



UEMP CSPM

Continuous visibility and posture management across cloud estates.

BRING CLOUD POSTURE INTO THE SAME EXPOSURE PICTURE AS THE REST OF THE ENTERPRISE.

Product Overview

Invinsense UEMP Cloud Security Posture Management (CSPM) connects to cloud accounts, runs posture scans and maps results to compliance frameworks. It provides a common view across AWS, Azure, GCP, Kubernetes and Microsoft 365 and correlates cloud findings with the unified asset inventory. It replaces periodic, manual cloud audits with continuous, automated posture checks, so misconfigurations are closed in hours instead of surviving until the next review cycle.

Key Capabilities

Capability	What It Delivers
Multi-cloud onboarding	Supports AWS, Azure, GCP, Kubernetes and Microsoft 365 with encrypted credentials and asset synchronization.
Posture-check catalog	Maintains checks and map them to applicable frameworks.
Targeted scanning	Runs assessments by severity, service or compliance framework.
Findings and remediation	Presents findings with remediation guidance.
Compliance reporting	Provides framework-level summaries including CIS, PCI DSS, HIPAA and other supported frameworks.
Cloud-to-asset correlation	Links cloud findings to the unified asset inventory.

Business Outcomes



Establish multi-cloud posture visibility.



Identify misconfigurations across cloud services.



Relate findings to compliance frameworks.



Focus scans by severity, service or framework.



Provide remediation guidance and reporting.

Use Cases

- ✓ **Cloud risk visibility**
See misconfigurations in the same asset-centric exposure view.
- ✓ **Targeted assessment**
Focus effort on high-priority services and requirements.
- ✓ **Compliance readiness**
Understand posture findings in relation to applicable frameworks.
- ✓ **Unified remediation**
Coordinate cloud remediation with broader exposure workflows.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation.

Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved.

Gartner®

Infopercept is recognized as a representative vendor in multiple Gartner® reports

- UEMP (Exposure Management)
- AMTD (Preemptive Security)
- AEV (Security Validation)

[Learn More](#) →



Ready to try it out?

Sign up for a demo. Visit infopercept.com/book-a-meeting

Infopercept



Attacker's Mind. Defender's Brain.®

© Infopercept 2026

Contact us at
sos@infopercept.com

For more details visit
[Infopercept.com](https://infopercept.com)

Engage With Us  