CYCOGNITO

QUICK TAKE

Five Cloud Security Metrics that Matter

Measuring Risk Reduction and Operational Impact in the Cloud

Cloud security leaders don't need more data—they need the right signals. In an environment shaped by speed, scale, and shadow assets, quantifying real risk separates effective programs from checkbox security.

This quick take highlights five KPIs that matter. These metrics show what's exposed, how fast your teams respond, and where risk hides across your cloud estate. If your reporting isn't tied to these outcomes, neither you — nor your board — see the full picture.

METRIC 1

Mean Time to Remediate (MTTR) Critical Cloud Risks

Why it matters: Long MTTR prolongs risk exposure increasing breach likelihood and regulatory risk.

What good looks like: Industry average is weeks or months. Leaders aim for <3 days.

Leadership takeaway: Invest in automation and workflows that accelerate triage and resolution. Track remediation times across geographies, divisions, and teams to understand risk profiles.

METRIC 2

% of Cloud Assets with Unresolved Critical Misconfigurations

Why it matters: Misconfigurations remain a top cause of cloud breaches (over 75%).

What good looks like: Ideally <5% of total assets with critical misconfigurations.

Leadership takeaway: Use this metric to assess the efficacy of cloud guardrails and controls. Invest in automated tools that capture issue evidence and asset ownership to assign remediation efficiently.

METRIC 3

Attack Path Density

Why it matters: Shows how many exploitable paths exist across your environment—from external to crown jewels.

What good looks like: Lower is better. A Cloud-Native Application Protection Platform (CNAPP) will map reachable attack paths for cloud assets and help reduce risk.

Leadership takeaway: Attack path data shifts your team from reacting to alerts to proactively eliminating high-impact risk. Quarterly reporting on attack path trends (sourced from CNAPP tools, for example) provides trackable metrics.

METRIC 4

Coverage of Cloud Asset Inventory

Why it matters: You can't secure what you can't see. Shadow IT and multi-cloud sprawl increase risk.

What good looks like: Ideally >95% visibility across all assets, including cloud accounts, regions, and services.

Leadership takeaway: Ensure your cloud security tooling (example, CNAPP) has visibility into all clouds in use. Augment tooling with seedless EASM technology to baseline asset inventories and provide insight into unsanctioned cloud usage. Monitor drift carefully.

METIC 5

Risk-Weighted Remediation Rate

Why it matters: Reveals how well teams prioritize real threats over background noise.

What good looks like: Ideally 80%+ of risk-weighted issues are addressed within SLAs.

Leadership takeaway: This is an additional layer on top of MTTR tracking that provides insight into how well remediation efforts are aligned with risk. It isn't just ticket closing rate, but also which tickets are prioritized.

AND AVOID THIS METRIC...

Total Number of Findings

Why it's misleading: A rising count may look like your tools are "doing more," but it doesn't account for risk severity, asset criticality, or exploitability.

The problem: Teams become overwhelmed, risk is obscured by noise, and executive reports misrepresent progress.

What to do instead: Track risk-weighted remediation rate and attack path density, which focus on impact over volume.

How Can CyCognito Help Your Organization?

CyCognito autonomously discovers and actively tests your exposed cloud estate, identifying critical issues others miss. Rich dashboards permit visualization of key success metrics useful for leadership to understand risk at an organizational level.

Check out our website and explore our platform with a self-guided, interactive dashboard product tour. To learn more about how CyCognito can help you identify and remediate emerging threats to your attack surface, request a customized demo.

CYCOGNITO