

# UEMP ASPM

Secure code, dependencies, secrets, containers and IaC across the development lifecycle.

SECURE THE SOFTWARE LIFECYCLE  
WITHOUT DISCONNECTING SECURITY  
FROM DEVELOPMENT.

## Product Overview

InVinsense UEMP Application Security Posture Management (ASPM) is the DevSecOps engine for application and software supply-chain exposure. It scans repositories across source code, secrets, dependencies, containers and infrastructure as code, then turns results into triaged, remediation-ready findings with reachability-aware analysis, AI assistance and merge-request security gates. It puts security checks directly into the pipelines developers already use, so application risk

## Key Capabilities

| Capability                   | What It Delivers                                                               |
|------------------------------|--------------------------------------------------------------------------------|
| Multi-engine scanning        | Cover SAST, hardcoded secrets, SCA, container and IaC risks.                   |
| SCM integrations             | Integrate GitHub, GitLab, Bitbucket and Azure DevOps.                          |
| AI workaround guidance       | Generate practical workarounds when a patch is unavailable.                    |
| Automated fixes              | Produce targeted fixes and open pull or merge requests for review.             |
| Reachability-aware triage    | Assess whether vulnerable dependencies are reachable and draft VEX statements. |
| VEX management               | Support review, confirmation or override and OpenVEX/PDF export.               |
| Merge-request security gates | Block merges when newly introduced security issues meet defined criteria.      |
| SBOM generation              | Produce repository component inventories for BOM Registry.                     |

## Business Outcomes



Bring application and supply-chain security into one workflow.



Prioritize reachable and meaningful dependency risk.



Accelerate fixes while retaining developer review.



Prevent new issues from entering production through merge gates.



Feed component inventories into BOM Registry.

## Use Cases

- ✓ **Developer-centric security**  
Bring actionable findings into the development workflow.
- ✓ **Risk-aware triage**  
Separate reachable application risk from non-reachable dependency findings.
- ✓ **Shift-left governance**  
Prevent new issues from moving toward production.
- ✓ **Supply-chain visibility**  
Maintain component context across repositories and releases.

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](https://infopercept.com/book-a-meeting)

## Infopercept



Attacker's Mind. Defender's Brain.®

© Infopercept 2026

Contact us at  
[sos@infopercept.com](mailto:sos@infopercept.com)

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

Engage With Us  