INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-22 19:02 UTC

Cloud Security Is Failing at Scale: Survey Data Exposes a Detection and Response Crisis Across 94% of Organizations

SECURITY ANALYSIS | HIGH | CVSS 7.5

SCC Item ID	SCC-STY-2026-0249
Type	Security Analysis
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Cloud environments broadly (multi-cloud and hybrid); enterprises using cloud control plane services across major providers
Discovery Source	Rss:T1 Threatintel

Executive Summary

A CrowdStrike-commissioned survey of enterprise security teams finds that 94% of organizations surveyed have suffered cloud intrusions leading to data exposure or exfiltration, pointing to systemic gaps in identity visibility, alert management, and tool integration rather than any single novel attack. The findings diagnose three structural gaps: blind spots in cloud control plane activity, alert fatigue burying high-fidelity detections, and fragmented tooling that prevents coordinated response, as the primary drivers of breach frequency at scale. For CISOs and boards, the data signals that cloud detection and response programs are broadly immature, and that incremental investment in perimeter controls will not close gaps rooted in identity architecture and operational workflow.

Technical Analysis

The survey data, commissioned by CrowdStrike and drawing on responses from enterprise security teams, frames the cloud intrusion problem as three compounding structural failures rather than a wave of sophisticated novel attacks. The underlying CWEs, CWE-284 (improper access control), CWE-287 (improper authentication), and CWE-778 (insufficient logging), are architectural debt problems, not zero-days. Attackers are exploiting them through well-documented TTPs mapped to the MITRE ATT&CK framework: cloud service discovery (T1580), cloud storage object discovery (T1619), data from cloud storage (T1530), transfer data to cloud account (T1537), valid account abuse including cloud accounts (T1078, T1078.004), and credentials from cloud instance metadata (T1552.005). Account discovery techniques (T1087, T1087.004) and impair defenses (T1562) round out the pattern, describing adversaries who establish footholds via identity weaknesses,

enumerate the environment quietly, then exfiltrate before detection fires. The first structural gap is cloud control plane invisibility. Identity and API-layer activity, service account misuse, role assumption chains, OAuth token abuse, generates the telemetry that would catch these intrusions early, but most organizations lack the instrumentation or correlation logic to surface meaningful signals from it. Attackers operating in the control plane can persist for extended periods without triggering conventional endpoint or network detections. The second gap is alert overload. High-fidelity detections exist in many environments but are deprioritized or delayed because analysts are processing volume rather than context. The survey positions this as an operational problem with a tooling dimension: without application context attached to runtime detections, analysts cannot rapidly distinguish a routine automated process from adversary lateral movement. The third gap is tool fragmentation. Organizations running separate cloud security posture management, workload protection, and CSPM tools without unified data planes face coordination failures during incident response, handoffs break, context is lost, and dwell time extends. The survey introduces CrowdStrike Falcon Cloud Security's CNAPP capabilities, specifically adversary-informed risk prioritization and application context in runtime detections, as a response architecture. Security teams should treat this data as a CDR program maturity benchmark: the gaps described are real and corroborated by the MITRE technique profile, even if the 94% figure carries the methodological limitations inherent to vendor-commissioned research. Independent corroboration of that specific statistic is not available in the provided source material.

Action Checklist

1. Step 1: Assess exposure, audit your cloud environments (multi-cloud and hybrid) for logging gaps in control plane activity; confirm that IAM, API gateway, and service account events are ingested into your SIEM or CDR platform and correlated against a baseline (NIST AU-2, CIS 8.2)
2. Step 2: Review controls, verify MFA enforcement for all cloud administrative and service accounts (NIST AC-7, CIS 6.3, CIS 6.4, CIS 6.5); audit role and permission assignments against least-privilege principles (NIST AC-6, CIS 5.4); confirm that dormant or over-privileged cloud accounts are identified and remediated (CIS 5.3)
3. Step 3: Update threat model, incorporate the MITRE ATT&CK techniques documented in this survey (T1078.004, T1552.005, T1537, T1580, T1619, T1562) into your cloud threat register; map current detection coverage against each technique and document gaps explicitly
4. Step 4: Evaluate CDR tooling maturity, assess whether your current cloud security tooling provides unified visibility across control plane, workload, and data layers; identify whether alert triage workflows are context-enriched or volume-dependent; document fragmentation points where incident response handoffs currently break
5. Step 5: Communicate findings, brief security leadership and cloud architecture owners on the specific gaps surfaced by this diagnostic framework; quantify alert-to-investigation latency in your environment and present it as a dwell-time proxy metric for board-level risk communication
6. Step 6: Monitor developments, track follow-on research or regulatory guidance from CISA on cloud security baseline requirements; if CrowdStrike publishes a full CDR survey report with additional methodology and breakdown data, review it for additional context on the 94% figure and sample composition

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to incident response immediately if any of the following are confirmed during the Step 1 audit: active CloudTrail or equivalent logging gaps coinciding with anomalous IAM role assumption events, evidence of service account key access from unexpected geographies or ASNs, S3 or cloud storage access patterns consistent with bulk enumeration (T1619) or exfiltration (T1537), or any indication that cloud management console MFA was bypassed; additionally, if the organization is subject to HIPAA, PCI-DSS, or state breach notification laws and cloud storage containing PII or PHI was accessible during any confirmed logging gap period, initiate breach notification assessment immediately.
Recovery Notes	Following any confirmed cloud control plane intrusion surfaced by this diagnostic, recovery must include full rotation of all service account keys and OAuth tokens that were active during the identified exposure window, not just those directly implicated, because the survey findings indicate broad identity visibility failures that make scope determination unreliable without complete key rotation. Re-enable and verify all disabled logging sources before returning workloads to production, and conduct a 30-day enhanced monitoring period using cloud-native anomaly detection (AWS GuardDuty, Azure Defender for Cloud, or GCP Security Command Center free tiers) with daily alert review to detect any persistence mechanisms established during the intrusion window. Validate that all IAM roles and service account permission boundaries reflect least-privilege state post-remediation before attestation to leadership.
Forensic Artifacts	AWS CloudTrail management event logs filtered for AssumeRole, CreateAccessKey, AttachRolePolicy, and PutBucketPolicy API calls during the exposure window — these are the primary control plane actions associated with T1078.004 (Valid Cloud Accounts) and T1580 (Cloud Infrastructure Discovery) as documented in the survey | Cloud instance metadata service (IMDS) access logs or proxy logs showing requests to http://169.254.169.254/latest/meta-data/iam/security-credentials/ (AWS) or the equivalent Azure IMDS endpoint — evidence of T1552.005 (Unsecured Credentials in Cloud Instance Metadata) credential harvesting that precedes lateral movement | Cloud storage access logs (AWS S3 Server Access Logs or CloudTrail S3 data events, Azure Blob Storage diagnostic logs, GCP Cloud Storage audit logs) showing bulk GetObject, ListBucket, or CopyObject operations to external destinations — direct evidence of T1619 (Cloud Storage Object Discovery) and T1537 (Transfer Data to Cloud Account) exfiltration activity | Cloud provider audit logs for GuardDuty disablement, CloudTrail trail deletion or update, Azure Defender suppression rules, or GCP Log Sink modification events — evidence of T1562 (Impair Defenses) actions used to blind defenders prior to or during exfiltration, which the survey identifies as a key enabler of the detection crisis | Identity provider (IdP) authentication logs (Okta system log, Azure Entra ID sign-in logs, AWS IAM Identity Center access logs) showing federated authentication events, MFA bypass attempts, or impossible travel indicators tied to cloud admin accounts during the exposure window — these logs establish the initial access timeline and are frequently absent from CDR tooling due to the fragmentation gap the survey diagnoses

Per-Action IR Details

Step 1: Assess exposure — audit your cloud environments (multi-cloud and hybrid) for logging gaps in control plane activity; confirm that IAM, API gateway, and service account events are ingested into your SIEM or CDR platform and correlated against a baseline (NIST AU-2, CIS 8.2)

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing logging infrastructure and detection baselines before an incident occurs

Controls: NIST AU-2 (Event Logging), NIST AU-3 (Content Of Audit Records), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: For teams without a commercial SIEM, deploy osquery with the aws_cloudtrail_events and gcp_audit_logs tables (where cloud agent support exists) or configure native free-tier logging: enable AWS CloudTrail with S3 delivery and use AWS Athena (free query tier) to run ad-hoc SQL against CloudTrail JSON logs; on Azure, enable Diagnostic Settings for Entra ID sign-in and audit logs and export to a Log Analytics workspace free tier. Use the open-source Matano or Panther Community Edition as a lightweight log pipeline alternative. A two-person team can baseline IAM event volume in 4–8 hours using this stack.

Evidence: Before making any configuration changes to logging settings, snapshot the current logging state: export existing CloudTrail trail configurations (aws cloudtrail describe-trails), Azure Monitor Diagnostic Settings (az monitor diagnostic-settings list), and GCP Cloud Audit Log exclusion filters. Document which services currently have data-plane and management-plane logging disabled — these gaps are themselves forensic evidence of pre-existing blind spots that an attacker may have exploited or that regulatory auditors will request. No volatile host state is altered by this audit step, but the current logging configuration is mutable and must be preserved before remediation changes overwrite it.

Step 2: Review controls — verify MFA enforcement for all cloud administrative and service accounts (NIST AC-7, CIS 6.3, CIS 6.4, CIS 6.5); audit role and permission assignments against least-privilege principles (NIST AC-6, CIS 5.4); confirm that dormant or over-privileged cloud accounts are identified and remediated (CIS 5.3)

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: hardening identity controls to reduce attack surface before cloud control plane compromise occurs

Controls: NIST AC-6 (Least Privilege), NIST AC-7 (Unsuccessful Logon Attempts), NIST AC-2 (Account Management), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Use cloud-native free tools: AWS IAM Access Analyzer (no cost) to identify cross-account and external access; run aws iam generate-credential-report and aws iam list-users --query to enumerate accounts with no MFA assigned; on Azure, run Get-MgUser -All | Where {$_.StrongAuthenticationMethods.Count -eq 0} via MS Graph PowerShell (free) to find MFA gaps; use GCP's IAM Recommender (free tier) for over-permissioned service accounts. For dormant accounts, script: aws iam list-users combined with get-login-profile and list-access-keys --user-name to find keys unused for 45+ days. Two-person team can complete this audit across a single cloud provider in one business day.

Evidence: Before remediating (disabling, modifying, or revoking) any cloud identity — including service account keys or federated role assignments — export the full current state: aws iam get-account-authorization-details (captures all users, groups, roles, and attached policies in one call), Azure az ad user list and az role assignment list --all, GCP gcloud projects get-iam-policy. These exports are volatile in the sense that they reflect the live IAM state at the moment of potential compromise; any attacker-added backdoor accounts or permission escalations will appear here and must be preserved as evidence before remediation overwrites them. Store exports as signed, timestamped artifacts per NIST 800-61r3 evidence handling guidance.

Step 3: Update threat model — incorporate the MITRE ATT&CK techniques documented in this survey (T1078.004, T1552.005, T1537, T1580, T1619, T1562) into your cloud threat register; map current detection coverage against each technique and document gaps explicitly

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: integrating current threat intelligence into detection and response planning, aligned with CSF [GV, ID] functions

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Use the free MITRE ATT&CK Navigator (https://mitre-attack.github.io/attack-navigator/) to load the Enterprise matrix, color-code the six techniques from this survey (Valid Cloud Accounts, Unsecured Credentials in

Cloud Instance Metadata, Transfer Data to Cloud Account, Cloud Infrastructure Discovery, Cloud Storage Object Discovery, Impair Defenses), and export the coverage heatmap as a gap document. Cross-reference each technique against existing Sigma rules (free, community Sigma rule repository at github.com/SigmaHQ/sigma) by searching for cloud-specific rules tagged to each technique ID. A two-person team can produce a documented gap matrix in 3–4 hours using Navigator plus the Sigma repo search.

Evidence: This step does not alter live system state and therefore does not trigger order-of-volatility obligations. However, document the threat model update with a dated version-controlled record (Git commit or timestamped document) so that post-incident reviews can confirm whether the techniques used in any subsequent intrusion were known and mapped prior to the event — this supports both lessons-learned analysis (NIST 800-61r3 §4) and any regulatory inquiry into due diligence.

Step 4: Evaluate CDR tooling maturity — assess whether your current cloud security tooling provides unified visibility across control plane, workload, and data layers; identify whether alert triage workflows are context-enriched or volume-dependent; document fragmentation points where incident response handoffs currently break

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: evaluating IR tooling and workflow capability gaps, including automation and communication infrastructure

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-7 (Audit Record Reduction And Report Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Conduct a structured tabletop exercise simulating a cloud control plane intrusion (e.g., attacker uses a compromised service account key to enumerate S3 buckets via T1619, then exfiltrates via T1537) and walk each alert through your current toolchain by hand, documenting every manual handoff. Use the free CISA Tabletop Exercise Packages (CTEPs) for cloud scenarios as a starting framework. Map the workflow against the six ATT&CK techniques from Step 3 to identify where automated context enrichment is absent. Produce a one-page fragmentation map showing tool boundaries and gap owners — this becomes the prioritized tooling roadmap.

Evidence: This is a process assessment step and does not alter live system state; no volatile evidence capture is required. Document all current tooling integration points, data flows, and triage SLAs as a baseline artifact. This documentation will be critical during post-incident review (NIST 800-61r3 §4) to assess whether tooling gaps contributed to dwell time, which the survey identifies as a primary risk driver in cloud intrusions.

Step 5: Communicate findings — brief security leadership and cloud architecture owners on the specific gaps surfaced by this diagnostic framework; quantify alert-to-investigation latency in your environment and present it as a dwell-time proxy metric for board-level risk communication

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: lessons learned, metrics reporting, and communicating findings to improve organizational posture and inform leadership

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting)

Compensating: Calculate alert-to-investigation latency manually by sampling the last 30 days of cloud security alerts from your ticketing system (JIRA, ServiceNow free tier, or even a spreadsheet) and computing mean time from alert creation to analyst first-touch. Present this single metric alongside the survey's 94% intrusion statistic as a concrete risk quantification for leadership. Use the free CISA Cloud Security Technical Reference Architecture as an authoritative external benchmark to contextualize your gaps without requiring a paid analyst report.

Evidence: This step does not alter live system state; no order-of-volatility actions apply. Preserve the raw alert latency data and gap findings as a dated, version-controlled record. If this briefing follows an actual cloud intrusion event, attach it to the incident record as a post-incident lessons-learned artifact per NIST 800-61r3 §4, which can also satisfy regulatory reporting obligations if cloud data exposure triggered breach notification requirements.

Step 6: Monitor developments — track follow-on research or regulatory guidance from CISA on cloud security baseline requirements; monitor CrowdStrike's published CDR survey full report for additional breakdown data and methodology disclosure

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: integrating external threat intelligence and regulatory updates into ongoing program improvement, aligned with CSF [GV, ID] functions

Controls: NIST AU-13 (Monitoring For Information Disclosure), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Subscribe to CISA's free email advisories at cisa.gov/uscert/mailing-lists-and-feeds and configure an RSS feed for CISA's Cloud Security guidance page. Use a free RSS aggregator (e.g., Feedly free tier) to consolidate CISA, NIST, and major vendor security blog feeds into a single daily digest. Assign one team member a 15-minute weekly review cadence to scan for new cloud baseline guidance and update the threat register from Step 3 accordingly — this is achievable by a two-person team without dedicated threat intelligence tooling.

Evidence: This is an ongoing monitoring and intelligence-collection step with no live system state changes; no order-of-volatility obligations apply. Maintain a dated log of intelligence sources reviewed and any resulting threat model or control updates — this log demonstrates continuous improvement posture and supports both internal audit and regulatory inquiries into whether the organization acted on available public guidance regarding cloud security systemic risks.

Detection Guidance

The MITRE technique profile associated with this survey points to a specific detection priority set for cloud environments. Focus on the following. First, monitor cloud identity and access logs for anomalous role assumption chains, unexpected service account activity, and OAuth token grants outside normal application flows, these map to T1078 and T1078.004 and are the primary entry and persistence mechanism described. NIST AU-2 requires organizations to define and log these event types; confirm they are captured. Second, alert on access to instance metadata services (T1552.005) from workloads where that access is not expected; this is a common credential harvesting step that precedes lateral movement in cloud environments. Third, implement detection logic for cloud storage enumeration and bulk access events (T1619, T1530), a spike in ListBucket, GetObject, or equivalent API calls from a non-standard principal or at an unusual time is a high-fidelity signal for pre-exfiltration staging. Fourth, monitor for impair-defenses activity (T1562): logging configuration changes, CloudTrail disablement, GuardDuty suppression rules, or equivalent actions in non-AWS providers are active attacker tradecraft and should trigger immediate escalation. Fifth, review external-facing application logs for exploit attempts (T1190) that could provide initial cloud footholds. For hunting hypotheses, query your SIEM for principals that have performed IAM enumeration (T1087.004) within 24 hours of first assuming a new role, this sequence correlates with post-access reconnaissance. Countermeasures directly applicable: Multi-Factor Authentication (MFA) for all cloud administrative access, User Account Permissions review and restriction, Credential Rotation for service accounts and API keys, Local and Cloud Account Monitoring for anomalous activity, and System File and Configuration Analysis for logging infrastructure tampering. NIST SI-4 monitoring controls and AU-9 audit protection controls apply directly to the logging gap described by CWE-778.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1580** — Cloud Infrastructure Discovery
- **T1537** — Transfer Data to Cloud Account
- **T1078** — Valid Accounts

- **T1619** — Cloud Storage Object Discovery
- **T1078.004** — Cloud Accounts
- **T1552.005** — Cloud Instance Metadata API
- **T1087.004** — Cloud Account
- **T1530** — Data from Cloud Storage
- **T1562** — Impair Defenses
- **T1087** — Account Discovery

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
- **AU-9** — Protection of Audit Information
- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AC-3** — Access Enforcement

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.312(a)(1)** — Access Control

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1580	Cloud Infrastructure Discovery	Discovery
T1537	Transfer Data to Cloud Account	Exfiltration
T1078	Valid Accounts	Defense-Evasion
T1619	Cloud Storage Object Discovery	Discovery
T1078.004	Cloud Accounts	Defense-Evasion
T1552.005	Cloud Instance Metadata API	Credential-Access
T1087.004	Cloud Account	Discovery
T1530	Data from Cloud Storage	Collection
T1562	Impair Defenses	Defense-Evasion
T1087	Account Discovery	Discovery

Sources

Source	URL	Tier
Blog	https://www.crowdstrike.com/en-us/blog/crowdstrike-state-of-cdr-sur...	T3
CrowdStrike Falcon Cloud Security Adds Application Context to ...	https://www.crowdstrike.com/en-us/blog/crowdstrike-falcon-cloud-sec...	T3

Source	URL	Tier
CrowdStrike Falcon® Cloud Security: Modern Security From Code to ...	https://www.crowdstrike.com/en-us/platform/cloud-security/	T3
CrowdStrike Advances CNAPP with Adversary-Informed Risk ...	https://www.crowdstrike.com/en-us/blog/crowdstrike-advances-cnapp-w...	T3
Rapid7 vs CrowdStrike: Cloud Security Detection Compared - Wiz	https://www.wiz.io/academy/detection-and-response/rapid7-vs-crowdst...	T3

Generated 2026-06-22 19:02 UTC by TJS Security Command Center