

UEMP EASM

Outside-in visibility across
your internet-exposed digital
footprint.

KNOW WHAT THE INTERNET CAN SEE
ABOUT YOUR ORGANIZATION—AND ACT
BEFORE ATTACKERS DO.

Product Overview

Invinsense UEMP External Attack Surface Management (EASM) provides an outside-in view of what is exposed to the internet. It continuously discovers and monitors domains, subdomains, IPs and exposed services, adding vulnerability, certificate, technology, data-exposure and brand-security context. It replaces slow, manual reconnaissance with continuous, evidence-backed discovery, so exposure is confirmed and actionable within hours, not weeks.

Key Capabilities

Capability	What It Delivers
Domain and asset discovery	Discover related subdomains, IP ranges and associated domains, including M&A domains.
Active vulnerability scanning	Scan discovered assets for exposed vulnerabilities, misconfigurations and services.
CVE verification	Validate potential vulnerabilities to filter false positives and confirm exposure.
Email security checks	Check SPF, DKIM and DMARC records posture.
SSL/TLS analysis	Review expiry, weak ciphers and certificate misconfigurations.
Technology fingerprinting	Identify technologies and compare them with newly published vulnerabilities.
Exposed secrets	Detect credentials and secrets exposed directly on the live surface.
Change tracking	Record new or removed subdomains, opened ports and certificate rotations.
Service validation	Confirm exposed services with supporting evidence.
Data and brand exposure	Monitor leaked credentials, stolen sessions, dark-web, ransomware, public code, cloud storage, Postman exposure and brand impersonation.

Business Outcomes



Discover external assets and services continuously.



Validate exposure instead of producing raw findings.



Identify leaked credentials, stolen sessions and exposed secrets.



Monitor dark-web, ransomware and public-code exposure.



Detect brand impersonation and phishing.



Track changes across the external footprint.

Use Cases

- ✓ **External asset visibility**
Maintain a current view of the internet-facing footprint.
- ✓ **Threat exposure monitoring**
Identify credentials, sessions and secrets that may enable compromise.
- ✓ **Continuous change awareness**
Track new assets, services and certificates as the footprint evolves.
- ✓ **Exposure validation**
Provide evidence-backed findings for remediation.
- ✓ **Brand protection**
Detect typosquatting, phishing pages and impersonating profiles.

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  