

APIs - MCP

for EASM + TPRM



Cyber exposure, built into your platform.

Embed Coinnect's proprietary EASM and TPRM capabilities into your products, customer portals and managed services through **APIs** and **MCP**.



Organizations, suppliers and shared digital dependencies. Connected to your product experience.



Assess on demand

Evaluate organizations and suppliers from available intelligence, without agents, credentials or initial target participation.



Bring the evidence

Retrieve asset inventories, exposure findings, CVE context and risk scores for your own dashboards and workflows.



Monitor change

Track new exposure and supplier-risk changes to support alerts, recurring services and remediation follow-up.

EASM and TPRM, ready to embed

EASM

External Attack Surface Management

Discover domains, IPs and cloud-facing services. Correlate observed technologies, configuration indicators and exposed-data signals with asset-level risk evidence.

TPRM

Third-Party Risk Monitoring

Assess suppliers and service providers. Compare risk across portfolios, map observable fourth-party dependencies and identify shared-provider concentration.

Extend your offering. Keep your experience.

Add external exposure and supplier-risk services without developing and maintaining a separate assessment engine. Keep your customer interface and workflows, while Coinnect provides the underlying EASM and TPRM technology.

Integrate. Differentiate. Deliver.

Choose the interface that fits your workflows and the partnership model that fits your business.

EASM & TPRM APIs

APPLICATIONS & WORKFLOWS

Use REST APIs to request assessments and retrieve status, results, asset-level evidence and supplier-risk data. Feed dashboards, alerts and workflows. Asynchronous jobs, webhooks and data exports can be included in the agreed integration scope.

Both interfaces connect to Coinnect technology. Tools, permissions and consumption limits are scoped per integration.

EASM & TPRM via MCP

AI AGENTS & COPILOTS

Connect AI agents and copilots to selected EASM and TPRM functions through Model Context Protocol. Retrieve existing assessments, inspect exposure evidence and investigate supplier risk. Authorized tools can also request new assessments within agreed permissions and quotas.

Built for your market

Cybersecurity vendors

Enrich SIEM, XDR, SOAR and vulnerability workflows with external exposure evidence.

Risk & compliance vendors

Add technical assessments and supplier monitoring to GRC and due-diligence workflows.

MSP / MSSP

Power multi-customer portals, managed exposure services and client reporting.



Choose how you go to market

Technology integration

Embed capabilities in your product with Coinnect attribution or co-branding, as agreed.

OEM / White label

Commercialize EASM and TPRM under your brand and product experience, with agreed redistribution rights.

Managed services

Bundle assessments and monitoring into recurring services for multiple end customers.

Licensing aligned to your scale

Annual or multi-year agreements. EASM: assets and domains. TPRM: third parties. Volume, usage and OEM terms defined by agreement.

Let's build your next capability.

Talk to Coinnect about integration scope, branding and licensing.