

CLOUD SECURITY
POSTURE MANAGEMENT.

Cloud environments change by the hour — **new resources, new permissions, new exposure**. CSPM continuously scans configurations against security baselines, catching the misconfigurations and posture drift that firewalls and endpoint tools were never built to see.

- CONFIGURATION SCANNING
- DRIFT DETECTION
- COMPLIANCE MAPPING
- REMEDIATION GUIDANCE

01 THE MECHANISM



Continuous Asset Inventory
Discovering every cloud resource across accounts and providers, **including the ones nobody remembers creating**.



Baseline Comparison
Checking every configuration against security benchmarks like **CIS and cloud-provider best practices**.



Drift Alerting
Flagging the moment a resource moves away from **its approved, secure configuration**.

02 THE FLOW

The Posture Cycle CONTINUOUS

1

Cloud APIs are polled continuously to discover **new and changed resources** across every connected account.

2

Each resource's configuration is checked against **security baselines** and compliance frameworks.

3

Findings are prioritized by **exploitability and business context**, not just severity score.

The Drift Cycle LIVE EVENT

1

A new open port, public bucket, or over-permissioned role **shifts a resource out of baseline**.

2

The posture engine detects the deviation and **raises a finding**, often within minutes.

3

Automated guardrails or an assigned owner **remediate before the exposure becomes an incident**.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Asset Inventory	Maintains a live, accurate map of every cloud resource across all connected accounts.
Configuration Scanning	Continuously checks resource settings against security baselines and benchmarks.
Drift Detection	Flags configuration changes that move a resource away from its approved state.
Remediation Guidance	Provides the exact steps or automation to fix a misconfiguration.

04 CLOUD POSTURE APPROACHES COMPARED

SIGNAL	SUFFICIENT ALONE?	WHAT IT MISSES
Manual Cloud Configuration Reviews	No	Point-in-time checks miss drift that happens between review cycles.
Native Cloud Provider Alerts Only	No	Covers one provider and misses cross-account or multi-cloud exposure.
Firewall & Endpoint Tools Alone	No	Built for network and device threats, blind to cloud config risk.
Periodic Compliance Audits	No	Confirms posture on audit day, not the other 364 days of the year.
CSPM (Inventory + Scanning + Drift Detection)	Yes	Continuously finds and prioritizes misconfigurations as they happen.

CLOUD SECURITY POSTURE.

SCAN · DETECT · REMEDIATE

05 PROGRAM OPERATIONS

Misconfigurations outnumber exploits.

Most cloud breaches trace back to a setting, not a zero-day.

Findings without ownership pile up.

A misconfiguration nobody is assigned to fix never gets fixed.

Multi-cloud multiplies blind spots.

Each provider has its own console, API, and defaults to track.

Shadow resources hide in plenty.

Forgotten test environments are common entry points.

06 CONTROL MAPPING

CIS BENCHMARKS

Provider-specific hardening baselines that CSPM tools check configurations against.

NIST CSF 2.0

Identify and Protect functions covering asset visibility and configuration.

CSA CCM

Cloud Controls Matrix mapping cloud-specific objectives to compliance frameworks.

SOC 2

Trust services criteria that cloud configuration posture directly supports.

07 WHAT THIS DOES NOT SOLVE

Application-layer vulnerabilities

Secure infrastructure config doesn't fix flaws in the code running on top of it.

Identity and access sprawl

A well-configured resource can still be reached by an over-permissioned identity.

Data classification gaps

CSPM flags exposed storage but doesn't know what sensitive data is actually inside it.

Alert fatigue at scale

Thousands of low-severity findings can bury the handful that actually matter.

08 MYTHS VS. REALITY

MYTH	REALITY
"Our cloud provider secures the infrastructure, so we're covered."	Shared responsibility still leaves configuration and access decisions on you.
MYTH	REALITY
"CSPM is just a compliance checkbox tool."	Its real value is catching exploitable misconfigurations before attackers do.
MYTH	REALITY
"One cloud account is easy to keep secure manually."	Configurations drift constantly even in a single account, let alone dozens.
MYTH	REALITY
"A clean scan means the cloud is secure."	A scan is a snapshot; posture changes with every deployment.
MYTH	REALITY
"More findings mean the tool is working harder."	Unprioritized findings just create a backlog nobody clears.

09 SPEAK THE PROGRAM — KEY TERMS

CSPM

Cloud Security Posture Management: continuous scanning of configurations against baselines.

DRIFT

Any change that moves a resource away from its approved, secure configuration.

MISCONFIGURATION

A resource setting that creates unintended exposure, such as a public storage bucket.

SHARED RESPONSIBILITY MODEL

The division of security duties between a cloud provider and its customers.

BASELINE

The approved, secure configuration standard a resource is expected to match.

REMEDIATION

The action taken to correct a misconfiguration and return a resource to baseline.