ThreatImpactIQ

LiongardIQ Data vs. Vulnerability Scanner Data

One Platform. One Risk Engine. Different Visibility.

ThreatImpactIQ prioritizes risk severity at the device level. What changes is **how devices are discovered and kept current inside the platform.**

- When ThreatImpactIQ is fed by **vulnerability scanner data,** risk is prioritized based on point-in-time **scan results.**
- When ThreatImpactIQ is fed by **LiongardIQ data**, risk is prioritized based on **continuous awareness of the environment.**

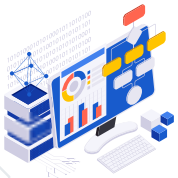
Same engine.
Different visibility.

What ThreatImpactIQ Does

ThreatImpactIQ evaluates risk at the **device / system level.**

Each device is assessed using:

- Software and version data
- Known vulnerabilities (CVE/CPE mapping)
- Threat intelligence (KEV, EPSS, exploit maturity)
- Business impact weighting



The outcome is:

- A prioritized list of device risk
- Clear remediation guidance
- Governance and audit-ready artifacts

This does not change based on data source.

> "Visibility is power—knowing when something changes can mean the difference between security and disaster. Liongard gives us that edge."
>
> Matthew Woehrle
> IT Systems Administrator
> Flagship Networks

FLAGSHIP

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.

liongard

How Device Visibility Differs

• ThreatImpactIQ + LiongardIQ Data

How devices appear

- Devices are identified through continuous discovery.
- Device risk is assessed within the context of the IT Environment.
- Records update automatically as changes occur.

What this means

- Device inventory is more complete.
- Risk visibility updates as the environment changes.
- Risk reflects **current operational reality.**
- Earlier and broader risk awareness

Best for: continuous risk awareness.

• ThreatImpactIQ + Vulnerability Scanner Data

How devices appear

- Devices are identified when a scanner reports them.
- Visibility depends on:
  - o Scan scope
  - o Credentials
  - o Scan frequency

What this means

- Devices outside scan scope are not evaluated.
- Risk visibility updates on scan cadence.
- Risk reflects a **point-in-time snapshot.**

Best for: validated vulnerability confirmation.

The Key Difference

Scanners tell ThreatImpactIQ what was scanned.
LiongardIQ tells ThreatImpactIQ what exists, period.

Both feed the same prioritization engine.
One is **scan-driven.**
One is **environment-driven.**

Why It Matters

Modern IT environments:
· Change constantly
· Are rarely fully documented
· Often include unknown or inherited devices

Relying only on scans can lead to:
· Alert fatigue
· Low-priority noise
· Blind spots between scans

Using LiongardIQ with ThreatImpactIQ helps ensure:
· Devices aren't missed
· Risk is evaluated sooner
· Prioritization starts from a more complete picture

▶ ThreatImpactIQ + LiongardIQ helps teams prioritize device risk based on what exists today, not just what was scanned.

Contact your Liongard Representative

www.liongard.com

liongard