INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-22 13:51 UTC

Google API Keys Remain Functional ~23 Minutes After Deletion, Breaking Revocation as IR Containment Control

SECURITY ANALYSIS | MEDIUM | CVSS 5.0

SCC Item ID	SCC-STY-2026-0152
Type	Security Analysis
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	Google Cloud, API Key Management (all API key types; no specific version boundary identified)
Published	2026-05-21T16:07:47
Discovery Source	Rss

Executive Summary

Google Cloud API keys remain functional for approximately 23 minutes after deletion, directly contradicting Google's documented practice of immediate revocation. This gap eliminates key deletion as a reliable containment action during incident response, an attacker holding a compromised key retains live access through the entire post-deletion window. The finding signals a broader risk: when cloud provider SLAs around credential revocation cannot be trusted, incident response playbooks built on those guarantees require revision to account for the documented delay.

Technical Analysis

Aikido Security researchers discovered that deleted Google Cloud API keys continue to authenticate successfully for roughly 23 minutes post-deletion across all API key types, with no specific version boundary identified. The behavior maps to CWE-672 (Operation on a Resource After Expiration or Release) and CWE-613 (Insufficient Session Expiration), suggesting the underlying cause is a cache-propagation delay in Google's key validation infrastructure, revocation state is not immediately reflected across all validation nodes.

The IR consequence is direct. Key deletion is a standard containment step in credential-compromise playbooks. MITRE ATT&CK techniques T1078.004 (Cloud Accounts), T1550.001 (Application Access Token), T1528 (Steal Application Access Token), and T1552.001 (Credentials in Files) all describe adversary paths that land an attacker in possession of a valid API key. The 23-minute window means that at the moment a defender executes what they believe is containment, the attacker retains a functional credential.

No exploitation by a threat actor has been reported, and no CVE has been assigned. The CVSS base score of 5.0 reflects the precondition: exploitation requires a key already compromised before deletion is initiated. However, that framing understates operational risk. In active incidents, defenders frequently don't know when a key was first accessed, meaning the window is exploitable precisely when it matters most.

Google Maps Platform security guidance recommends restricting API key permissions by scope and HTTP referrer as a baseline control, but this guidance predates the revocation finding and does not address the post-deletion window. No official Google acknowledgment or remediation timeline has been published as of this writing.

Action Checklist

1. Step 1: Assess exposure, audit your organization's Google Cloud API key inventory. Identify every key in use, its associated service account, and the applications or pipelines that depend on it. CIS 1.1 (Enterprise Asset Inventory) applies here: keys are assets and must be tracked.
2. Step 2: Revise your IR playbooks immediately, remove key deletion as a standalone containment step for Google Cloud API keys. Document the ~23-minute post-revocation window explicitly. Treat key deletion as a deferred control, not an immediate one. Reference NIST SP 800-61 Section 3 (Containment) and your containment phase documentation.
3. Step 3: Layer compensating controls during incident response, before or concurrent with deletion, (a) restrict the compromised key's API scope to the minimum possible permissions (NIST AC-6, Least Privilege; CIS 5.4), (b) rotate all secrets and downstream credentials that the key had access to (D3-CRO, Credential Rotation), and (c) revoke any OAuth tokens or service account bindings associated with the compromised identity.
4. Step 4: Enforce pre-issuance key restrictions as baseline policy, apply HTTP referrer restrictions, IP restrictions, and API scope restrictions to all Google Cloud API keys at creation time, per Google Maps Platform security guidance. This limits blast radius if a key is compromised and limits what an attacker can do during any revocation window. Maps to NIST AC-3 (Access Enforcement) and D3-UAP (User Account Permissions).
5. Step 5: Instrument the revocation window, configure logging (NIST AU-2, AU-12; CIS 8.2) to capture API key usage events. During an active incident, monitor for API calls using a key after deletion is initiated. Flag any authenticated request from a deleted key as a high-priority alert. This turns the window into a detection opportunity.
6. Step 6: Update your threat model, add 'post-revocation exploitation window' as an explicit threat scenario in your cloud IR runbooks. Assign a risk register entry. Brief cloud security engineering and IR teams on the finding. This is not a theoretical risk; it is a documented behavioral gap in a widely used platform.
7. Step 7: Monitor for Google's response, track the Aikido Security blog and Google Cloud release notes for any official acknowledgment, architectural fix, or revised SLA language. Assign ownership for tracking this disclosure. Do not stand down compensating controls until a verified fix with tested behavior is confirmed.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to CISO and legal/compliance if Google Cloud Audit Logs confirm API calls on a deleted key during an active incident (evidence of post-revocation exploitation), if the compromised key had access to storage buckets, databases, or services containing PII or PHI triggering breach notification obligations under GDPR, HIPAA, or state privacy laws, or if IR team lacks the GCP permissions required to execute scope restriction and rotation within the ~23-minute containment window.
Recovery Notes	After all compromised API keys are deleted and downstream credentials rotated, verify recovery by running 'gcloud services api-keys list' to confirm no residual keys exist for the affected service accounts, and auditing IAM policy bindings with 'gcloud projects get-iam-policy PROJECT_ID' to ensure no attacker-created service account keys or bindings persist. Monitor Google Cloud Data Access Audit Logs for the affected APIs and service accounts for a minimum of 30 days post-containment, specifically for any authenticated requests originating from source IPs or user agents observed during the compromise window. Do not remove compensating controls (scope restrictions on surviving keys, enhanced logging) until Google officially confirms and you have empirically validated that the ~23-minute revocation delay has been resolved.
Forensic Artifacts	Google Cloud Admin Activity Audit Logs — 'google.apikeys.v2.ApiKeys/DeleteKey' events: timestamp of deletion request is the forensic baseline for measuring the post-revocation exploitation window; preserve with 'gcloud logging read' and store to immutable Cloud Storage bucket with Object Hold. | Google Cloud Data Access Audit Logs — API calls bearing the compromised key string timestamped after the DeleteKey event: any entry within ~23 minutes of deletion is direct evidence of post-revocation exploitation; cross-reference protoPayload.authenticationInfo.callerIp against known legitimate source ranges. | Google Cloud Admin Activity Audit Logs — 'CreateKey' and 'UpdateKey' events for the compromised key: establishes when the key was created, whether restrictions were ever applied, and whether the key was modified (scope expanded) by an attacker prior to detection. | VPC Flow Logs or Cloud Armor WAF access logs — source IP and request volume to Google API endpoints during the compromise window: identifies whether the attacker used the key from a consistent C2 IP or rotated infrastructure, and confirms which downstream Google services were actually called during the post-deletion window. | Google Cloud IAM audit logs — 'google.iam.admin.v1.CreateServiceAccountKey' and 'SetIamPolicy' events associated with the compromised service account: determines whether an attacker used the API key's access to create persistent backdoor credentials (service account keys or IAM bindings) that would survive the original key's deletion and require separate remediation.

Per-Action IR Details

Step 1: Assess exposure — audit your organization's Google Cloud API key inventory. Identify every key in use, its associated service account, and the applications or pipelines that depend on it. CIS 1.1 (Enterprise Asset Inventory) applies here: keys are assets and must be tracked.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establish IR capability and asset visibility before incidents occur

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 5.1 (Establish and Maintain an Inventory of Accounts), NIST AC-2 (Account Management), NIST RA-2 (Security Categorization)

Compensating: Run 'gcloud services api-keys list --project=PROJECT_ID --format=json' across all projects via a bash loop using the gcloud CLI (free, no SIEM required). Pipe output to jq to extract keyString, createTime, restrictions, and any associated serviceAccount fields. Store results in a versioned CSV. For multi-project orgs, use 'gcloud projects list' to enumerate projects first, then iterate. Two-person team: one runs enumeration, one validates against application

dependency documentation.

Evidence: Before auditing, capture a point-in-time snapshot of Google Cloud Audit Logs (Admin Activity log) for the 'google.apikeys.v2.ApiKeys' service — specifically 'CreateKey', 'UpdateKey', and 'ListKeys' method calls — to establish a baseline of key creation history and any recent modifications that may indicate attacker activity prior to discovery. Export via 'gcloud logging read' with filter 'protoPayload.serviceName=apikeys.googleapis.com' covering at minimum the last 90 days.

Step 2: Revise your IR playbooks immediately — remove key deletion as a standalone containment step for Google Cloud API keys. Document the ~23-minute post-revocation window explicitly. Treat key deletion as a deferred control, not an immediate one. Reference NIST IR-4 (Incident Handling) and your containment phase documentation.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Maintain IR playbooks and update them based on new threat intelligence about platform behavioral gaps

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST PM-9 (Risk Management Strategy), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Add a literal callout block to your existing Google Cloud IR runbook (Confluence, wiki, or even a shared Google Doc): 'WARNING: Google Cloud API key deletion does NOT provide immediate revocation. Keys remain live for approximately 23 minutes post-deletion per Aikido Security research (2025). Do NOT treat deletion as a containment action. Proceed immediately to scope restriction and downstream credential rotation.' Tag the playbook update with the discovery date so auditors can verify the revision timeline.

Evidence: Document the specific Aikido Security research finding as a named reference in the playbook revision — include the approximate 23-minute window, the affected platform (Google Cloud API Key Management, all key types), and the date of discovery. This creates an auditable record that the organization was aware of the behavioral gap and updated controls accordingly, which matters for post-incident regulatory review under frameworks requiring documented IR plan maintenance.

Step 3: Layer compensating controls during incident response — before or concurrent with deletion, (a) restrict the compromised key's API scope to the minimum possible permissions (NIST AC-6, Least Privilege; CIS 5.4), (b) rotate all secrets and downstream credentials that the key had access to (D3-CRO, Credential Rotation), and (c) revoke any OAuth tokens or service account bindings associated with the compromised identity.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Choose containment strategy based on ability to keep attacker unaware while limiting damage

Controls: NIST AC-6 (Least Privilege), NIST AC-3 (Access Enforcement), NIST IR-4 (Incident Handling), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Execute scope restriction immediately via gcloud CLI: 'gcloud services api-keys update KEY_ID --project=PROJECT_ID --api-target=service=SAFE_API_ONLY' to narrow the key to a single harmless API target while deletion propagates. Simultaneously run 'gcloud iam service-accounts keys list --iam-account=SA_EMAIL' to enumerate all service account keys attached to the compromised identity and revoke each with 'gcloud iam service-accounts keys delete KEY_ID --iam-account=SA_EMAIL'. For OAuth tokens, use 'gcloud auth revoke' for any associated user credentials. These are all free gcloud SDK operations requiring no SIEM.

Evidence: Before executing scope restriction or rotation, capture Google Cloud Audit Logs for the compromised key's recent API call history: run 'gcloud logging read protoPayload.authenticationInfo.principalEmail=SERVICE_ACCOUNT_EMAIL' covering the 72 hours prior to detection. Document exactly which Google APIs were called, from which source IPs, and at what timestamps — this establishes the attacker's operational scope during the pre-detection window and informs what downstream systems and data may have been accessed during the ~23-minute post-deletion window.

Step 4: Enforce pre-issuance key restrictions as standing policy — apply HTTP referrer restrictions, IP restrictions, and API scope restrictions to all Google Cloud API keys at creation time, per Google Maps Platform security guidance. This limits blast radius if a key is compromised and limits what an attacker can do during any revocation window. Maps to NIST AC-3 (Access Enforcement) and D3-UAP (User Account Permissions).

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Implement preventive controls that reduce incident impact and limit attacker capability during response windows

Controls: NIST AC-3 (Access Enforcement), NIST AC-4 (Information Flow Enforcement), NIST AC-6 (Least Privilege), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Audit existing key restrictions using: 'gcloud services api-keys list --project=PROJECT_ID --format=json | jq ".[] | select(.restrictions == null or .restrictions == {})"' — any key returning results has no restrictions and is fully unrestricted. For each, apply IP restriction via 'gcloud services api-keys update KEY_ID --allowed-ips=CIDR_RANGE' or referrer restriction via '--allowed-referrers=DOMAIN'. Codify this as a gcloud org-policy or document it as a mandatory step in your key issuance SOP so future keys are born restricted. No cost beyond gcloud SDK.

Evidence: For a key compromised without pre-issuance restrictions, capture VPC Flow Logs (if API calls traversed GCP infrastructure) or Cloud Armor request logs (if a WAF was in path) to identify source IPs that called the unrestricted key. Compare these IPs against known application source ranges — any IP outside expected ranges during the post-deletion window (up to ~23 minutes after deletion initiation) represents confirmed attacker exploitation of the revocation gap. Export with 'gcloud logging read resource.type=gce_network'.

Step 5: Instrument the revocation window — configure logging (NIST AU-2, AU-12; CIS 8.2) to capture API key usage events. During an active incident, monitor for API calls using a key after deletion is initiated. Flag any authenticated request from a deleted key as a high-priority alert. This turns the window into a detection opportunity.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Monitor systems and correlate events to identify malicious activity; use the revocation window as an active detection opportunity

Controls: NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Enable Google Cloud Audit Logs for the 'apikeys.googleapis.com' service under 'Data Access' log types in IAM & Admin > Audit Logs — this is free within Cloud Logging. During an active incident, run a polling loop every 60 seconds: 'gcloud logging read "protoPayload.serviceName=apikeys.googleapis.com AND protoPayload.request.keyString=COMPROMISED_KEY_VALUE" --freshness=2m --format=json' to detect any API call using the deleted key string during the ~23-minute window. Record timestamps of any hits — these confirm active attacker exploitation of the revocation gap and constitute high-confidence evidence of post-deletion API abuse. Two-person team: one monitors the polling loop, one begins downstream impact assessment.

Evidence: The primary artifact for this step is Google Cloud Data Access Audit Logs scoped to the compromised key's API calls timestamped after the deletion event was initiated. Cross-reference the 'DeleteKey' Admin Activity log entry timestamp (which records the moment deletion was requested) against any subsequent Data Access log entries bearing the same key identifier — any such entries falling within the ~23-minute window are direct forensic evidence of the revocation gap being exploited. Preserve these log entries to immutable storage (Cloud Storage bucket with Object Hold enabled) immediately.

Step 6: Update your threat model — add 'post-revocation exploitation window' as an explicit threat scenario in your cloud IR runbooks. Assign a risk register entry. Brief cloud security engineering and IR teams on the finding. This is not a theoretical risk; it is a documented behavioral gap in a widely used platform.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Use lessons learned to update policies, improve detection, and share intelligence about newly identified threat vectors

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST PM-9 (Risk Management Strategy), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Create a named risk register entry (spreadsheet or GRC tool) titled 'Google Cloud API Key Post-Revocation Exploitation Window (~23 min)' with fields: affected platform, discovery source (Aikido Security research), inherent risk rating (Medium, CVSS 5.0), compensating controls applied, residual risk rating, and control owner. Schedule a mandatory 30-minute brief for cloud security and IR teams using the Aikido Security research as the primary source document. No specialized tooling required — this is a process and documentation action.

Evidence: Before closing this action, document whether any prior IR incidents involving Google Cloud API key compromise were handled using key deletion as a primary containment step — if so, those incidents must be retroactively reviewed to assess whether the ~23-minute window was exploited and whether post-deletion API activity was ever logged or detected. This retroactive review is itself a forensic action: query historical Cloud Audit Logs for 'DeleteKey' events followed within 23 minutes by Data Access events on the same key, covering the maximum log retention window available.

Step 7: Monitor for Google's response — track the Aikido Security blog and Google Cloud release notes for any official acknowledgment, architectural fix, or revised SLA language. Assign ownership for tracking this disclosure. Do not stand down compensating controls until a verified fix with tested behavior is confirmed.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Integrate threat intelligence updates into ongoing IR posture; maintain compensating controls until vendor remediation is verified

Controls: NIST SI-2 (Flaw Remediation), NIST RA-5 (Vulnerability Monitoring and Scanning), NIST IR-8 (Incident Response Plan), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Assign a named individual as control owner for tracking this disclosure. Set a recurring calendar reminder (monthly minimum) to check Google Cloud release notes at 'cloud.google.com/release-notes' filtered for 'API Keys' and 'IAM', and the Aikido Security blog for follow-up reporting. When Google publishes an acknowledgment or fix, operationally validate revocation speed before retiring compensating controls: delete a non-production test key and immediately poll for successful API calls at 1-minute intervals for 30 minutes to empirically confirm whether the window has closed. Do not rely solely on vendor documentation — test behavior directly.

Evidence: Maintain a dated log of monitoring actions taken — each check of Google's release notes and Aikido's blog, with a timestamp and finding (no update / partial update / fix confirmed). This log serves as evidence of due diligence if the revocation gap is later implicated in an incident during the period compensating controls were in place. It also satisfies audit requirements under NIST SI-2 (Flaw Remediation) for tracking known vendor behavioral gaps to resolution.

Detection Guidance

Primary detection surface is API audit logging in Google Cloud. Enable and review Cloud Audit Logs, specifically Data Access logs, for API key authentication events. After initiating deletion of a compromised key, query logs for any authenticated requests that reference the deleted key's identifier during the 23-minute post-deletion window. Any successful API call from a deleted key after the deletion timestamp is an anomaly that warrants immediate escalation.

Behavioral patterns to hunt: (1) API key usage from unexpected IP ranges or geographic locations (T1078.004), especially immediately preceding or following deletion; (2) high-frequency API calls in a short window that may indicate an attacker exfiltrating data before access is cut (T1528); (3) API key usage from automated pipelines at unusual hours, which may indicate a compromised CI/CD credential (T1552.001).

Log sources to check: Google Cloud Audit Logs (Admin Activity and Data Access), Cloud Monitoring alert policies scoped to API key operations, and any SIEM ingesting GCP logs via Pub/Sub or the Security Command Center integration.

Policy gap to audit: verify that all API keys in production have explicit IP restrictions and API scope restrictions applied. Keys without restrictions present a materially larger risk during any revocation window. Map this audit against CIS 8.2 (Collect Audit Logs) and NIST AU-6 (Audit Record Review, Analysis, and Reporting) compliance requirements.

D3FEND countermeasures applicable: D3-LAM (Local Account Monitoring) adapted to cloud API key monitoring; D3-CRO (Credential Rotation) as a detection-adjacent control that narrows the attacker's window; D3-UAP (User Account Permissions) to reduce what a compromised key can observe or exfiltrate during the window.

Framework Mappings

MITRE-ATTACK

- **T1078.004** — Cloud Accounts
- **T1550.001** — Application Access Token
- **T1190** — Exploit Public-Facing Application
- **T1552.001** — Credentials In Files
- **T1078** — Valid Accounts
- **T1528** — Steal Application Access Token

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-4** — System Monitoring

CIS-V8

- **8.2** — Collect Audit Logs

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078.004	Cloud Accounts	Defense-Evasion
T1550.001	Application Access Token	Defense-Evasion
T1190	Exploit Public-Facing Application	Initial-Access
T1552.001	Credentials In Files	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1528	Steal Application Access Token	Credential-Access

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/identity-access-management-security/goo...	T3
Manage API keys | Authentication - Google Cloud Documentation	https://docs.cloud.google.com/docs/authentication/api-keys	T3
How Google's Insecure-by-Default API Keys and a 30-Hour ... - Reddit	https://www.reddit.com/r/googlecloud/comments/1s7v5x9/how_googles_i...	T3
Google API keys keep working after you delete them - Aikido Security	https://www.aikido.dev/blog/google-api-keys-deletion	T3
Google Maps Platform security guidance	https://developers.google.com/maps/api-security-best-practices	T3

Generated 2026-05-22 13:51 UTC by TJS Security Command Center