GAT LABS TRAINING RESOURCES

2

DLP + Alerts Across Google Workspace



Ē٦

Training Resources

DLP and Alerts Across Google Workspace

Learn how to proactively prevent data breaches, control sensitive data exposure, and receive alerts for critical activities using GAT+.

Understanding DLP in GAT+

Data Loss Prevention (DLP) helps monitor and control sensitive data movement across Google Workspace to prevent accidental or intentional leaks.

Key DLP Features in GAT+:

- Sensitive Content Search (SSNs, financial data, keywords, etc)
- File Exposure Controls
- Automated Remediation Actions

Types of Alerts in GAT+:

- Applications
- Emails
- Drive
- YouTube
- Mobile device
- Users
- Users Logins

Related Articles: Better reporting for Google Workspace DLP



1. Drive DLP Rules: Top 3 Actions You Can Take

Take immediate control over file sharing activities and prevent sensitive information from leaving your domain with these top DLP actions.

1.1. Identify and Remove External Sharing for Sensitive Files

GAT+ helps you detect and take corrective action on files that have been shared externally.

Navigate:

GAT+ > Drive > File Content Search

Steps:

- Enter specific sensitive keywords or patterns (e.g., "SSN", "Confidential").
- Use advanced syntax for precise filtering.
- Select users, groups, or OUs to apply the search.
- Review results and take immediate action by adjusting sharing permissions.

🟓 GAT+ - <	æ	Files	File Content Search	Files Deleted	Shared Drives	Events	Folders Tree	External Domains
🛓 Barren Nigeler 🔺 👻		2	2	Querv				~
希 Dashboard							-	
AUDIT AND MANAGEMENT					Ful	nly?		
🐣 Users				User / group			Org. Unit	
嶜 Groups							Include sul	OUs
Contacts					Search files	Previous	searches C	ear
🞓 Classroom								
Classroom Insights								
Applications								
ChromeOS Devices								
Devices								
🔒 Drive 🚺								
🔄 Email								
🚠 Classic Sites								

Related Articles: Search for Sensitive Content in Files



1.2. Auto-Remove Public Sharing Permissions

You may find that users from your domain have shared Google files publicly. Use this method to quickly restrict those files

Navigate:

GAT+ > Drive > Audit table > Select Full Public (everyone) or Public with link (everyone with link)

Steps:

- Apply a filter where the Sharing Flag contains Public or Public with link.
- Add an extra filter: Sharing Flag does not contain Shared In to exclude files shared into your domain from external domains.
- Review the results and take corrective actions.

 infrigue donce <	🔶 GAT+ 🔹 <	E Files File Content	Search Files Delet	ted Shared Drives	Events Folders Tree	External Domains	Domain Connection G	raph External Users		
Cashbadd Cashbadd Cashbadd Cashbadd Cashbadd Cashbadd Cashbadd Cashbadd Cashbadd Cashbadd Cashbadd Cashbadd Cashbadd Cashbadd Cashbadd Cashbadd Cashbadd Cashbadd </td <td>🛔 Enrique Gomez 🛛 🌲 👻</td> <td>Total 30251 files/folders</td> <td></td> <td></td> <td></td> <td>17608 files</td> <td>C</td> <td>] 12843 folders</td> <td>A 221 Shortcuts</td> <td></td>	🛔 Enrique Gomez 🛛 🌲 👻	Total 30251 files/folders				17608 files	C] 12843 folders	A 221 Shortcuts	
280.0pen to P.tatio with lask 16415 Open to pactor internal werp) 100 fm 100 fm 200 f	A Dashboard	27 Open to full public	1147	Open to specific external us	er(s)	1071 docume	nts [1424 text files	902 image files	
All Market Control Control Control <td></td> <td>258 Open to Public with link</td> <td>1641</td> <td>5 Open to specific internal u</td> <td>ser(s)</td> <td>12064 spread</td> <td>sheets</td> <td>4 audio files</td> <td>1084 PDFs</td> <td></td>		258 Open to Public with link	1641	5 Open to specific internal u	ser(s)	12064 spread	sheets	4 audio files	1084 PDFs	
▲ Londa peter Schward Drive Files 327 Drivend Drive Files with satura status: 1 or since 1 or since 1 or since ▲ Conda 0 contracts	ALIGIT AND MANAGEMENT	1263 Files owned by us shared out	173 F	Files owned by others shared	lin	129 presentat	ions E	299 video files	1 2 maps	
Straubal 15550 Private 9 Tashed Bower state for the current filter Casaroom Straubal 0 suff-errors Casaroom Cast Unlock Help CastronoolS Devices ConsonoolS Devices ConsonoolS Devices CastronoolS Devices <t< td=""><td>🛓 Usera</td><td>968 Shared Drive Files</td><td>327 5</td><td>Shared Drive Files with extra</td><td>sharos</td><td>54 forms</td><td></td><td>17 sites</td><td>3 24 drawings</td><td></td></t<>	🛓 Usera	968 Shared Drive Files	327 5	Shared Drive Files with extra	sharos	54 forms		17 sites	3 24 drawings	
Contacts Contacts Conservoin Conservoin <	👹 Groups	13560 Private	9 Tra	shed		Show stats for th	e current filter			
C Cusarconn C Cusarconn C Cusarconn C Curarconne C Cu	Contacts	94 orphaned	D aut	ih errors						
Classroom Insights I Applications I Applications I Applications I Modie Devices I Table I Table I Table I Applications I Table I Applications I Table I Applications I Table I Applications I Appli	Classroom									
Applicators Applicators ChromoloS Devices Modile Devices ChromoloS Devices <t< td=""><td>Classroom Insights</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>	Classroom Insights									
Chromodo D Davicas Mobile Devices Chromodo D Davicas Mobile Devices Chromodo D Davicas Chromodo D Dav	## Applications	Q GAT Unlock Help	3			'Files with sharing f	lag: 'Public with link' filter	- at least 26 records	ть Д.	
Modele Devices	ChromeOS Devices									
Christe Tritice Paths Owner Contributors Vewer* Updated 2 Flags Saring flags Action Conscionation Conscionation Paths Owner Contributors Vewer* Updated 2 Flags Saring flags Action Conscionation Paths Paths Paths Conscionation Paths Paths Contributors Paths Paths Paths Action Conscionation Paths		· 1 2 ·							25	50 100
Second Secon	🔒 Drive	Title F	Paths	Owner	Contributors	Viewers	Updated \Rightarrow	Flags	Sharing flags	Actions
Classic Sites	🖂 Email					Ø everyone (with linig 💌			Spearits ownernal sweets?	
Caleradars Meet Voctube Caleradars Voctube Caleradars Conscience Caleradars Conscience Caleradars Conscience Caleradars Conscience C	Classic Sites	🗆 🍓 testing 👻 4	4 Replace Public on web	4 Replace Public on web	•	@ 3 goclusternation.com	Remove permission for on	ly this file		*
Meet Weet You Tube One Click Reports Geogle Workspace DLP Roles & Privileges Adresis Consolitation for membership Consolitation for membership <t< td=""><td>🛗 Calendara</td><td></td><td></td><td></td><td></td><td>e evenuone leith linid</td><td>Rem 🕄 everyone (with lin</td><td>k) as Viewer from files in co</td><td>urrent filter</td><td></td></t<>	🛗 Calendara					e evenuone leith linid	Rem 🕄 everyone (with lin	k) as Viewer from files in co	urrent filter	
Workspace DLP -/ Sovercastly -/ Sovercastly Remove everyone (with link) as Contributor and Veryer from files in current filter Consolita webm = -/ Sovercastly -/ Sovercastly -/ Sovercastly -/ Sovercastly Google Workspace DLP Socials Phylicity -/ Sovercastly -/ Sovercastly -/ Sovercastly A long & -/ Sovercastly -/ Sovercastly -/ Sovercastly -/ Sovercastly A long & -/ Sovercastly -/ Sovercastly -/ Sovercastly -/ Sovercastly A long & -/ Sovercastly -/ Sovercastly -/ Sovercastly -/ Sovercastly A long & -/ Sovercastly -/ Sovercastly -/ Sovercastly -/ Sovercastly A long & -/ Sovercastly -/ Sovercastly -/ Sovercastly -/ Sovercastly - -/ Sovercastly -/ Sovercastly -/ Sovercastly -/ Sovercastly -/ Sovercastly - - - -/ Sovercastly -/ Sovercastly -/ Sovercastly -/ Sovercastly -/ Sovercastly -/ Sovercastly - - - - - - -/ Sovercastly -/ Sovercastly -/ Sovercastly -/ Sovercastly <td>Meet</td> <td>🗆 🝓 testing 🕶 💡</td> <td>/ Public on the web</td> <td>2 Remove Only the following Ex</td> <td>Cernel Stretes</td> <td>2 gedudemober.com</td> <td>Remove everyone (with lin</td> <td>k) as Contributor from files</td> <td>in current filter</td> <td></td>	Meet	🗆 🝓 testing 🕶 💡	/ Public on the web	2 Remove Only the following Ex	Cernel Stretes	2 gedudemober.com	Remove everyone (with lin	k) as Contributor from files	in current filter	
• Loss Logists • Jossen Logist • Jossen Logists • Jossen Logists • Jossen Logists • Jossen Logist • Jossen Logists • Jossen Logist • Jossen • Jos	🖽 YouTuba						Remove everyone (with lin	k) as Contributor and View	er from files in current filte	er
• One Click Reports • One Click Reports • My Dife / Screenaally • • Patie with the Screenaally • • Patie with the Screenaally • • •	🚱 User Logins	- Admin	. / Screencastily	camils.b@gedudemobss.com		everyone (with link)	2 months and		Specific internal user(it)	
¹ Google Workspace DLP ¹ Relate 8 Privileges ¹ Alarts ¹ Relate 8 Privileges ¹ Alarts ¹ Status Chromatook ¹ / Salis 0 Promotion ¹ Salis 0 Privileges ¹ Salis 0	One Click Reports	console.webm •	My Drive / Screencastify	*	- grossenitos - sm	*		_	Public with link Shweet out	
Roles & Privileges Alerts Alerts Alerts Alerts Model Alerts Model Alerts Alerts Model Alerts M	A Google Workspace DLP					@ meanstone benth linist				
Alerto Alerto Alerto Alerto Alerto Alerto My Alerto M	A Roles & Privileges	🗋 🛐 Testing 🕶 🕴 4	4 Replace Public on web	4 Heplace Public on web	-	© 2 gecludemoben.com	5 months ago	Shared Drive Shared Drive Extra ACLs	Specific internal user(s) Public was link - Brand out	۲
Constrained Master Chrometook ./ Salto Chrometook ./ Salto Chrometook	Alarte									
CourseLine Course Line Course		Master Chromebook	/ Sal's ChromeOS	ferdows#geducismobsrucom	_	ovoryanu (mil): link) 💌	. A months and		Specific Internel user(s)	
\$\$6 General My Drive answerster den damate = excepted balls \$20 - \$2466 attribute \$24		T Dat - Distribution Sheet	Devices Exports	•		przemaktestikyedudemoto	4 monens ago	-	Public with link drived out	
	🖧 General	🗆 🍙 Logs 🕶 🛛 🛔	My Drive	student.stan@geducionecbs	-	avaryona (alit 2nk) 💌	2 years ago	-	Public with link Shared out	

Related Articles: Find Publicly Shared Google Drive Files



1.3. Enforce Download Limits to Prevent Data Exfiltration

Receive alerts when a user downloads more than X files in a short timeframe.

Navigate:

GAT+ > Configuration > Alert Rules

Steps:

- Click on the + sign, and a new window will be displayed. Fill in the details.
- Alert recipients: Enter recipient emails who will receive an email for the alert (optional) By default, all alerts will be shown in *GAT+ > Alerts*
- Select "Alert on a number of files downloaded."
- Set the threshold to trigger the alert.

115000000000000000000000000000000000000				
		tiles in a 24 hour period		
		Exclude the following applications from calculation		
		Google Drive for desktop	3	
	Γ	Search for an application that should be excluded from the alert		
		Type in the application name 2 •		
		The alert will be triggered when 50 different files are downloaded.		
		Downloads counted by this alert don't have to come from an active user. Files downloaded by third-party applications will be counted too. The user reported to have downloaded the files would be the user who authorized the application with the access.		
		A third-party application can have users' credentials and do the downloads, even if the users are inactive, haven't logged in for a while or don't take any actions that would give them direct access to the files reported by this alert.		
Alert on number of files shared out				
Alert if regex matches a newly shared out file (doc.			+	
spreadsheet, presentation, PDF, text files):				
Alert if 'share to' address matches specified pattern				
			4	

Related Articles: Set Up a Google Drive DLP Alert When the Number of Downloaded Files Exceeds X



2. Expanding DLP to Gmail and Mobile Devices

Take your DLP efforts beyond Drive to protect email and mobile environments.

Navigate: (

GAT+ > Configuration > Alert Rules

2.1. Gmail DLP Controls

Choose any of the options available for the Email alert rules:

- Alert on External email forwarding (when email forwarding is enabled)
- Alert on Email delegation (when email delegation is set)
- Alert on new Gmail filters (when a new Gmail filter is added)
- Alert on new email "send as"
- Alert on number of external emails received (emails in a 24 hour period)
- Alert on number of external emails sent (emails in a 24 hour period)
- Alert on number of external emails sent (by number. of recipients)
- Alert on number of internal emails received
- Alert on number of internal emails sent

Alert Ru	les				
+					at least 26 re
Ad	d / edit alert rule				22
Name ¢	Name	Email	alarms		
	Enabled	Emails		•	
Email alarm:	Scope	Group		•	n
	Destation		gedudemobsn.com ×		
	Alert on External email		jeudemoush.com x		
Applications access to G	Alert on email delegation				
	Alert on new Gmail filters				
Drive alerts	Alert on new email Send As Alert on number of external emails received		50 • emails in a 24 hour parind		
	Alert on number of external emails sent		70 • emails in a 24 hour period		
Youtube aler videos				H Save	Cancel



Related Articles:	 Set Up a How to set up Gmail alerts for Google Workspace users Set up a Google Alert when a new filter is
	added in Gmail Drive DLP Alert When the Number of Downloaded Files Exceeds X

2.2. Mobile Device DLP Controls

Using the Alert Rule mechanism provided in GAT+, Super Admins or Delegated Auditors can alert on violations detected on corporate-enrolled mobile devices.

Steps:

- Set the Type to Mobile Device.
- Define the scope: User, Group, or Org. Unit.
- Select alert recipients to receive notifications.

Alert Rules		
+		'Unnamed' filter - 2
Add	/ edit alert rule	×
Youtube aler	Name	Mobile devices alert for not synchronized and idle devices
videos	Enabled	
Youtube Aler	Туре	Mobile devices
	Scope	Org. Unit
		 O you can use wildcard character [*], which will be interpreted as any number of characters (0 or more). Example of use: (* - full domain (root OU and all sub OUs), /Testou* - all OUs that start with /TestOU, /Testou/* - all sub OUS of /TestOU.
	Recipients	jedudemobsn.com ×
	Alert when a mobile device is not synchronized for a period of time Alert when a mobile device is	 5 • days, device has not been used at all in stated number of days 5
	idle for a period of time	• days, device has been idle for the stated number of days prior to its last use
		Cancel

Related Articles: Alert on Non-Synchronizing and Idle Mobile Devices



3. Setting Up User Login Alerts

Proactively monitor suspicious login activities to prevent unauthorised access and potential data leaks.

Navigate:

GAT+ > Configuration > Alert Rules

Steps:

- Click the '+' icon to create a new alert.
- Enter a rule name and enable the rule.
- Set the Alert Type to Users.
- Define the scope: Individual user, group, or organizational unit.
- Add recipients to receive real-time notifications.
- Select the login events you want to monitor:
 - Login Success
 - Logout
 - Suspicious Login
 - Login Verification
 - Login Challenge
 - Login Failure
- Save the rule.



Related Articles: Setting Up User Login Alerts in GAT+



4. Location-Based Alerts and Access Control for Chromebooks

GAT Shield supports the use of Location maps to provide alerting and/or access control for Admins.

Alert Rules A	dd alert rule - Loca	ition
+ Add a rule +	Alert rule name	Alert rule name (max. 64 characters)
Alert on .io sites except sketc	Active	
Alert when visited.	Location bounds	D Select area
Block visits to the Google Ima Credit Card #		Required GAT will generate an alert if a Shield instance is used outside of the selected location.
Dublin Zone Breach	Scope	Select or type an email Select or type an org. unit path
Executable Downloaded		O Rule recipients. If no value is specified, all domain users are affected. If any value is specified, any user who meets the criteria is affected. Start typing for suggestions. Click on a selected item or hit TAB/COMMA key to add it.
Guns Alert	Scope exclusions	Select or type an email
Homophobic Language Detec		Select or type an org. unit path
Homophobic Language Detec		D Excluded recipients, in any value is specified, any user who meets the cirteria is anected. Overheles above rule. Start typing for suggestions. Click on a selected item or hit TAB/COMMA key to add it.
New REGEX for bad languag	End user action	Display warning message
Not Allow TEST		
Visit Rule	Alert recipients	User, group or other valid email addresses that will be used for notification when alert is triggered. If no value is specified, no one will be emailed. Start typing for suggestions. Click on a selected item or hit
Visit Rule	Screen capture	TAB/COMMA key to add it.
Warsaw zone breached	Webcam capture	Do not report

Tips:

- If you don't want to alert end users outside the approved area, set the end-user action to No Action.
- You can enable webcam capture for security incidents.

Related Articles: Location-Based Alerts and Access Control for Chromebooks



5. YouTube Content Monitoring Alerts

Prevent data exposure through public video content by monitoring when users publish videos to YouTube.



GAT+ > Configuration > Alert Rules

Steps:

- Click the '+' icon to create a new alert.
- Enter a rule name and enable the rule.
- Set the Alert Type to YouTube.
- Define the scope: User, Group, or Organizational Unit.
- Select the recipients for real-time notifications.
- Enable the option Notify on new YouTube published videos.
- Save the rule.

Alert Rules		
-		at least 26
Add / edit alert rule		8
Name Name	YouTube alert on new videos	
Enabled		
Туре	Youtube	
Email alar Scope	Org. Unit ▼	
	O You can use wildcard character •, which will be interpreted as any number of characters (0 or more). Example of use: • /* - full domain (root OU and all sub OUs), · //restou* - all OUs that start with <i>/TestOU</i> , • //restou/* - all sub OUS of <i>/TestOU</i> .	
Application	edudemobsn.com ×	
access to Notify on new YouTube published videos		
Drive aler	H Save	Cancel

Use Cases:

- Monitor users publishing potentially sensitive or unauthorized content.
- Audit brand reputation risks from public video posts.
- Ensure that corporate accounts are not used for personal content sharing.



Tips:

• You can also view and audit this activity in GAT Shield under the YouTube Audit section.

Related Articles: How to Set Up an Alert on New YouTube Published Videos

DLP Best Practices for Google Admins

- Establish clear thresholds for download and sharing alerts.
- Combine **DLP scans with scheduled reports** for 2. continuous monitoring.
- Educate file owners to remediate exposure risks directly.
- Review and adjust DLP rules quarterly based 4 on emerging risks.
- Leverage Shield for endpoint-level controls and 5. download blocking.





Want To Learn More?

VISIT OUR WEBSITE

VISIT OUR RESOURCES PAGE

TRAINING SESSIONS CALENDAR

