

AI-Driven Risk Prioritization Powered by Liongard Intelligence

Cut through noisy vulnerability data with prioritized, business-aligned risks derived directly from Liongard's deep asset intelligence. With passive scanning, live threat intelligence, and smart context, ThreatImpactIQ helps teams act faster, prove defensibility, and strengthen security without adding another heavy tool to the stack.

What It Delivers



Continuous Risk Monitoring

Uses Liongard's continuously updated asset data to identify vulnerabilities through passive analysis and automatically reopen risks if they return.



Contextual Risk Scoring

Applies business context, threat activity, and environment intelligence to prioritize vulnerabilities by real-world impact, not just CVSS scores.



Remediation Workflow

Send AI-suggested actions to Jira, ServiceNow, ConnectWise, or internal teams. Supports mitigation, acceptance, and deviation tracking.



Evidence-Ready Reporting

Generate clear, defensible reports that show identified risks, remediation progress, and overall security posture.



"Visibility is power—knowing when something changes can mean the difference between security and disaster. Liongard gives us that edge."

Matthew Woehrl
IT Systems Administrator
Flagship Networks



About Liongard

Liongard is redefining Attack Surface Management with an intelligent, AI-powered platform built for modern IT and security operations. Trusted by MSPs, MSSPs, and IT providers to protect over 70,000 end customers, Liongard delivers unified visibility across users, systems, networks, and cloud environments. With over 85 integrations, Liongard empowers teams to uncover hidden risks, enforce cybersecurity posture, and automate the actions that matter most. By combining deep asset intelligence with real-time insight and scalable remediation, Liongard fuels cyber resilience, operational efficiency, and sustainable growth.



Why It's a Game Changer

● Powered by Liongard Asset Intelligence

ThreatImpactIQ's direct integration with LiongardIQ uses Liongard's continuously updated asset and configuration data to identify vulnerabilities through passive analysis.

This isn't just another scanner. ThreatImpactIQ delivers a true vulnerability management process. Live threat intel and business context are applied continuously so you see real risk, prioritize what matters, and take action faster, generating outcomes, not alerts.

● Optional: Expand with Traditional VM Tools

For organizations using platforms like Tenable or Rapid7, ThreatImpactIQ can ingest those scan results alongside Liongard data. This unlocks deeper capabilities such as compliance validation, web application scanning, and more complete software-level vulnerability detection.

These tools enhance visibility and compliance coverage, but are not required for ThreatImpactIQ to deliver meaningful risk insights, remediation tracking, and posture reporting powered by Liongard's asset intelligence.

Purpose-Built For



Security-Driven QBRs

Show measurable risk reduction.



vCISO Programs

Prioritize and track remediation plans.



Cyber Insurance Readiness

Provide defensible posture evidence.



Operational Efficiency

Eliminate noise, reduce analyst fatigue.

Why It Matters



Prioritize What Matters

Focus on the vulnerabilities that pose real-world threats, not endless CVEs.



Cut Time to Resolution

Save hours with auto-updating risk states, enriched context, and structured workflows.



Deliver Proof, Not Promises

Show exactly how risk was reduced with defensible reports and remediation logs.



Scale Without Overhead

Automate context, prioritization, and reporting across every client.

► Ready to Stengthen Your Security Posture?

Contact your Liongard Representative to see how ThreatImpactIQ helps reduce risk, enforce best practices, and eliminate the guesswork in vulnerability remediation.