

YOUR CLOUD IS GROWING. SO IS YOUR EXPOSURE.

Continuous cloud security posture management that finds misconfigurations, enforces compliance, and closes risk gaps - before attackers find them first.

Discover

Assess

Enforce

Prove Compliance



82%

of breaches involve cloud misconfigurations

Multi-Cloud

AWS, Azure & GCP - one unified posture view

Real-Time

Continuous detection, not quarterly audits

THE RISK

Your Cloud Moves Fast. Misconfigurations Move Faster.

Every time a developer spins up a new resource, a team changes an access policy, or a new cloud service is adopted, your security posture shifts. These changes happen dozens - sometimes hundreds - of times a day. And each one is an opportunity for a misconfiguration that quietly opens a door to attackers.

Cloud environments are too dynamic, too complex, and too interconnected for periodic audits to keep pace. By the time a quarterly review finds a problem, it may have been exploited for months.

Misconfigurations Are Inevitable

In fast-moving cloud environments, even experienced teams leave storage buckets exposed, ports open, and permissions over-provisioned - unintentionally.

Blind Spots Across Accounts

Most organizations have dozens of cloud accounts, services, and regions. Without unified visibility, risk hides in the gaps between teams.

Compliance Is A Moving Target

Frameworks like CIS, NIST, ISO 27001, and PCI-DSS require continuous adherence - not just a snapshot at audit time.

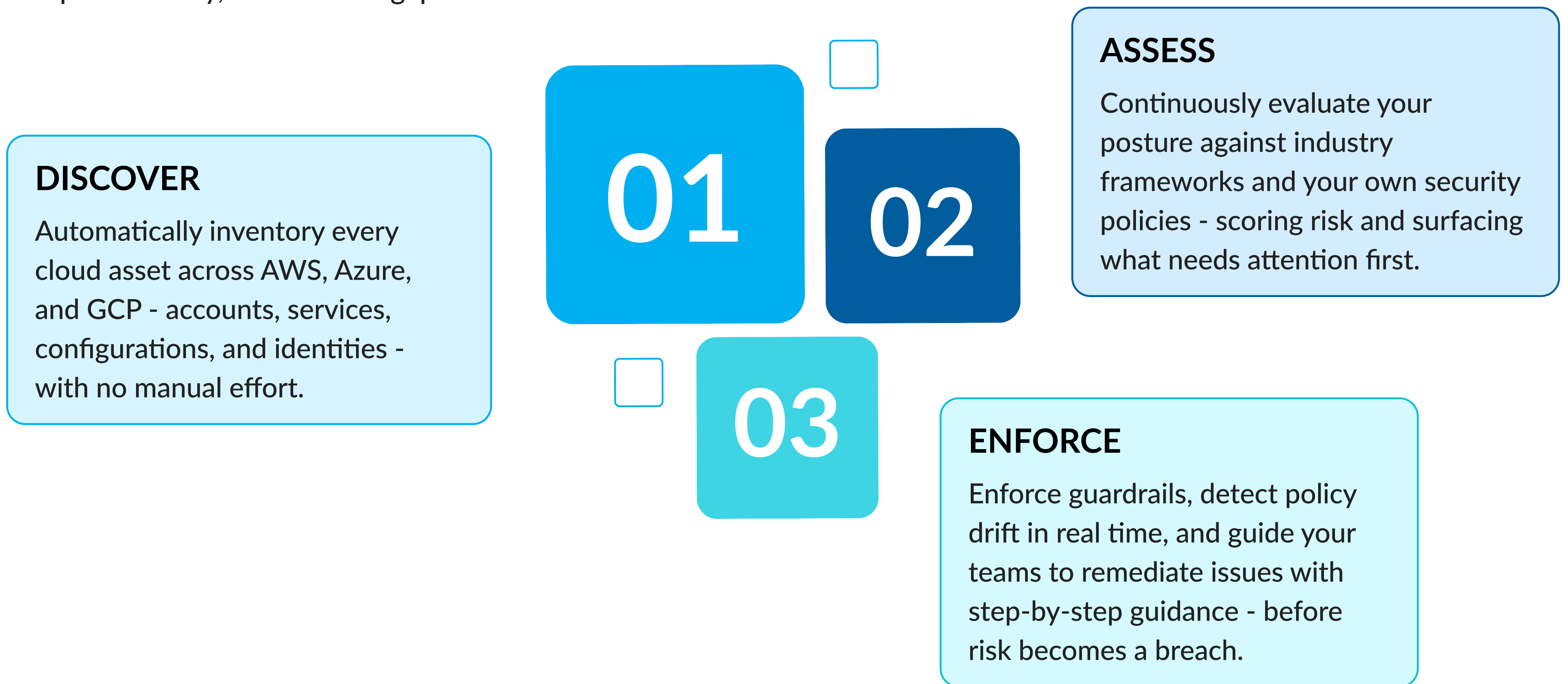


THE SOLUTION

CSPM - Cloud Security Posture Management

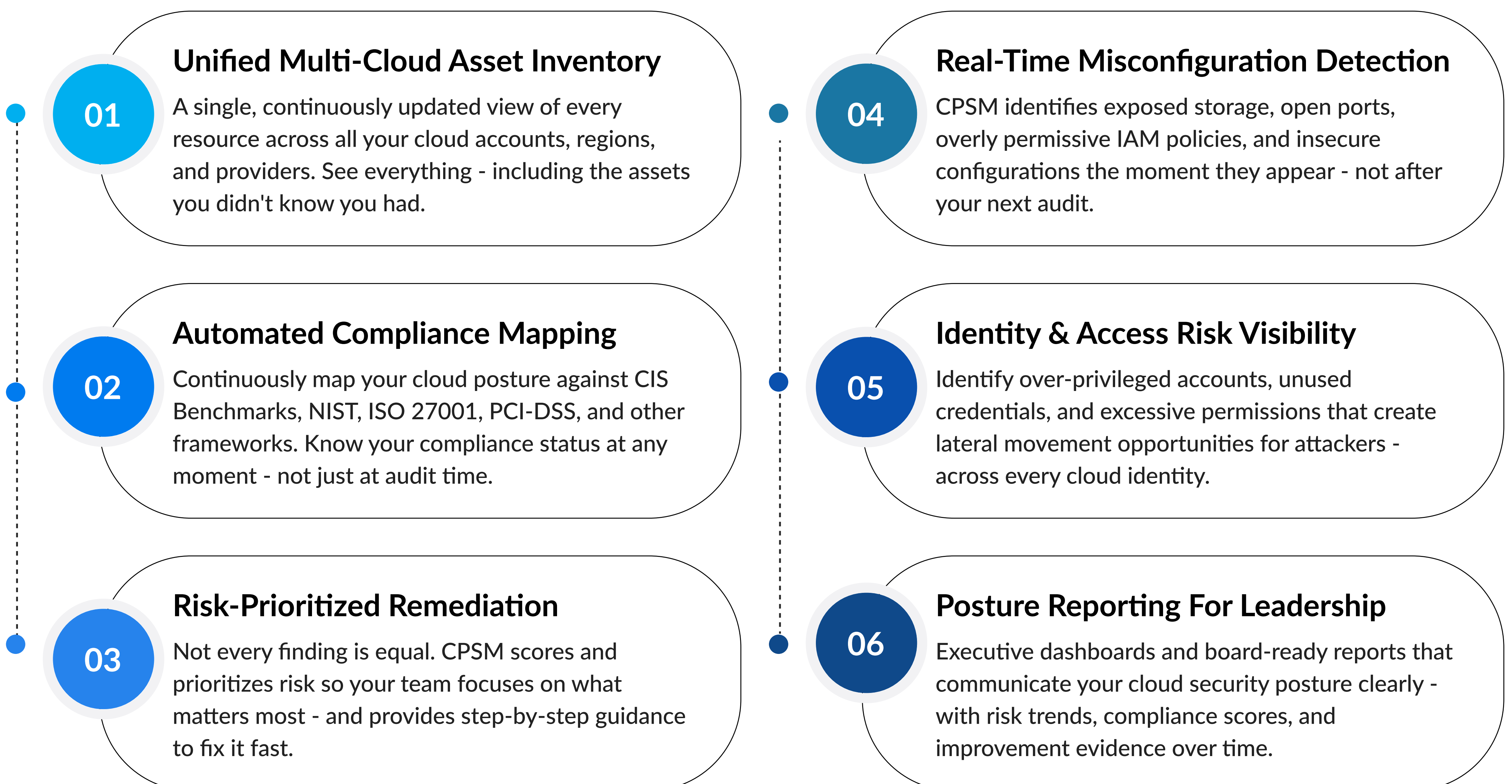
TechOwl CSPM gives your security team complete, real-time visibility into the security posture of your entire cloud environment - across every account, region, and service - and the tools to enforce policy, remediate risk, and demonstrate compliance continuously.

It's not a one-time audit. It's an always-on security layer that watches your cloud the way attackers do - constantly, comprehensively, and without gaps.



PLATFORM CAPABILITIES

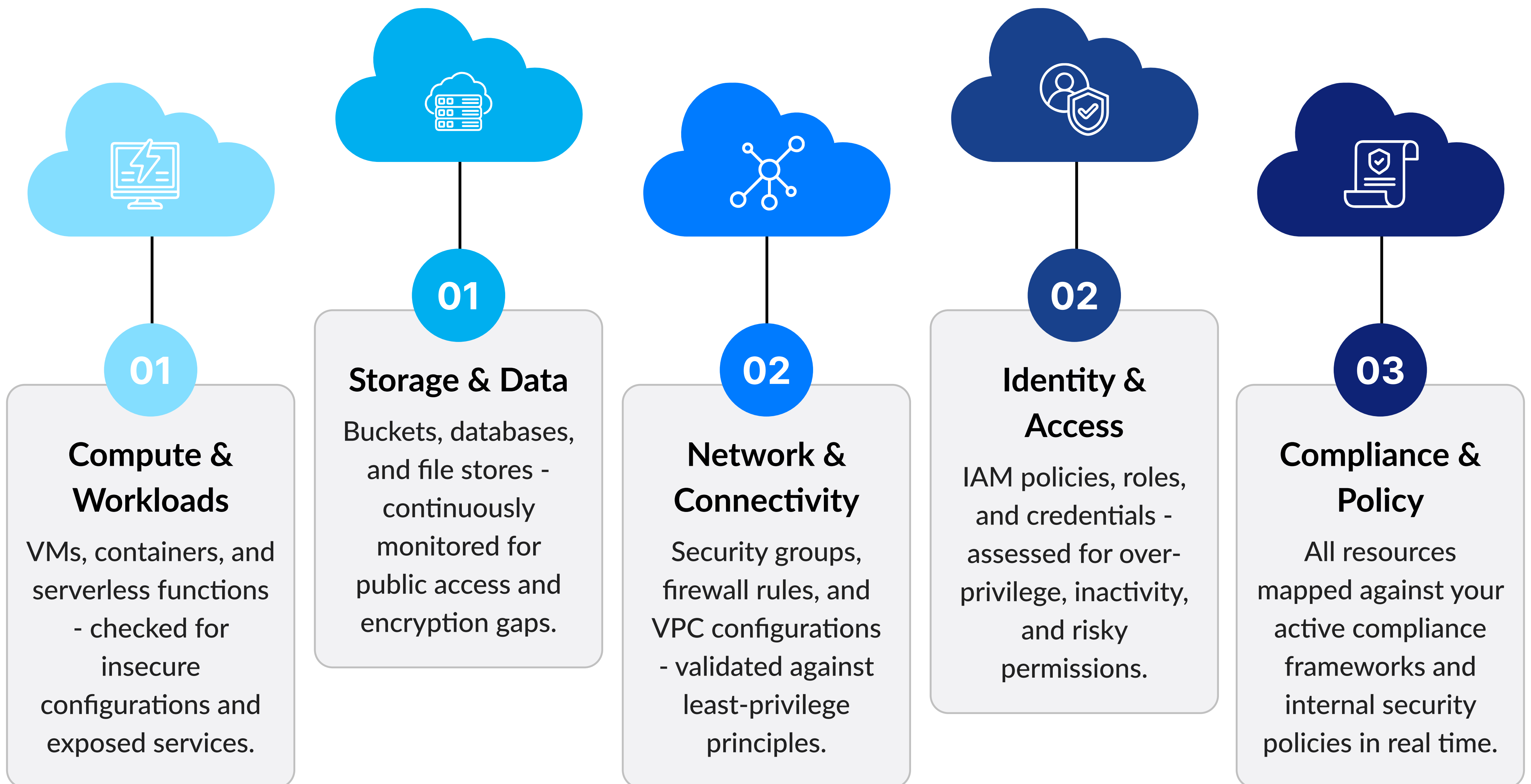
Complete Posture Management Across Your Entire Cloud



COVERAGE

Every Layer of Your Cloud - Continuously Protected

Cloud security risk doesn't live in one place. It spans compute, storage, networking, identity, and data services across multiple providers. CPSM watches all of it.



MULTI-CLOUD SUPPORT

One Platform. Every Cloud.

Your cloud environment doesn't live in one provider - and your security posture management shouldn't either. CPSM delivers consistent, policy-driven security visibility across all major cloud platforms under a single unified view.



Amazon Web Services

EC2, S3, RDS, IAM, Lambda, VPC, CloudTrail, and 100+ services - fully assessed and continuously monitored.

Microsoft Azure

Virtual Machines, Blob Storage, Azure AD, NSGs, Key Vault, and the full Azure service catalog - all in scope.

Google Cloud Platform

GCE, GCS, BigQuery, Cloud IAM, VPC firewall rules, and GCP-native services - monitored with the same rigor.

BUSINESS OUTCOMES

What Changes When Your Cloud Posture Is Under Control



COMPLIANCE & GOVERNANCE

Always Audit-Ready. Never Scrambling.

Compliance in the cloud isn't a point-in-time exercise - it's a continuous commitment. CPSM maps your live cloud posture against the frameworks that matter to your organization and your auditors, all the time.



Cloud compliance is not a one-time snapshot. Regulators increasingly expect organizations to demonstrate that controls are enforced continuously - not assembled for review day.

WHY CLOUDSHIELD

Continuous Posture vs Periodic Audits - There Is No Comparison

A cloud audit tells you where you stood at a point in time. CPSM tells you where you stand right now & alerts you the moment that changes. That difference is what separates organizations that discover breaches from those that prevent them.

NO.	CAPABILITY	TRADITIONAL CLOUD AUDITS	TECHOWL CLOUDSHIELD
1	Point-in-time cloud audits	✓	✓ Continuous, not periodic
2	Multi-cloud support (AWS, Azure, GCP)	✗	✓
3	Real-time misconfiguration detection	✗	✓
4	Automated compliance framework mapping	✗	✓
5	Risk-prioritized remediation guidance	✗	✓
6	Identity & access risk visibility	Limited	✓
7	Asset inventory across all cloud accounts	✗	✓
8	Drift detection & policy enforcement	✗	✓
9	Board-ready posture reporting	Limited	✓
10	Integrated security platform visibility	✗	✓

WHO IT'S FOR

Built for Organizations Running Critical Workloads in the Cloud

Enterprises



Manage security posture across complex multi-account, multi-region cloud environments at scale.

>

BFSI



Meet stringent regulatory mandates for cloud workload security and data protection in financial services.

>

Healthcare



Secure patient data and clinical workloads in cloud environments with continuous compliance assurance.

>

Cloud-Native Teams



Give DevOps and engineering teams guardrails that maintain security without slowing development velocity.

>

Regulated Sectors



Demonstrate cloud security control effectiveness to auditors, regulators, & enterprise customers.

Part of the TechOwl Security Platform

 TechOwl SHIELD Attack Surface Monitoring	 TechOwl DMARC+ Email Trust Assurance	 TechOwl TPRM Third-Party Risk Intelligence	 TechOwl CSPM Cloud Security Visibility
 TechOwl Phishlens Employee Risk Readiness	 TechOwl ThreatPulse Threat Signal Intelligence	 TechOwl ThreatLab Advanced Threat Detonation	 TechOwl Simulens Continuous Breach & Attack Simulation

See Your Cloud Posture - Right Now.

Stop discovering cloud risk after the fact. CSPM gives you the continuous visibility, policy control, and compliance confidence your cloud environment demands.

