unosecur

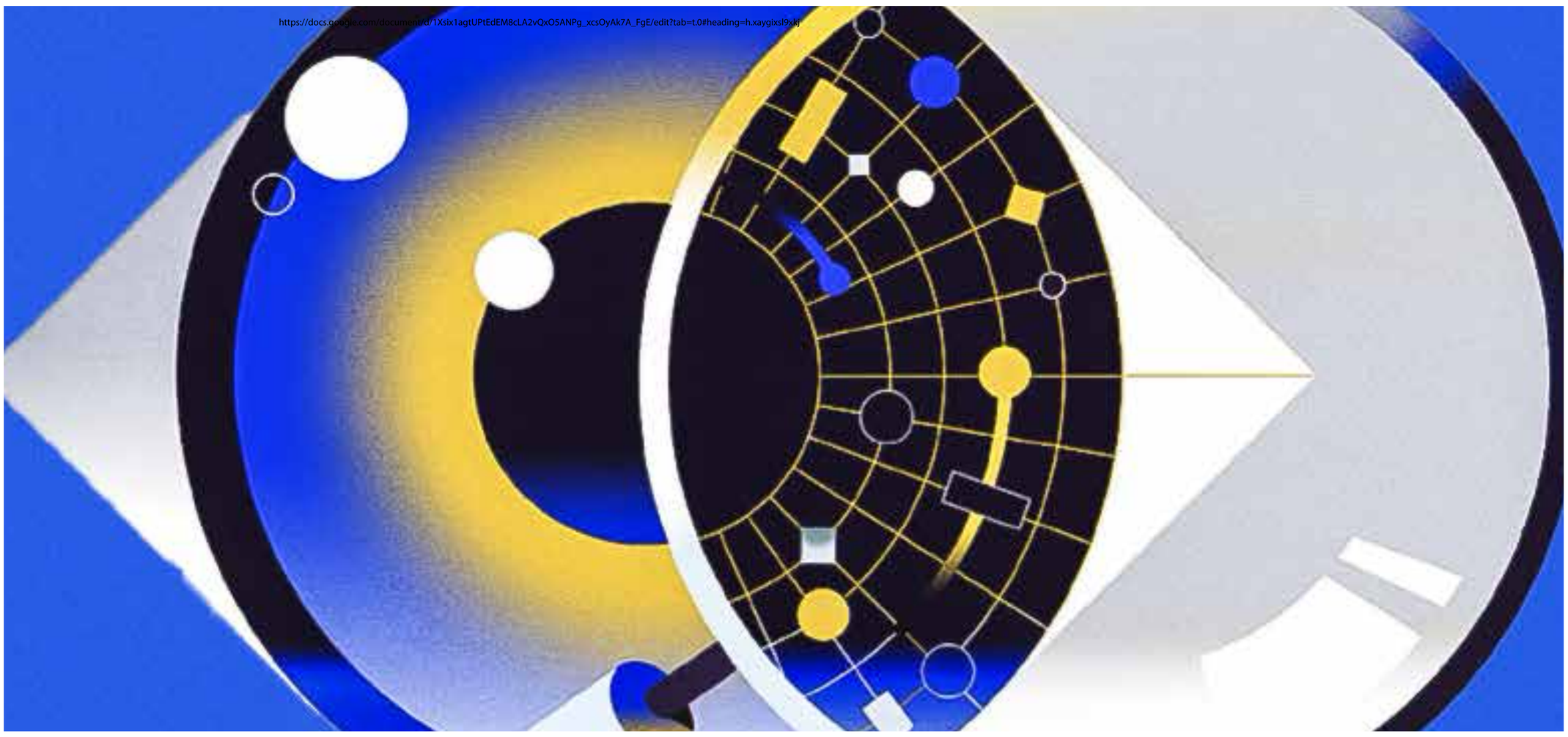
Cloud Compliance Pulse 2025

The half-year cloud identity and access compliance benchmark

Table of Contents

Executive summary

From the Unosecur Research & Intelligence Team: July 2025



Every board is now on the hook for two promises: “Innovate fast” and “Never be tomorrow’s breach headline.” Yet most published cloud-security studies rely on self-reported surveys that can’t be traced back to real controls—or they’re dominated by one region or industry. Our enterprise customers told us they need something different: a data-pure, statistically balanced view of where cloud-control hygiene really breaks down so they can justify budgets, tune roadmaps, and walk into audits with hard numbers instead of anecdotes.

How we built a credible snapshot

Between 1 January and 30 June 2025, 169 organisations ran our free Identity-Security Posture Test. We drew a stratified random sample of 50 firms, balanced across industry, geography, and primary cloud provider, to hit a 90% confidence level with ±10% precision while still publishing on a half-year cadence. Every record is an automated scan mapped directly to ISO 27001/27002, PCI DSS v4, SOC 2, CIS v8, and GDPR clauses; all company identifiers were pseudonymized in line with GDPR. The result is laboratory-grade data that a regulator, insurer, or auditor can reproduce.

What Part 1 tells: Key insights

40 is the average control failures per tenant.

98% of firms had at least one high-severity gap in the sample.

68% of tenants violated ISO 27002 - 5.17: privileged accounts without MFA (#1 violated clause).

70% of high-severity findings stem from four gap families: missing MFA, over-privileged roles, stale or duplicate credentials, and unmanaged service-account keys.

Cloud-specific weak spots: AWS = password-only admins; GCP = project-wide TokenCreator roles; Azure = subscription-level “Owner/Contributor.”

How we built a credible snapshot

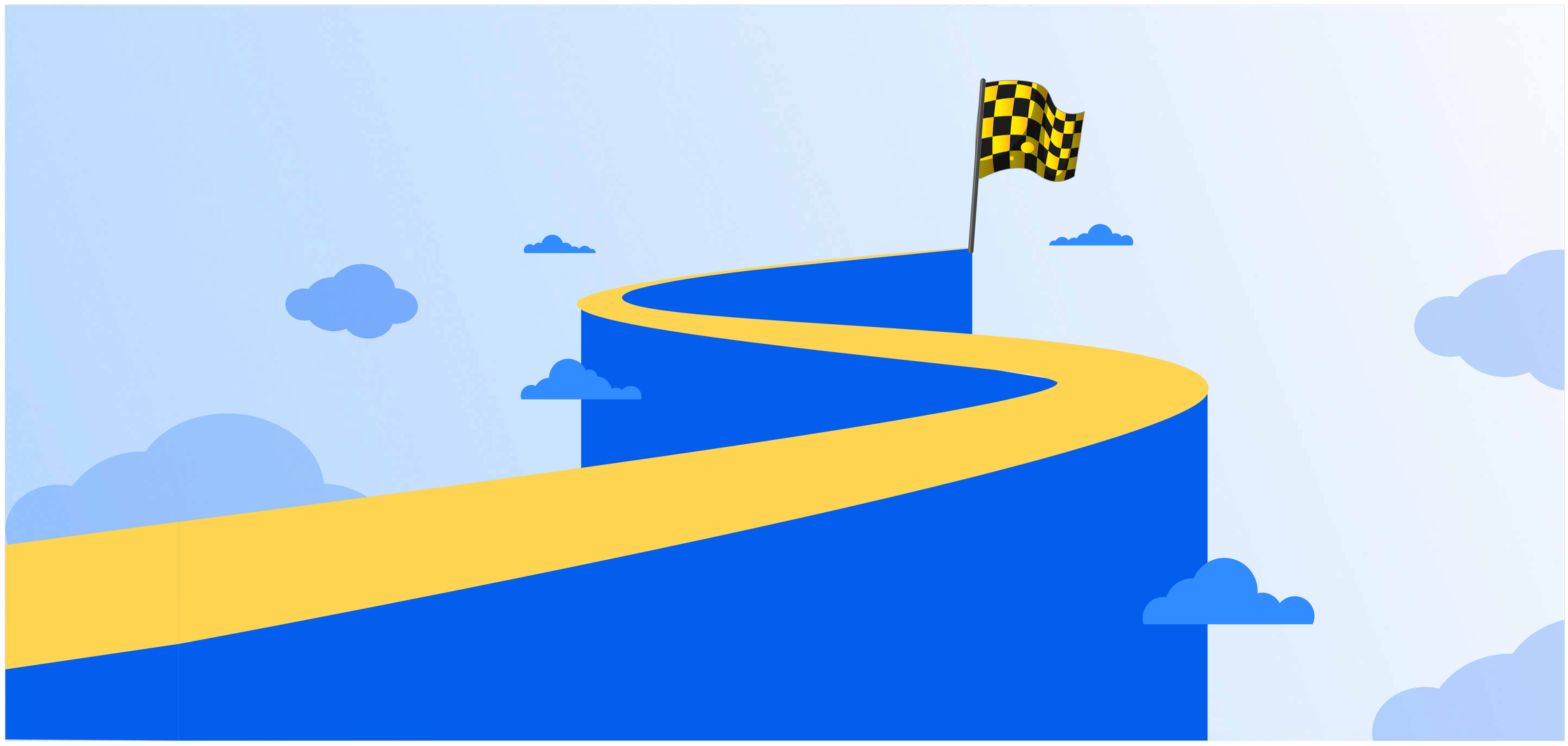
01 **Missing MFA and excessive privilege aren’t bleeding-edge threats**—they’re unlocked doors that ransomware crews and auditors spot first. These basic gaps are often the entry point for major breaches and compliance failures.

02 **Organizations that adopt these controls report clear outcomes:** faster audit cycles, reduced cyber-insurance premiums, and a stronger position in enterprise sales engagements.

03 **Enforcing four core controls can eliminate most audit findings and breach paths**: IdP-based MFA, just-in-time admin elevation, automatic rotation of keys older than 30 days, and vaulting service-account secrets.

04 **Unosecur’s platform—and this benchmark**—exist to make that shift measurable every six months, helping teams stay proactive and accountable.

Part 1
Half-yearly cloud-compliance benchmark



Coverage window: 1 January – 30 June 2025

Sample analysed : 50 organisations

Most public “state-of-cloud-security” studies pool breach anecdotes or self-reported surveys. Our benchmark is different: every data point comes from an automated control scan that maps one-for-one to ISO 27001, PCI DSS v4, SOC 2, CIS v8, and GDPR clauses. Because we stratified by industry, geography, and primary cloud provider, security leaders can compare their estate against peers on an apples-to-apples basis.

Consider this study as a market-wide “medical check-up” for cloud security. Instead of self-reported surveys, it uses real diagnostic scans, so the findings are as concrete as blood test numbers. If your competitors are showing high cholesterol (weak MFA, stale keys), you need to know where you stand before the next breach or audit hits the headlines.

The 50-company sample is 18 tech/SaaS, 9 financial, 8 healthcare, 8 retail, 7 manufacturing, with 23 based in the AWS-heavy Americas, 16 in EMEA where AWS and GCP are evenly split, and 11 in Azure-dominant APAC.

Like any credible market survey, results depend on how you pick the sample. We deliberately balanced companies by size, industry, and geography, so no single giant bank or West Coast tech firm can tilt the averages. That means you can trust that the percentages represent “normal” businesses, not just outliers.

Global headline findings

Ten most-broken cloud-control checks in our 50-organisation benchmark

Rank	Control violated (plain wording)	Orgs affected (out of 50)	% of sample	Why it matters
1	Admin account without MFA (ISO 27002 § 5.17)	34	68%	One phished password can hand over the whole cloud estate.
2	Project-wide Service-Account User / TokenCreator role (GCP)	26	52%	Any workload can mint tokens for every service account.
3	No separation-of-duties on KMS keys	24	48%	One person can both create and decrypt master keys.
4	No SoD on service-account roles	23	46%	The same user grants and uses machine privileges, hiding abuse.
5	Write permissions granted with no business justification	22	44%	Auditors flag it as a PCI DSS v4 Req 7.2 breach.
6	User-managed service-account keys older than 90 days	21	42%	Leaked JSON key = permanent, MFA-less API access.
7	Self-managed SA keys instead of provider-managed	20	40%	Keys sit in code repos; no auto-revocation on staff exit.
8	Users bypassing corporate SSO for local log-ins	20	40%	Breaks MFA policy and central logging; SOC 2 CC6 hit.
9	Service account with Admin privileges	19	38%	Malware running as the build bot gets root-like power.
10	Human user allowed to impersonate service accounts	18	36%	An insider can act as any workload, blurring audit trails.

On average, each company had 40 cloud control failures. Think of them as unlocked doors or spare keys under the mat. Nearly all firms had at least one high-risk gap, and the worst offender (missing MFA on admin accounts) is the digital equivalent of leaving the server room unlocked.

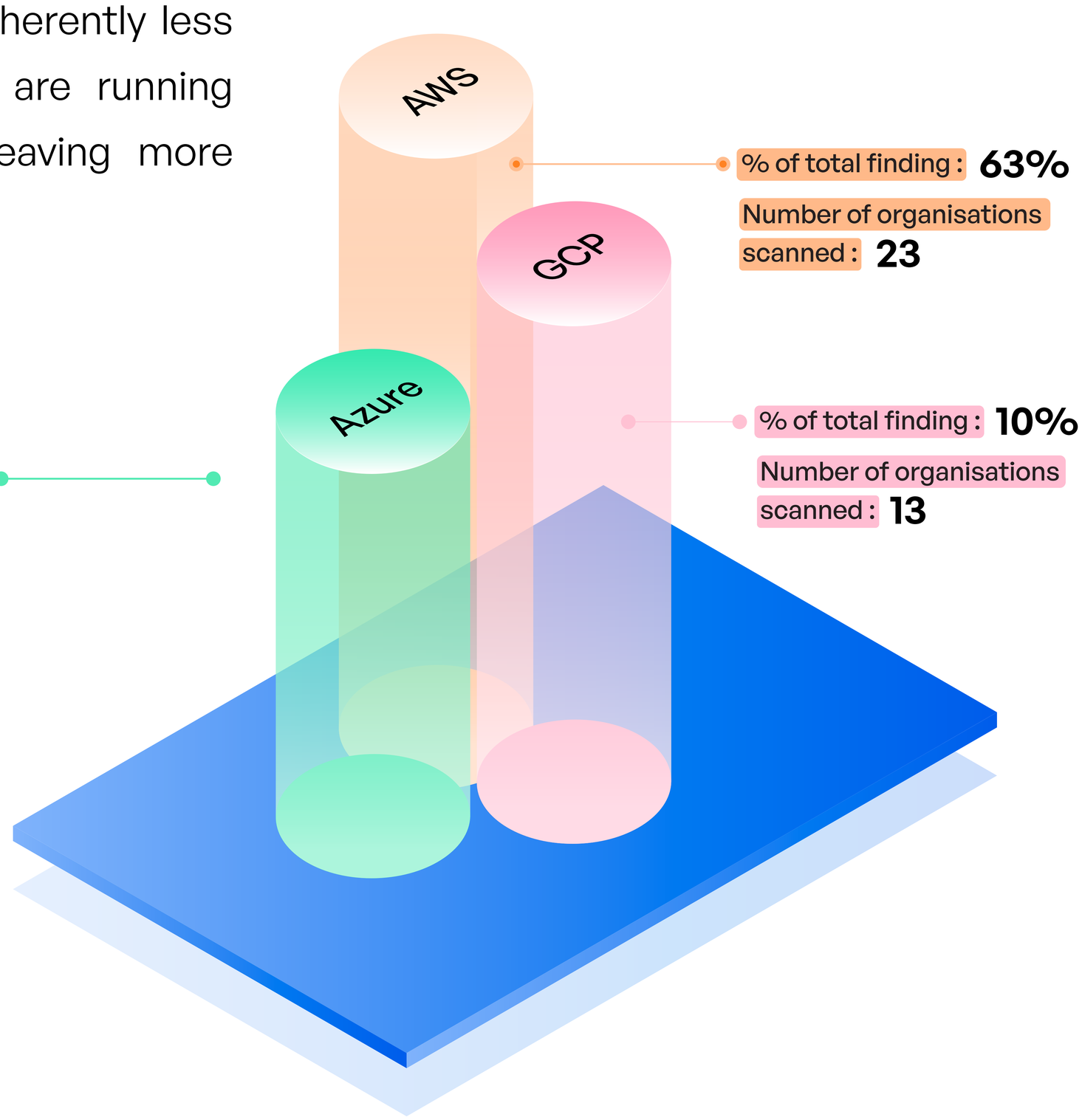
Breakdown by cloud service provider

Different clouds have different ways of optimal working. In AWS, too many admins still operate without two-factor login. In Google Cloud, machine accounts hold sweeping powers. In Azure, companies leave subscription-wide “Owner” roles lying around. If you run multi-cloud, you can’t assume one provider’s settings protect you in another.

Cloud compliance findings: Overview

01 AWS is also the most-used platform in the study (23 of 50 companies), but even after adjusting for that, AWS still shows the highest per-tenant failure count.

02 This does not mean AWS is inherently less secure; it means customers are running more workloads there and leaving more controls unchecked.



03 Azure’s low share may reflect lighter adoption or incomplete scanner onboarding, so organisations should confirm all subscriptions are being examined.

Top compliance violations and business impact

Cloud provider	Top failed control	Typical business impact
AWS	IAM user with AdministratorAccess and no MFA	Full-account compromise - ransomware, data exfiltration
GCP	Service Account User/TokenCreator at project scope	Token forgery; lateral movement across projects
Azure	Owner/Contributor role at subscription level	Unrestricted resource deletion or crypto-mining

The changing percentage share may partly reflect less scanning coverage. What the data tells us is simple: if your company runs on any of these three platforms, you have a ready reckoner of the most common compliance violations. For multi-cloud businesses, this data reinforces that not all environments carry the same risk. Assuming they do could leave serious gaps unaddressed.

Santhosh Jayaprakash
Founder and CEO, Unosecur

Recommendations at a glance

Enabling MFA and pruning admin roles are settings in your identity provider, not multi-year transformations. Rotate old keys and vault machine credentials, and you've neutralised 70% of what auditors flagged, often in a single quarter.

01 Mandate MFA on every privileged login : ISO 27002 § 5.17, SOC 2 CC6, PCI 8.5.1.

02 Adopt just-in-time elevation & PIM/PAM : strip standing admin, owner, or project-wide SA roles.

03 Rotate & vault long-lived keys: auto-disable IAM keys >30 days; migrate GCP JSON keys to Workload ID.

04 Verify scanner coverage : Azure subs often unmonitored; onboard and run baseline scan.

05 Track four KPIs : Privileged MFA %, standing admin roles, stale keys, vaulted SA keys.

Our half-year benchmark confirms what incident headlines hint: **basic identity controls, especially MFA and least-privilege, remain the soft spot in multi-cloud estates.** The pattern is plain: most companies still stumble on basic identity hygiene.

The good news is the fix list is short, cheap, and measurable. If you tackle these basics now, you'll not only avoid tomorrow's breach headlines but also sail through ISO, SOC 2, and PCI audits with fewer findings and lower insurance costs.

Part 2: Cloud-provider deepdives

Cloud security and IAM vulnerabilities

2025 IAM & Cloud Security Incidents (Q1–Q2)

aws Vulnerabilities and Fixes related to IAM (Early 2025)

A timeline of key IAM and cloud security vulnerabilities disclosed and patched by AWS in early 2025, highlighting affected services, exploit types, and remediation actions.

January 16, 2025

CVE-2025-0693: IAM Username Enumeration Flaw

Key IAM-related vulnerabilities have been disclosed and fixed in early 2025. For example, AWS identified CVE-2025-0693, a username-enumeration flaw in the IAM user sign-in flow (prior to 16 Jan 2025). An attacker could distinguish valid IAM usernames via timing differences. AWS resolved this by normalizing response times across failure cases, eliminating the timing channel.

February 2025 (Early)

CVE-2025-1969: TEAM Feature Spoofing Flaw

Another IAM issue, CVE-2025-1969, affected the Temporary Elevated Access Management (TEAM) feature of AWS IAM Identity Center; a spoofing flaw in request validation allowed attackers to forge an approval in versions <1.2.2. AWS patched it in TEAM v1.2.2 and issued guidance to upgrade.

March 2025

CVE-2025-2598: Credential Leak in AWS CDK CLI

Similarly, CVE-2025-2598 involved the AWS CDK CLI: certain credential plugins could inadvertently leak temporary credentials in console output. AWS fixed this in CDK CLI v2.178.2, and advised users to rotate any exposed credentials.

Path Traversal in EC2 SSM Agent (Reported by Cymulate)

Another report by Cymulate (coordinated with AWS) described a path-traversal weakness in the Amazon EC2 SSM Agent: malicious plugins could traverse into the SSM plugin ID, potentially leading to privilege escalation. AWS fixed this in the SSM Agent (versions ≥3.3.1802.0) in March 2025.

CVE-2025-21614 / ALAS-2025-2739: DoS in Amazon Linux SSM Agent

AWS also patched related issues in its agent's dependencies: e.g. ALAS-2025-2739/CVE-2025-21614 in the Amazon Linux SSM Agent for a Go-git DoS.

Microsoft Azure Vulnerabilities and Mitigations (First Half of 2025)

A snapshot of major Azure vulnerabilities and mitigation efforts disclosed in early 2025, including CVEs and evolving security defaults around access control.

CVE-2025-29813 (Azure DevOps token hijacking)

In the first half of 2025, Microsoft disclosed several high-severity Azure vulnerabilities.

Notably, CVE-2025-29813 (Azure DevOps token hijacking) was a critical (CVSS 10.0) privilege-escalation flaw in the Azure DevOps pipeline token system: an attacker able to edit pipelines could swap short-lived tokens for long-lived ones.

Microsoft says this issue has been fully mitigated in its service (no user action needed).

CVE-2025-29972 (Azure Storage Resource Provider SSRF)

Other Azure CVEs include CVE-2025-29972, an Azure Storage Resource Provider SSRF that could allow spoofing of network requests (patched by Microsoft).

CVE-2025-29827 (Elevation-of-Privilege in Azure Automation)

CVE-2025-29827, an Elevation-of-Privilege in Azure Automation (patch released).

CVE-2025-47733 (Azure Power Apps data exposure)

A bug in Azure Power Apps (CVE-2025-47733) also exposed sensitive data, which Microsoft fixed under its Update Guide.

Azure Misconfigurations

In addition to CVEs, misconfigurations remain a focus: researchers reported scenarios where overly broad Azure RBAC or Azure AD misconfigurations could be exploited for lateral movement or token misuse.

Microsoft's Mitigation Measures

Microsoft's evolving mitigation includes more granular Conditional Access defaults and mandatory MFA for all Azure accounts (announced in late 2024 for 2025 roll-out).

Google Cloud Platform Vulnerabilities and Fixes (Early 2025)

In the first half of 2025, Google addressed multiple vulnerabilities across its cloud services—ranging from privilege escalation in Cloud Run and Cloud Composer to IAM improvements and patching of CVEs. Below is a breakdown of these events by month:

January 2025

"ImageRunner" Bug in Cloud Run

Google addressed the "ImageRunner" bug in Cloud Run: a tenant with Cloud Run edit rights (but no Container Registry access) could nevertheless pull private images and inject code. Google fixed it by Jan 28, 2025 (eliminating the unintended IAM combination).

April 2025

“ConfusedComposer” Issue in Cloud Composer

In April, Google closed the “ConfusedComposer” issue: Cloud Composer environments could use a malicious PyPI package to escalate privileges to the underlying Cloud Build service account. Google removed the problematic privilege on April 13, 2025 to thwart this attack.

CVE-2025-4600: Parsing Bug in Classic Load Balancer

Google’s bulletins also list several updates: e.g., a parsing bug in Classic Load Balancer (CVE-2025-4600) was fixed in April 2025.

Login Flaw in Looker BI

Google’s Looker BI service had a login flaw patched on Apr 29, 2025.

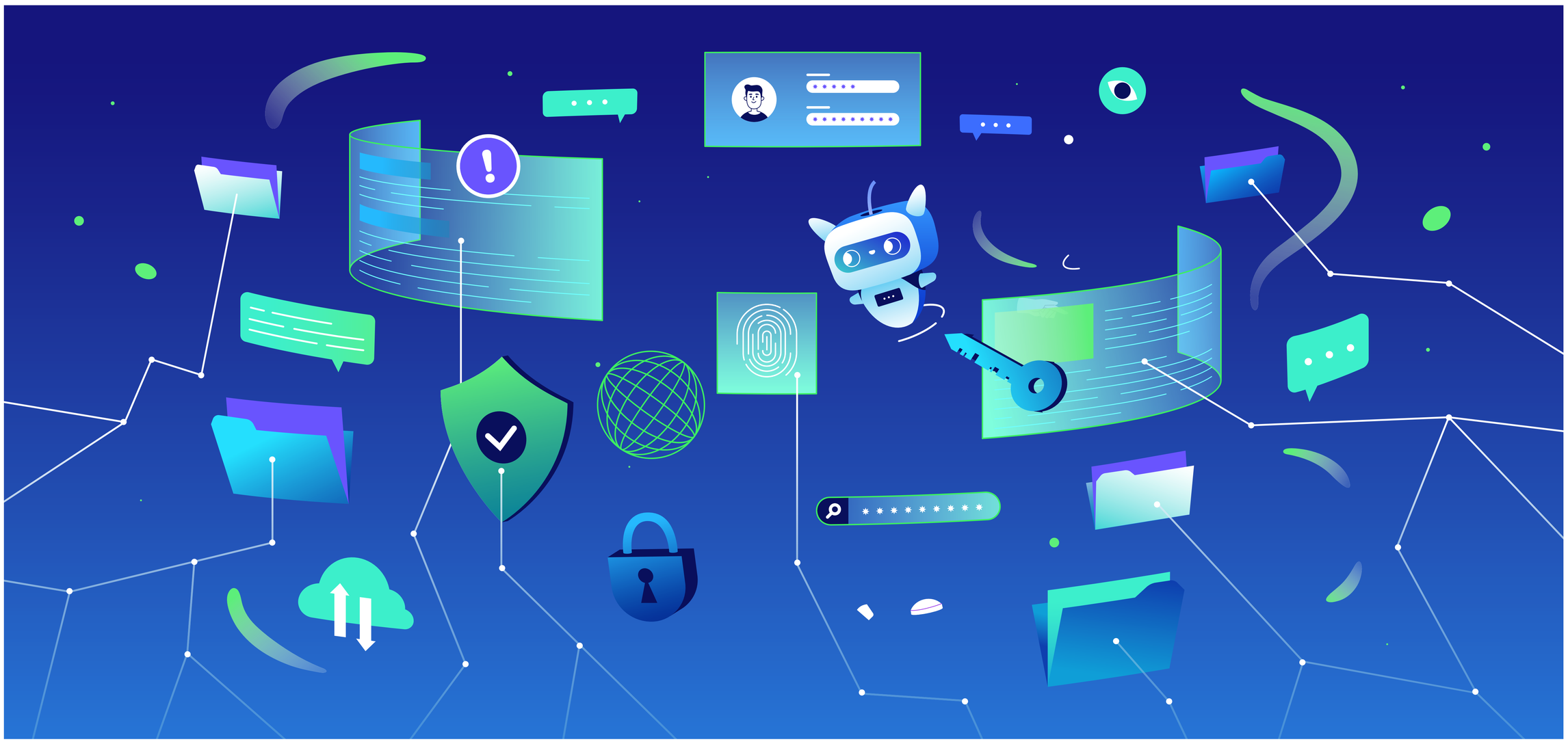
General / Ongoing Improvements

IAM Hardening Across GCP

Certain GCP-wide improvements, such as upcoming mandatory MFA and strengthened OAuth token controls, have been taken to improve IAM.

Part 3: Regulatory radar

Legal provisions: cloud security, IAM, AI identities



Global Overview

Globally, regulations are tightening around cloud security, identity management, and AI agents. In the EU, the eIDAS 2.0 framework will mandate member states to issue verifiable Digital Identity Wallets (allowing citizens to prove identity with apps): implementing acts were adopted in May 2025.

The EU's Digital Operational Resilience Act (DORA) entered into force on 17 Jan 2025: it applies to financial firms and their ICT providers (including cloud services) to ensure robust identity and access controls and incident reporting. The EU also continues enforcing GDPR and NIS2 (cybersecurity) against cloud providers and emphasizes non-human identity (e.g., new draft rules against AI deepfake impersonations as identity fraud).

Around the world, regulators are converging on the same message: use strong MFA, give every human or machine only the access it needs, and prove you're watching. To stay ahead, organisations should start with one crucial step: roll out MFA for all privileged accounts. Zero trust is one tidy set of steps that satisfies audits and frustrates attackers alike.

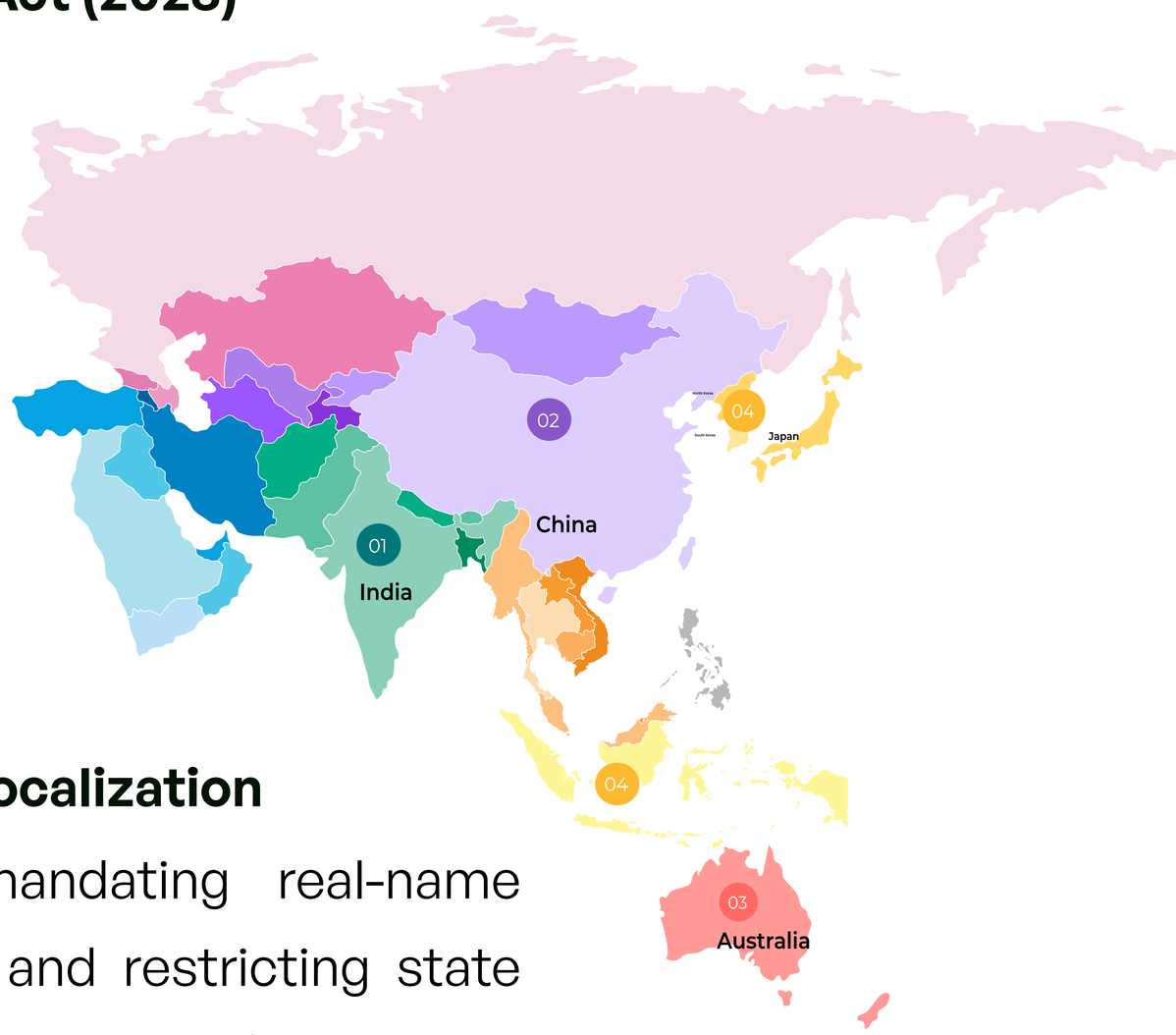
Santhosh Jayaprakash
Founder and CEO, Unosecur

Regional Trend: Data & AI Laws Impacting Cloud IAM

In APAC, countries are rolling out data and AI laws affecting cloud IAM.

01 India: Digital Personal Data Protection Act (2023)

Notably, India's Digital Personal Data Protection Act (2023) came into force on 26 Oct 2024, placing strict consent and data-handling obligations on all digital services (including cloud/identity providers) handling Indian user data.



02 China: Real-Name Verification & Data Localization

China has issued new guidelines mandating real-name verification for certain online identities and restricting state data export (cloud reliance on local identity systems).

03 Australia & Others: Privacy Law Reforms

Australia and other APAC nations are also strengthening privacy laws (e.g., Australia's pending Privacy Act reforms with heavier breach penalties and identity

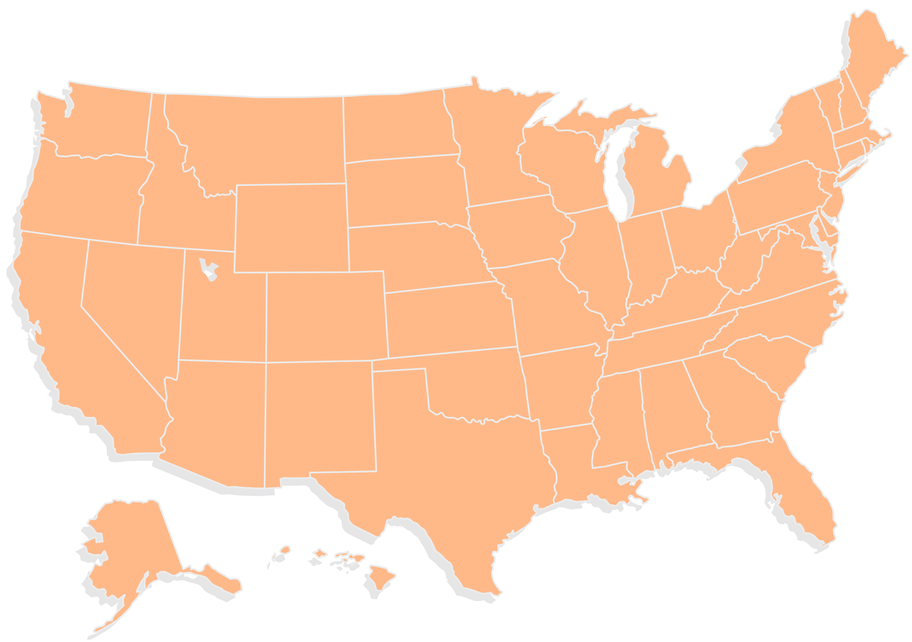
04 AI Governance Rising Across APAC

AI governance is rising: Singapore, Japan, and Korea have published AI strategies or bills that touch on ethical use of AI identities (e.g., Korea's AI Act bans "malicious imitation" of real voices or identities).

05 Emerging Standards for AI Identity Management

While specific "AI agent identity" laws are nascent, many APAC countries now require that AI-generated content be marked and that any digital identity (even machine or bot) be managed under secure authentication schemes.

United States



01 State-Level Identity Law Expansion

In the US, several new laws and enforcement actions address identity-based cloud risks. At the state level, legislatures have expanded identity fraud statutes; for instance, New Jersey's 2025 legislation (A3912) explicitly extends identity theft to include "fraudulent impersonation or false depiction by means of AI or deepfake".

02 Federal Enforcement Action

Federal regulators have also acted. The NY Department of Financial Services fined PayPal $2 million in early 2025 for a 2022 breach caused by credential stuffing (improperly reused passwords).

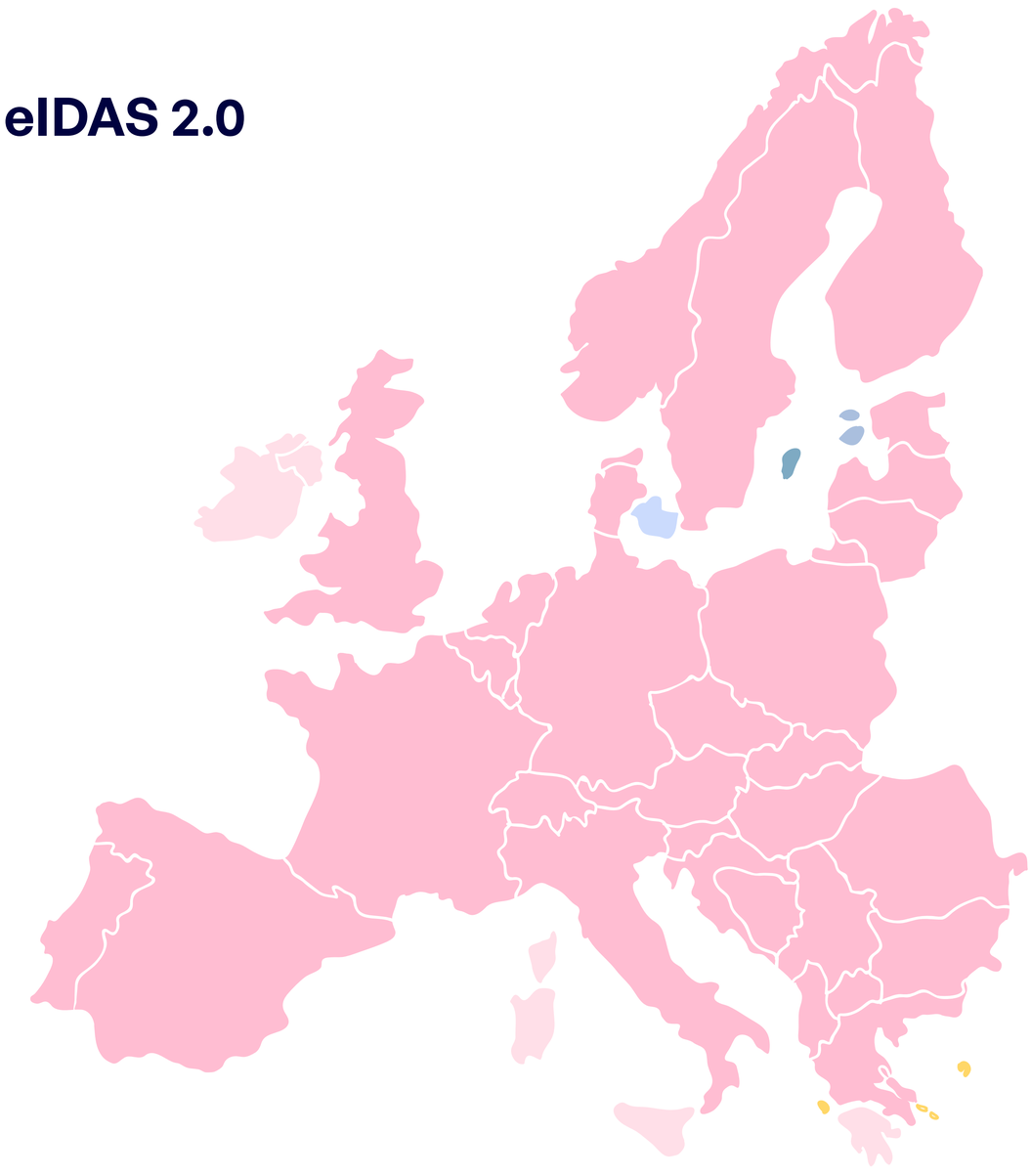
03 National IAM Mandates & Zero Trust Push

On the national front, US agencies continue rolling out identity mandates: the White House and CISA are pushing Zero Trust, requiring multifactor authentication and continuous identity vetting for cloud access.

04 Legislative & Standards Evolution

Meanwhile, new bills in Congress (such as the Cyber Incident Reporting for Critical Infrastructure Act 2.0) and evolving NIST standards (SP 800-63 digital ID guidelines) emphasize stronger identity proofing and accountability in cloud services.

European Union



01 Regulatory Momentum Beyond DORA and eIDAS 2.0

Besides DORA and eIDAS 2.0, the EU is advancing AI and privacy law.

02 EU AI Act (Expected Mid-2025)

The upcoming EU AI Act (expected mid-2025) will classify AI systems (including AI agents) by risk and require providers to manage identities of high-risk AI (e.g., bans on untraceable deepfakes).

03 GDPR and ePrivacy Rule Evolution

The EU's GDPR remains a backstop for automated identity systems, and new ePrivacy rules are under negotiation (impacting cloud messaging and IoT identity).

04 Enforcement Highlights (2025)

Notably, EU enforcement actions in 2025 have targeted IAM lapses; for example, a major EU social network was fined for failing to secure user credentials in a breach.

05 Policy Direction: Strong Authentication & Transparency

Overall, EU law is moving towards mandating strong authentication and transparency for both human and non-human (e.g., AI bot) identities in the cloud.

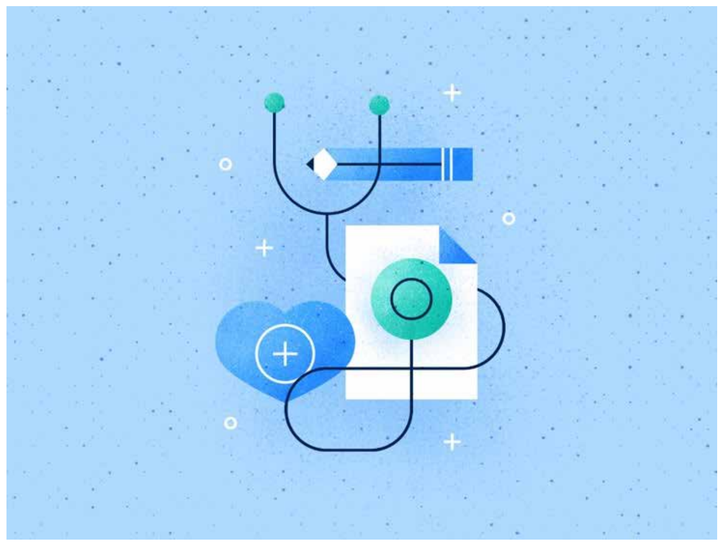
Part 4: Identity-driven breach casebook

Data breaches and identity-based threats

These are the major breaches since January 2025 attributable to stolen or misused identities (credential compromise or insider action), organized by sector and region. (Where known, we note cause and impact.)

Healthcare/Education

01 **PowerSchool (US, Dec 2024–Jan 2025)—** Student information system exfiltrated via a compromised employee password. NBC and Bleeping Computer report up to 62 million records of student and staff data (names, SSNs, grades) were accessed.



02 **Western Sydney Univ (Australia, Jan–Feb 2025)—** OneLogin SSO credentials were compromised, and nearly all personal data was exposed via a vulnerability. Bleeping Computer notes WSU had multiple incidents, including O365 admin compromise.

03 **Ascension Health (US, 2024/2025) —** In Apr 2025 Ascension notified 437,329 patients that demographic/health data (names, DOBs, SSNs) was stolen after Ascension inadvertently shared files with a third-party partner that was later breached. The state reports say this stemmed from a cloud-based interface flaw. Ascension is offering two years of credit monitoring.

04 **Alternate Solutions Health et al. (US, May 2024, reported Apr 2025) —** Four U.S. healthcare entities (Alternate Solutions Health, Park Royal Hospital, etc.) reported in April 2025 that employee email accounts were breached via credential theft, exposing ~107,000 patient records.

05 **Onsite Mammography (US, Oct 2024 discovered)—** Discovered Apr 2025: hackers used a stolen support account to access email and leak PHI of >350,000 patients. In each case, stolen credentials or session tokens were the root cause.

Finance/Business

01 **TD Bank (US, Aug–Dec 2022; disclosed 2024/2025) —** A former employee illegitimately accessed TD customers' data (names, SSNs, DOBs, account numbers) over months in 2022. A March 2025 class-action lawsuit alleges TD failed to safeguard against this insider threat. DFS fined TD $2M for a related credential-stuffing incident.

02 **Freddie Mac (US, Feb 2025) —** Reported Feb 19, 2025, a breach exposed consumer names and Social Security numbers. The origin is unclear, but the firm notified customers to watch for fraud. (All regions are potentially affected.)

03 **Hertz (US, Dec 2024–Apr 2025) —** In Apr 2025 Hertz revealed that hackers broke into its partner Cleo Communications (a data-transfer vendor) and exfiltrated license, credit card, and contact data (including SSNs) on recent renters. The cause was stolen/abused Cleo account credentials.

04 **DecisionFi (US, Jan 2025) —** A fintech firm disclosed that an attacker accessed its financial web portal and stole consumer data (details unspecified) in January 2025, apparently via a compromised account.

05 **VeriSource (US, Feb 2024; disclosed Apr 2025) —** An employee-benefits firm revealed in April 2025 that a Feb 2024 breach (via stolen credentials) had exfiltrated personal info of ~4 million people (including 4M SSNs).

06 **Phemex Exchange (Crypto, global, Jan 2025) –** (By stolen private keys, not identity-based.)

Government/Public Sector:

01 **AT&T/FBI (US, late 2024) —** In Jan 2025 it emerged that AT&T's systems were hacked, compromising call logs of over 20,000 FBI accounts. The breach (likely via stolen AT&T corporate credentials) exposed agents' call metadata, risking informant identities.

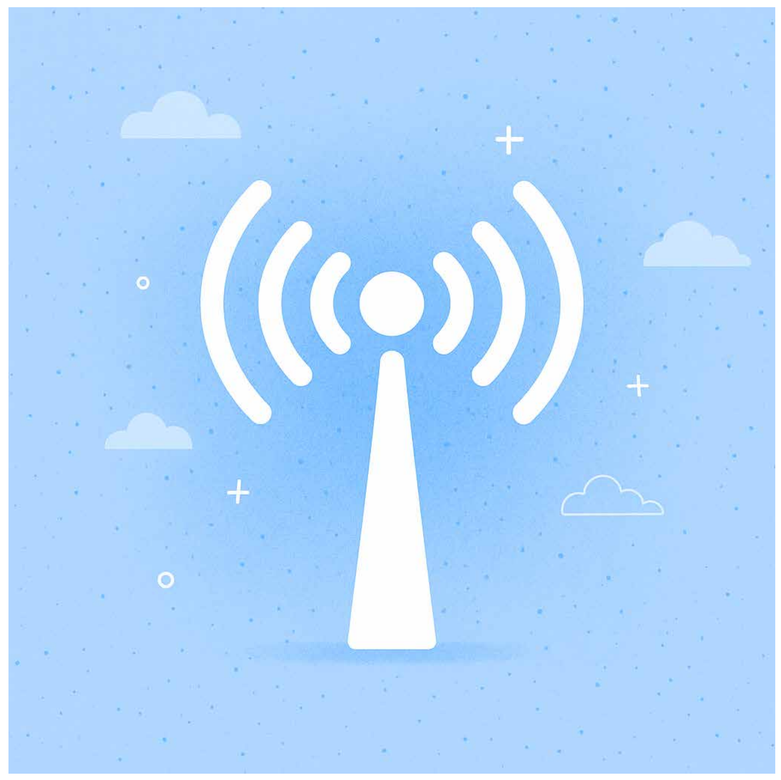
02 **Texas Health & Human Svcs (US, 2023/25) —** In April 2025 Texas HHS reported that nine (now-fired) state employees improperly accessed and disseminated ~95,000 Texans' benefit records (SSNs, health ID#s). The insider disclosures (3.4M pages of data) came to light in multiple waves (latest 33K records in Apr 2025). Watch for fraud. (All regions are potentially affected)

03 **Urban One (US, Mar 2025)—**Media company attacked via a social-engineering scheme in Feb 2025; employee credentials were phished. The hackers (Cactus ransomware gang) extracted employees' personal data and company documents.

04 **New York University (US, Mar 2025)—**A hacktivist defaced NYU's website and leaked ~3 million admissions records (names, test scores, financial data) from an internal data warehouse. This was not credential-based, so it is outside our scope except to note the impact on the educational sector.

Telecom/Technology:

01 **Orange Group (Romania/EU, Jan 2025)** — A hacker "Rey" broke into Orange Romania and stole ~6.5 GB (≈600K customer and employee records, PII, and source code) via compromised operational credentials or insider access. Orange confirmed the breach and noted "gaps in threat detection."



02 **Telefónica (Spain/EU, Jan 2025)** — In Jan 2025 Telefónica announced an internal ticketing system breach after attackers used stolen employee credentials to exfiltrate 2.3 GB of data. Affected data included network configurations and some personal info of Spanish employees.

03 **SK Telecom (South Korea/APAC, Apr 2025)** — On Apr 18, 2025, Korea's largest mobile carrier detected malware that exfiltrated customer data. The breach (revealed Apr 27) reportedly involved stolen admin credentials; SKT warned that millions of user records may be affected.

04 **Marks & Spencer (UK/EU, Feb–Apr 2025)** — Outage-inducing Scattered Spider ransomware in early 2025 compromised M&S's Windows domain (stealing the AD NTDS.dit file). The attackers had likely phished an admin credential back in Feb. M&S confirmed on Apr 28, 2025 that the ransomware attack caused a major data leak and payment disruption.

05 **Jaguar Land Rover (UK/EU, Mar 2025)** — Ransomware group Hellcat claimed they obtained ~700 internal documents, including JLR employee credentials and source code, by stealing Jira admin credentials via malware. The company is reviewing its access controls after the March 2025 leak.

06 **Western Sydney Univ. (Australia/APAC, Apr 2025)** — (Covered above under Education.)

Identity hygiene now, resilient cloud tomorrow: Takeaways and next steps

Our half-year benchmark shows one thing: identity hygiene still decides whether a cloud estate withstands or suffers the next breach.

- In our 50-company sample, four basics—privileged-user MFA, least-privilege roles, key rotation, and service-account vaulting—caused 70% of all high-severity issues.

- These very gaps drove almost every 2025 CVE and breach: timing leaks in AWS log-ins, long-lived Azure pipeline tokens, overpowered GCP service accounts, and stolen credentials in the wild.

- Regulators are closing in. DORA is live, eIDAS 2.0 passed in May 2025, U.S. zero-trust orders shorten MFA deadlines, and India's DPDP plus Australia's privacy overhaul demand auditable machine identities.

- Sector rules echo the shift: proposed 2025 HIPAA amendments explicitly call for MFA to protect healthcare data.

Three forces will shape the next cycle.

- **MFA everywhere :** AWS now offers passkeys for IAM users and hints at root-user support; Microsoft is auto-enabling MFA across Azure; HIPAA and DORA make it non-negotiable.

- **Mature machine-identity governance :** Token provenance, tight SA scoping, and AI-agent tagging will move from "nice to have" to audit checklist under PCI DSS 4.0, the EU AI Act, and refreshed NIST 800-63.

- **Live evidence over static attestations :** Insurers, regulators, and customers increasingly demand real-time dashboards proving least privilege, key age, and privileged MFA.

All of these reinforce the fact that identity is the new perimeter. One stolen password or over-privileged service account can breach your entire multi-cloud stack. Regulators now mandate MFA and least privilege. Fail to tighten identity controls, and you face both attackers and fines.

For identity security, they trust us

Rakuten ZEOTAP INNOVAPPTIVE

aikido axel springer

Ready to secur your enterprise identities?

Take a free risk assessment!

+100 more apps & integrations

Unosecur | Unified Identity Fabric at Runtime