

UEMP RBVM

Turn scanner output into
business-prioritized
remediation.

PRIORITIZE WHAT CAN ACTUALLY HURT
THE BUSINESS—NOT SIMPLY WHAT
SCANNERS REPORT.

Product Overview

Invinsense UEMP Risk-Based Vulnerability Management (RBVM) turns scanner output into a prioritized, business-aware remediation queue. It ingests, deduplicates, enriches and scores findings, maps vulnerabilities to assets and attack paths and tracks them to closure against SLAs. It replaces sprawling, undifferentiated vulnerability backlogs with a single risk-ranked queue, so teams fix the handful of issues that actually drive down risk first.

Key Capabilities

Capability	What It Delivers
Multi-scanner ingestion	Ingest Nessus and Acunetix directly and accept Nessus, Acunetix, Nuclei, Trivy and Excel/CSV inputs.
Calibrated risk scoring	Combine severity, EPSS, CISA KEV, known exploit tooling and exposure into a 0-100 score.
SSVC decision support	Derive track, attend or act decisions using published data and business context.
Financial risk	Express risk in monetary terms at vulnerability and organizational levels.
Attack-path analysis	Map vulnerabilities onto network topology and identify routes to critical assets.
Business context	Add asset criticality, network zone, business unit and data classification.
SLA and aging	Track breach or at-risk status, MTTR and compliance trends.
Risk acceptance	Maintain auditable acceptance records with revocation.
Unified inventory	Correlate the same host across scanners into one asset record.

Business Outcomes



Normalize findings from multiple scanners.



Prioritize by exploitability, exposure and business context.



Map vulnerabilities to attack paths and critical assets.



Express risk in business and financial language.



Track SLA, aging, remediation and risk acceptance.

Use Cases

- ✓ **Risk-based queue**
Give teams a prioritized queue instead of an undifferentiated backlog.
- ✓ **Attack-path remediation**
Focus on choke points and routes to critical assets.
- ✓ **Continuous tracking**
Measure aging, SLA performance and remediation progress.
- ✓ **Executive risk**
Translate technical exposure into business and financial language.
- ✓ **Governed exceptions**
Document and control accepted risk.

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  