AccuKnox®

Cloud Security Posture Management Report (CSPM)

Report Period **30 Days** - **Feb 12, 2025 12:00:00** to **Mar 12, 2025 12:00:00 (IST)**

Prepared for
Acme Corp

Prepared by
AccuKnox
support@accuknox.com

Report Summary

The CSPM scan assessed **22 cloud accounts** across **20 AWS**, **1 GCP**, and **1 Azure** environments, covering **1.2k cloud assets**. A total of **2.3k findings** were identified, including **300 High**, **100 Medium**, and **1.9k Low** severity issues. These findings span **10** unique security misconfigurations.

The account with the highest number of issues was **100**, while **10** had the least. The most frequently affected asset type was **IAM**, indicating a critical area for remediation.

Cloud Findings

Feb 12, 2025 12:00:00
to **Mar 12, 2025 12:00:00**

Cloud Accounts

Data is based on time of report generation

21 Accounts ● 18 Active ● 3 Inactive

8 Accounts
● 7 Active
● 1 Inactive

9 Accounts
● 7 Active
● 2 Inactive

4 Accounts
● 4 Active
● 0 Inactive

Manage multiple cloud accounts effortlessly with real-time visibility. Quickly identify active and inactive accounts for better control and governance.

Total Asset Count by Cloud Provider

55.6k Assets
32.2k assets with findings

1,200 Assets
923 assets with findings

2,100 Assets
542 assets with findings

View total cloud assets at a glance with clear insight into impacted assets. Easily track assets affected by security findings for faster risk mitigation.

Total Assets

Monitor total assets growth or reduction over time with historical trends. Gain insights into infrastructure changes and optimize resource planning.

Assets by Category

Assets	Count
Containers	18.5k
AWS Identity	1.5k
Serverless	1,000
Database	1,100
Storage	150
+ Others	120

Get a clear breakdown of assets by category for better resource visibility. Quickly identify distribution across compute, storage, network, and more.

Cloud Findings

Feb 12, 2025 12:00:00
to **Mar 12, 2025 12:00:00**

Top 10 Assets with Findings

Asset	Findings	Severity			
69e37648-d32f-46a0-a45e-e983eb816225"	200	100 C	75 H	15 M	10 L
cddefense-trail-log-bucket-186751747428	450	350 C	50 H	25 M	25 L
cf-templates-12sefmmdn2iv0-us-east-1	10	3 C	2 H	5 M	5 L
shaped-infusion-402417	2	2 C	0 H	0 M	0 L
prod_asset_new	1	1 C	0 H	0 M	0 L

Highlight the top 10 assets with the most security findings for focused remediation. Prioritize high-risk assets to reduce your threat exposure efficiently.

Newly Added Assets

Track newly added assets for improved visibility into recent infrastructure changes. Stay updated on onboarding trends and potential security gaps in fresh assets.

Findings by Cloud Provider

1,212 Findings

Cloud Provider	Findings		Severity			
AWS	↑ 5%	1,100	100 C	300 H	400 M	300 L
GCP	↓ 12%	67	2 C	5 H	40 M	20 L
Azure	↓ 12%	45	3 C	2 H	25 M	15 L

View security findings categorized by cloud provider for cross-platform risk visibility. Easily compare and prioritize issues across AWS, Azure, GCP, and more.

Cloud Findings

Feb 12, 2025 12:00:00
to **Mar 12, 2025 12:00:00**

Cloud Findings

109
Critical Findings

1,298
High Findings

120
Medium Findings

8
Low Findings

Cloud Findings Trend

Highlights exposed credentials, tokens, and keys categorized by severity. It helps users prioritize and remediate high-risk secrets that could lead to unauthorized access or data breaches.

Shows how secret-related risks (like leaked API keys or credentials) change over time.

Top 10 Cloud Findings

Finding	Severity	Assets
CloudTrail global services event logging is not enabled:	Critical	120
IAM Master and Manager Roles not found	Critical	88
Key Vaults are not being used to store secrets	High	64
Maximum password reuse of: 1 passwords is less than 5	High	12
Network Watcher is not enabled in the region	High	9

Discover the top 10 cloud findings ranked by severity or frequency. Focus remediation efforts on the most critical vulnerabilities across your environment.

Top 10 Cloud Accounts by Severity

Cloud Account	Findings					Severity
prod-applications	↑ 5%	1,100	100 C	300 H	400 M	300 L
dev-analytics	↓ 12%	67	2 C	5 H	40 M	20 L
stage-security	↓ 12%	45	3 C	2 H	25 M	15 L
prod-networking	↓ 12%	8	8 C	0 H	0 M	0 L
prod-datawarehouse	↑ 5%	2	2 C	0 H	0 M	0 L

Identify the top 10 cloud accounts with the highest severity findings for prioritized remediation. Quickly address critical security risks and reduce exposure across high-impact accounts.

Cloud Findings

Feb 12, 2025 12:00:00
to **Mar 12, 2025 12:00:00**

New Cloud Findings Trend

Stay on top of newly discovered findings for timely risk mitigation. Quickly identify emerging security issues as they surface across your environment.

Findings by Insights

Insight	Severity	Findings
Public Buckets Access	Critical	3,239
Publicly Available Database	Critical	233
Access Keys Older than 180 Days	High	122
Misconfigured Identity and Access Management (IAM) Policies	Medium	9
All/Custom Ports Publicly Available	Low	2

View security findings categorized by specific insights for deeper analysis. Understand vulnerabilities, misconfigurations, and compliance gaps through detailed insights.

Findings by Tags

300 Potential Exposure	**102** Authentication & Authorization	**65** Privileged Assets	**300** Outdated Components	**102** Encryption Issues	**65** Public Exposure
20 Availability Issues	**1** Logging & Monitoring	**90** Maintainability Issues	**90** Unused Assets		

Categorize findings by tags to streamline risk management and tracking. Easily filter vulnerabilities, misconfigurations, and other issues based on custom tags for better context.

Cloud Findings

Feb 12, 2025 12:00:00
to **Mar 12, 2025 12:00:00**

Findings Metrics

300 Opened	**102** Resolved	**65** Ignored
20 Accepted	**1** Unticketed	**90** Inprogress

Track key findings metrics, such as total count, severity distribution, and resolution time. Measure security posture progress with clear data on vulnerabilities and issues over time.

Findings by Status

Status	Findings
Active	120
Potential	90
Inprogress	75
Mitigated	12
Duplicate	8

Highlight the top 5 findings categorized by their current status for efficient remediation. Quickly identify critical issues marked as open, in-progress, or resolved to track progress.

Open Tickets for Critical & High Severity Findings

Ticket ID	Finding	Ticket Severity	Age (Days)
1001	CloudTrail global services event logging is not enabled:	Critical	120
1002	IAM Master and Manager Roles not found	Critical	88
1003	Key Vaults are not being used to store secrets	High	64
1004	Maximum password reuse of: 1 passwords is less than 5	High	12
1005	Network Watcher is not enabled in the region	High	9

Automatically open tickets for critical and high-severity findings to ensure prompt action. Streamline incident management by prioritizing high-impact issues with clear, actionable tickets.

SLA Status

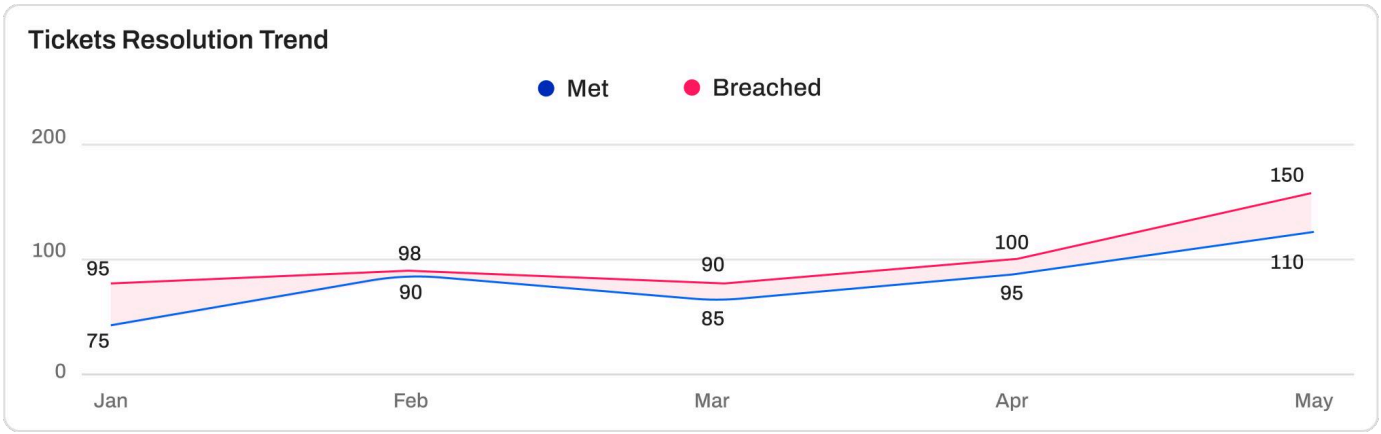
660 Open Tickets

Status	Total	Severity			
Breached	200	100 C	75 H	15 M	10 L
At Risk	450	350 C	50 H	25 M	25 L
Within SLA	10	3 C	2 H	5 M	5 L

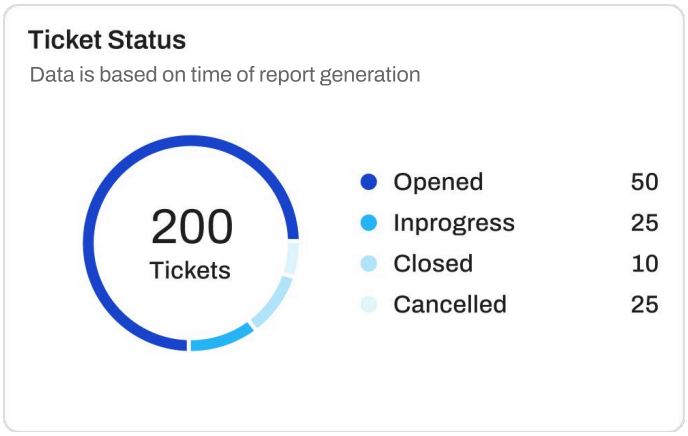
Track the SLA status of tickets to ensure timely resolution and compliance. Easily identify tickets approaching their SLA deadline or those that have breached the SLA for faster intervention.

Cloud Findings

Feb 12, 2025 12:00:00
to **Mar 12, 2025 12:00:00**



Visualize ticket resolution trends over time with counts of SLA met vs. breached. Identify performance patterns and optimize response efforts across teams.



Track support or remediation progress with a snapshot of ticket statuses. Quickly view open, in-progress, and resolved tickets to stay on top of issues.