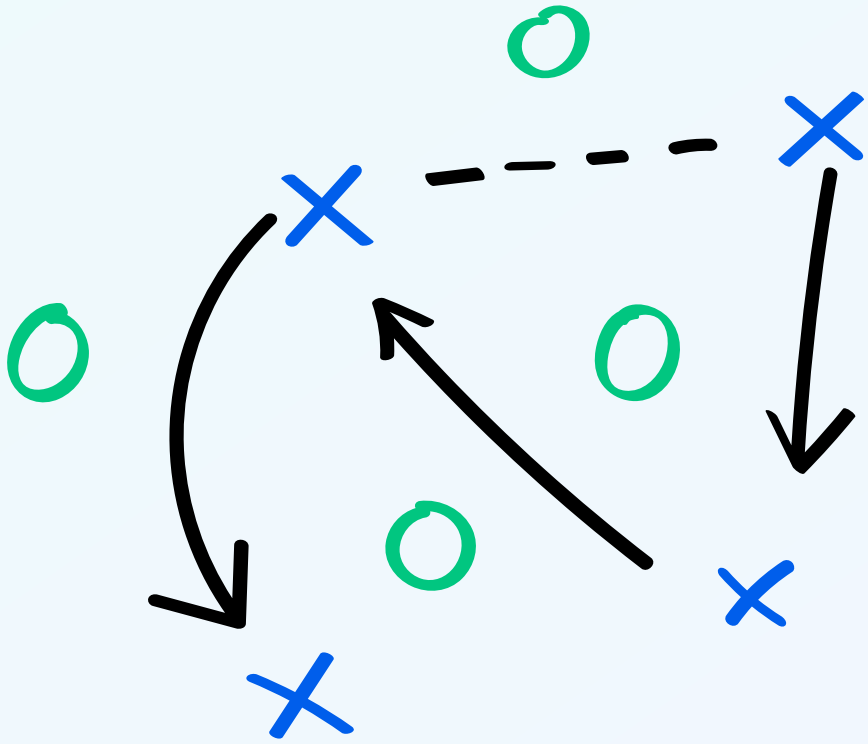
ENTERPRISE RESOURCES

Compromised Google Workspace Account Response Playbook

Who this is for: Google Workspace Admins responding to a potentially compromised user account who need to quickly contain the threat, determine what actions were taken, identify any data that may have been accessed or exposed, and restore the account to a secure state.



GAT labs

How to Use This Playbook

A compromised Google Workspace account can expose sensitive emails, files, and business data within minutes.
This playbook provides a step-by-step process to contain the threat, investigate the incident, determine what data was exposed, and strengthen security moving forward.

Use this playbook if:

- You receive an alert about suspicious login activity
- A user reports unauthorized account access
- You discover unexpected file sharing or email forwarding
- A third-party application has been granted suspicious access
- You suspect sensitive information may have been exposed

What you'll learn

This guide walks through seven key phases:

1. Contain the account immediately
2. Build the investigation timeline
3. Investigate Drive activity
4. Investigate Gmail activity
5. Determine what data was exposed
6. Check for broader domain impact
7. Remediate and strengthen security controls

At the end of this guide, you'll find an **incident response checklist** to help track your investigation and ensure no critical steps are missed.

Best Practice

Follow the phases in order. Contain the threat first, then investigate the activity and any potential data exposure. Use the findings to improve future security and monitoring.

Phase 1: Contain the Account Immediately

Your first priority is to stop the attacker from doing further damage before you investigate.

1. Force the user to sign out from all active sessions using GAT Flow

This terminates any live attacker access immediately.

KNOWLEDGE BASE ARTICLES

How to Force Sign Out Users in Google Workspace with GAT Flow

2. Reset the user's password

This blocks re-entry using compromised credentials.

KNOWLEDGE BASE ARTICLES

Change Google Workspace User Passwords in Bulk

3. Revoke all connected third-party apps

OAuth tokens can provide persistent access even after a password reset.

KNOWLEDGE BASE ARTICLES

Revoke All Apps for a Google Workspace User with GAT Flow

4. Delete app-specific passwords

These bypass 2-Step Verification and can be used as a hidden backdoor.

KNOWLEDGE BASE ARTICLES

Delete App-Specific Passwords

5. Delete 2-Step Verification backup codes

An attacker may have captured these during the compromise.

KNOWLEDGE BASE ARTICLES

Delete 2-Step Verification Backup Codes

Phase 2: Build the Investigation Timeline

Now that the account is contained, establish when the compromise began and build a timeline of attacker activity.

6. Review Login History and Activity Reports

Use login history and the Google Workspace Activity Report together to reconstruct the compromise from the initial login through to the attacker's final activity.

Look for:

- Suspicious logins
- Unusual locations or IP addresses
- Unrecognized devices
- Activity outside normal working hours
- Drive activity
- Gmail activity
- Calendar activity
- Administrative actions
- Third-party app authorizations

KNOWLEDGE BASE ARTICLES

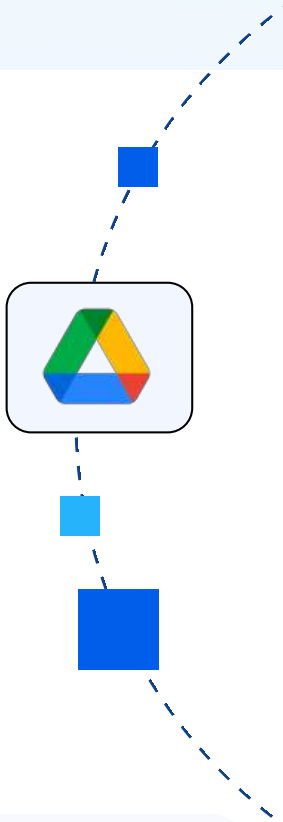
Investigate Google Workspace Account Compromise with GAT+

Use this information to identify:

- The first suspicious login
- The duration of attacker access
- Key actions performed during the compromise
- Other users, files, or systems that may have been affected

Phase 3: Investigate What Was Accessed in Drive

Google Drive is often one of the primary targets during an account compromise.



7. Review all Drive activity

View all actions performed by the compromised account, including:

- Files viewed
- Files edited
- Files downloaded
- Files shared
- Files deleted

KNOWLEDGE BASE ARTICLES

View Any Action Taken in Google Drive by a Specific User

8. Review external sharing activity

Determine if files were shared outside the organization during the compromise period.

KNOWLEDGE BASE ARTICLES

Find and Take Actions on Externally Shared Files with GAT+

Domain Security Monitoring with GAT+ Activity Report

9. Identify files published to the web

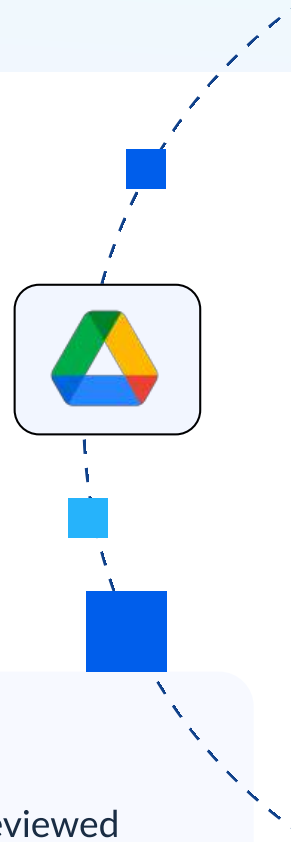
The perpetrator may make files publicly accessible without creating external shares.

KNOWLEDGE BASE ARTICLES

View All Files Published to Web in Google Drive with GAT+

Phase 3: Investigate What Was Accessed in Drive

Google Drive is often one of the primary targets during an account compromise.



10. Review deleted files

Determine if data was intentionally removed or destroyed.

KNOWLEDGE BASE ARTICLES

Scheduled Report for Deleted Files Across Google Drive

How to Find Who Deleted a File in Google Drive

11. Review Shared Drive activity

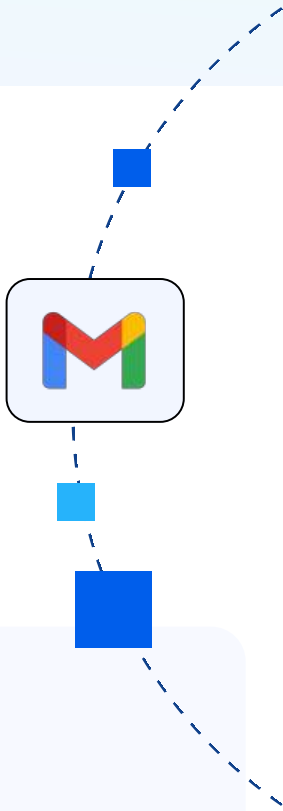
Shared Drives often contain broader organizational data and should be reviewed separately.

Look for:

- Files accessed
- Files downloaded
- Permission changes
- Membership changes

Phase 4: Investigate What Was Accessed in Gmail

Review Gmail activity to determine whether messages were accessed, forwarded, deleted, or used to establish ongoing access.



12. Audit emails sent and received

Review email activity during the compromise window.

KNOWLEDGE BASE ARTICLES

How to Audit Email in Google Workspace

Find Emails Sent and Received by the User with GAT+

13. Check for email forwarding rules

Attackers commonly create forwarding rules to maintain visibility after access is removed.

KNOWLEDGE BASE ARTICLES

How to Set Up and Manage Email Auto-Forwarding in GAT+

14. Check for suspicious email filters

Look for filters that:

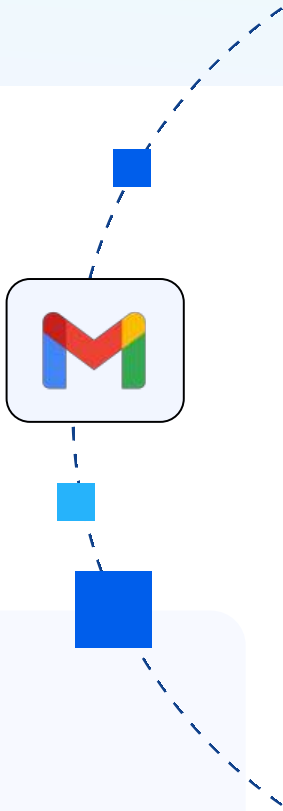
- Hide responses
- Mark emails as read
- Delete incoming messages
- Redirect security notifications

KNOWLEDGE BASE ARTICLES

Remove User Email Filters for Several Users in Bulk via GAT Flow

Phase 4: Investigate What Was Accessed in Gmail

Review Gmail activity to determine whether messages were accessed, forwarded, deleted, or used to establish ongoing access.



15. Check for mailbox delegation

Determine if access was granted to another account.

KNOWLEDGE BASE ARTICLES

Alert for Email Delegation from Google Users

16. Review deleted emails

Attackers often delete evidence, warning notifications, or user responses. Review deleted messages and unusual mailbox activity where possible.

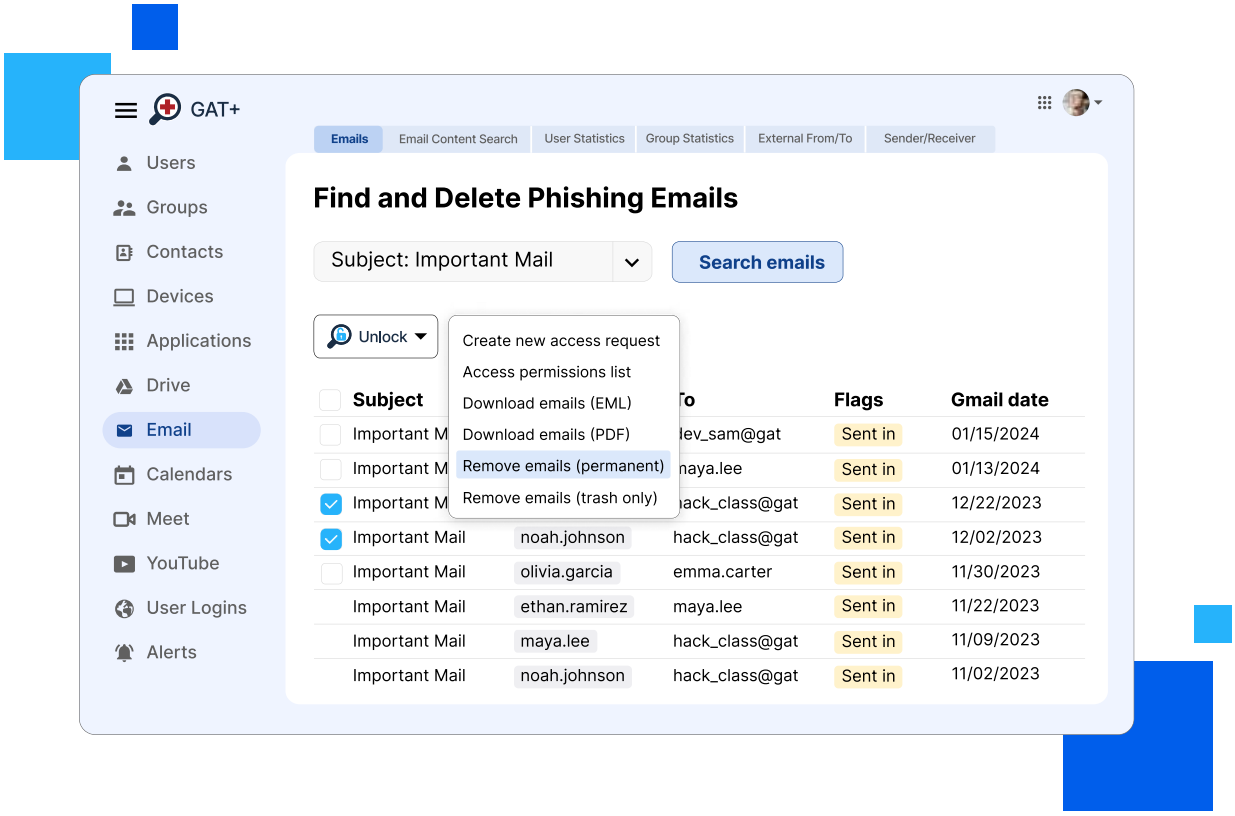
Phase 5: Determine What Data Was Exposed

Once you've identified the perpetrator's activity, assess the impact of the compromise and determine whether sensitive information may have been exposed.

Questions to answer:

- What information was accessed?
- What information left the organization?
- Were sensitive files downloaded or uploaded to external services?
- Were emails containing sensitive information exposed?
- Were customer, employee, HR, legal, or financial records involved?
- Does the incident require internal reporting or compliance notification?

At this stage, document your findings and identify the systems, users, and data affected by the compromise.



Phase 6: Check for Broader Domain Impact

Determine whether the perpetrator gained access to other systems, applications, devices, or administrative functions.

17. Audit authorized third-party applications

Determine if malicious or unauthorized applications were granted access.

KNOWLEDGE BASE ARTICLES

Audit and Manage Third-Party Applications in Google Workspace

18. Review administrative activity

If the account had elevated privileges, review all administrative actions performed during the compromise period.

KNOWLEDGE BASE ARTICLES

How to Access the Record of Administrative Actions with GAT+ Admin Log

19. Review device access

Look for unknown or suspicious devices that were used to access the account.

KNOWLEDGE BASE ARTICLES

Audit All the Devices Used in Your Domain with GAT+

20. Check for persistence mechanisms

Review:

- OAuth applications
- App-specific passwords
- Backup codes
- Mail forwarding rules
- Email filters
- Mailbox delegation

Confirm all persistence methods have been removed.

Phase 7: Remediate and Harden

Remove unauthorized access, reverse malicious changes, and implement monitoring to help prevent future incidents.

21. Remove unauthorized external sharing

Remove any unauthorized external shares created during the compromise to prevent ongoing access to sensitive information.
Use bulk actions to remove external permissions from affected files.

KNOWLEDGE BASE ARTICLES

Find and Take Actions on Externally Shared Files with GAT+

22. Remove unauthorized external collaborators

Remove access granted to external users who should not have access.

KNOWLEDGE BASE ARTICLES

How to Globally Remove External Collaborator Access in Google Drive with GAT+

23. Configure ongoing security monitoring

Set up alerts to detect future incidents earlier.
Recommended alerts include:

- Login anomalies
- New email forwarding and delegation rules
- New email filters
- Unusual file sharing activity
- Third-party app authorizations
- 2FA changes

KNOWLEDGE BASE ARTICLES

How to Set Up User Security Alerts with GAT+
Alert When 2FA is Disabled for Any User in Your Google Domain
Set Up a Google Alert When a New Filter is Added in Gmail
Remove External Sharing on Files with Sensitive Information

Lessons Learned and Prevention

Once the investigation is complete, review how the compromise occurred and identify improvements that can reduce the likelihood of a future incident.

Questions to consider:

- Was MFA enabled and enforced?
- Did a third-party application contribute to the compromise?
- Were alerts configured before the incident?
- Were users following least-privilege principles?
- Could earlier monitoring have detected the incident sooner?
- What changes should be made to prevent a similar incident from happening again?

Documenting these findings helps strengthen your overall Google Workspace security posture.

Prevent Future Compromises

Most account compromises leave warning signs before significant damage occurs.

Consider implementing ongoing monitoring for:

- Login anomalies
- New email forwarding rules
- Email delegation changes
- Third-party app authorizations
- External file sharing
- 2FA changes
- File uploads to external services

The goal is not just to respond faster. It is to detect suspicious activity before sensitive data is exposed.

Compromised Account Investigation Checklist

Phase 1: Contain the Account

- [ ] Force sign out the user from all active sessions
- [ ] Reset the user's password
- [ ] Revoke all connected third-party apps
- [ ] Delete app-specific passwords
- [ ] Delete 2-Step Verification backup codes

Phase 2: Build the Investigation Timeline

- [ ] Review login history for unusual locations, IPs, devices, or times
- [ ] Review the Activity Report
- [ ] Identify the first suspicious login
- [ ] Determine the duration of attacker access
- [ ] Identify key actions performed during the compromise

Phase 3: Investigate Drive Access

- [ ] Review Drive activity
- [ ] Check for files shared externally
- [ ] Check for files published to the web
- [ ] Check for deleted files
- [ ] Review Shared Drive activity

Compromised Account Investigation Checklist

Phase 4: Investigate Gmail Activity

- [ ] Audit emails sent and received
- [ ] Check for email forwarding rules
- [ ] Check for suspicious email filters
- [ ] Check for mailbox delegation
- [ ] Review deleted emails

Phase 5: Determine What Data Was Exposed

- [ ] Review downloaded files
- [ ] Review sensitive files accessed
- [ ] Review file upload activity
- [ ] Review external sharing activity
- [ ] Review Shared Drive activity
- [ ] Review sensitive email activity
- [ ] Determine whether compliance reporting is required

Note: Review file upload activity during the compromise window. Attackers may upload sensitive documents to external websites, third-party applications, AI platforms, personal cloud storage accounts, or file-sharing services. Understanding what was uploaded can be just as important as understanding what was downloaded or shared externally.

Compromised Account Investigation Checklist

Phase 6: Check for Broader Domain Impact

- [ ] Audit authorized third-party apps
- [ ] Review admin activity
- [ ] Review device access
- [ ] Check for persistence mechanisms

Phase 7: Remediate and Harden

- [ ] Remove unauthorized external sharing
- [ ] Remove unauthorized collaborators
- [ ] Configure login anomaly alerts
- [ ] Configure 2FA alerts
- [ ] Configure email forwarding and email delegation alerts
- [ ] Configure email filter alerts

Investigation Notes

Compromise date/time confirmed:

Accounts affected:

Files exposed:

Investigated by:

Date completed:

Want To Learn More?

VISIT OUR WEBSITE

VISIT OUR RESOURCES PAGE

TRAINING SESSIONS CALENDAR