

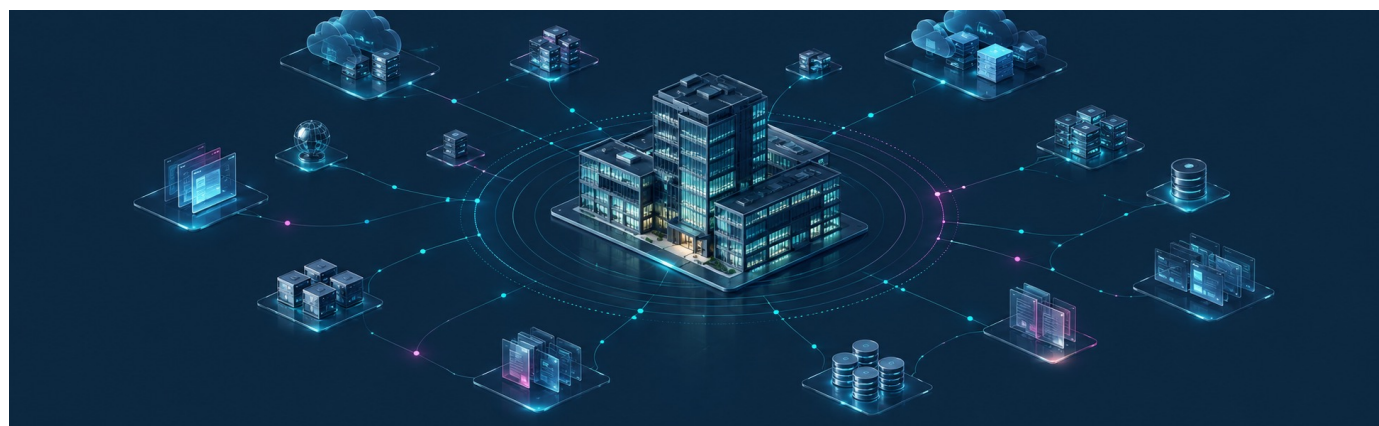
EASM



External Attack Surface Management

Cyber intelligence with asset-level technical evidence

Discover your organization's externally observable assets, correlate exposure signals and turn technical findings into clear security priorities.



Domains, IPs, exposed services, cloud assets and observed technologies



Asset inventory

Review domains, subdomains, IPs, cloud services and observed technologies in one organization view.



Technical evidence

Inspect asset-level findings, CVE context and exposed-data signals behind risk scores.



Exposure changes

Follow asset changes and new risk signals. Use alerts and remediation guidance to focus the team's response.

Intelligence-based assessment

Coinnect correlates available cyber intelligence to deliver assessments near real time, without agents, credentials, internal access or target participation. Security teams can review exposure without a deployment project, then use asset-level evidence and remediation guidance to prioritize action. This reduces operational effort and enables repeatable risk reviews.

Technical capabilities

Each finding connects an asset to its exposure context, so your team can inspect the evidence, understand its relevance and assign a remediation priority.

External asset inventory

An inventory of domains, subdomains, IPs and cloud-facing services, with observed technologies. Identify assets missing from internal inventories.

Vulnerability & CVE context

Asset-linked CVE context and configuration indicators. Inspect affected assets and distinguish observed evidence from technology-based inference.

Credentials & brand exposure

Exposed credentials, breach and botnet intelligence associated with the organization. Lookalike-domain monitoring highlights potential brand abuse.

Technology & dependencies

Observed software, cloud, hosting and IT-provider relationships. Identify legacy technologies and exposed OT or IoT where observable.

Cyber Risk Score

Risk scores with affected-asset evidence and AI-assisted explanations. Review why a finding matters and use guidance to prioritize remediation.

Monitoring & data export

Exposure changes, new risk signals and alerts. Export reports and data for operational review, management reporting and follow-up.

Optional TPRM module

Third-Party Risk Management

Extend EASM to suppliers and service providers. Compare supplier exposure, review observable fourth-party dependencies and identify concentration across shared technologies or providers.

Independent assessment

Assess suppliers without initial participation. Use asset-level findings and portfolio views to prioritize exposure and identify shared-provider dependencies.

Collaborative remediation

Add questionnaires and invite suppliers to review technical findings. Coordinate remediation and track improvements through the collaboration workflow.

