remove users email filters in bulk
- Configure a set of actions to do when offboarding users (transfer files, remove app tokens, set Out of Office reply)

  Actions available when offboarding users
- Deploy the GAT Shield extension to everyone in your organization

  Deploy GAT Shield