

The Fragmentation Crisis

As organizations adopt more technologies to manage and secure modern IT environments, the operational reality becomes fragmented. The result is a growing gap between what teams believe exists and what actually exists.

TOOL SPRAWL

As environments grow, organizations accumulate dozens of operational and security tools. Each system operates in isolation, creating fragmented visibility and slowing response times.



UNRELIABLE DATA

Asset and configuration data quickly becomes outdated or inconsistent across systems, forcing teams to reconcile conflicting information before they can take action.



SECURITY BLIND SPOTS

When visibility is fragmented, hidden assets, misconfigurations, and unmanaged change introduce risk that often goes undetected until it becomes an incident.



OPERATIONAL FRICTION

Teams spend significant time gathering information across tools, validating data, and manually documenting environments instead of focusing on higher-value operational and security work.



LiongardIQ: The System of Authority for Asset Intelligence

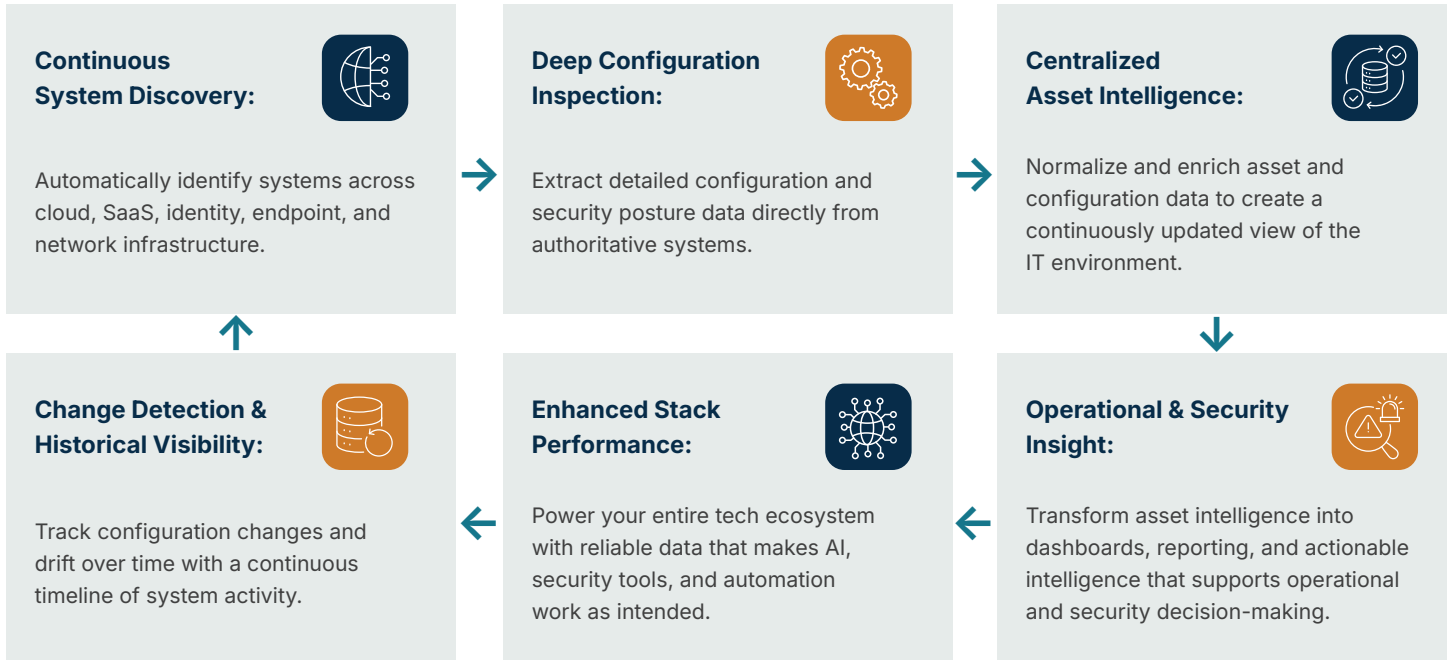
LiongardIQ establishes a system of authority for asset intelligence by continuously discovering, inspecting, and monitoring systems across the IT environment. Instead of relying on fragmented tools that each maintain a partial view of the environment, LiongardIQ centralizes asset intelligence into a continuously updated, authoritative understanding of what exists, how it is configured, how it changes, and what risk it introduces.

By connecting directly to core systems across cloud, SaaS, identity, endpoint, network, and security platforms, LiongardIQ performs deep inspection to collect structured configuration, identity, and asset data. This information is normalized, enriched, and continuously validated to create a trusted operational view of the environment.

The result is a **unified intelligence layer** that enables teams to operate with confidence through providing the visibility, context, and automation required to manage complex environments efficiently and securely.

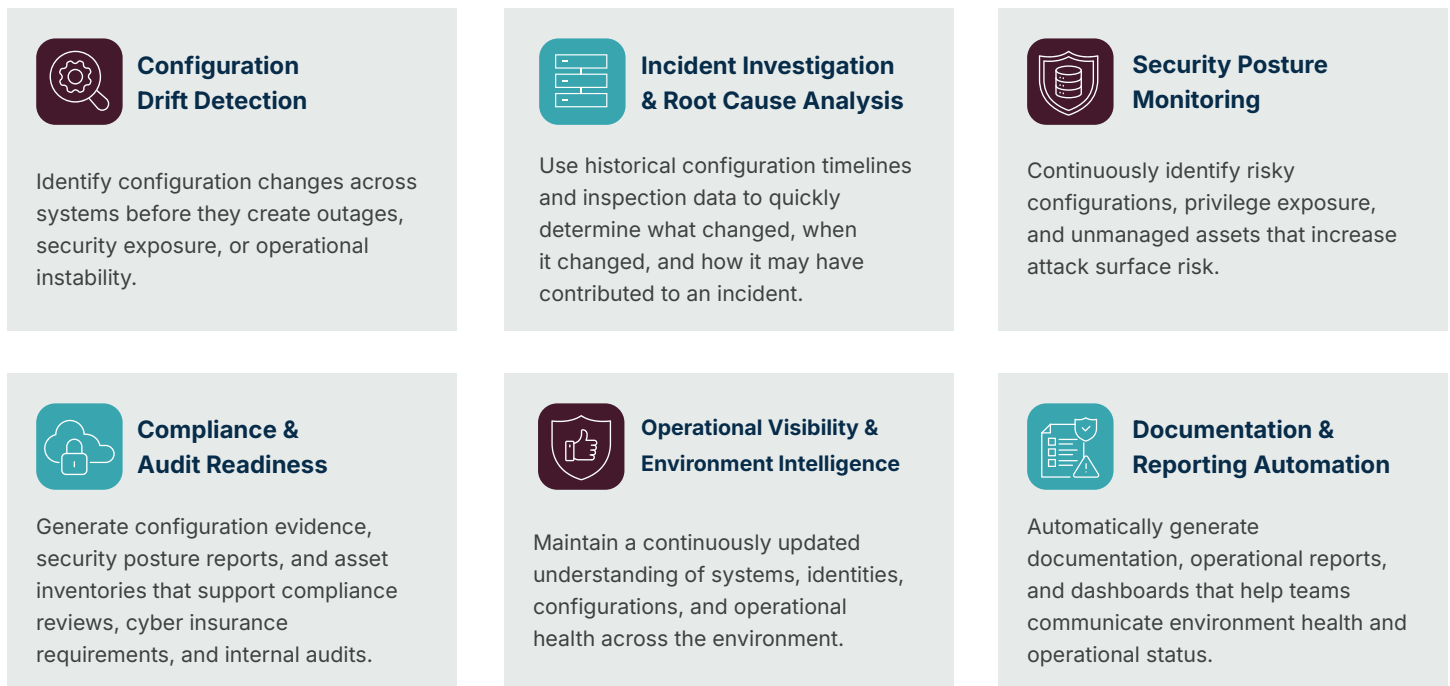
How LiongardIQ Works

Discover → Inspect → Monitor → Surface Insight



Operational Use Cases

LiongardIQ supports a wide range of operational and security workflows by continuously analyzing configuration and asset data across integrated systems.



LiongardIQ Platform Capabilities

ASSET DISCOVERY & INVENTORY

Identity Discovery & Inventory	Identity discovery triangulated across System Inspections with enriched and deduplicated Inventory with identity asset data fields and tagging capabilities.
Device Discovery & Inventory	Device discovery triangulated across System Inspections and native Network Discovery with enriched and deduplicated Inventory with device asset data fields and tagging capabilities. This covers Windows, Mac, Linux, virtualized, network & IoT infrastructure.
Software Discovery & Inventory	Identify installed software across systems to maintain visibility into applications present throughout client environments.
Data Discovery & Inventory	Discover and catalog locations where organizational data resides to improve visibility into data storage across systems.
Device Status Monitoring	Track operational status and metadata for network devices to maintain visibility into device availability and operational state.

SYSTEM INSPECTION & CONFIGURATION INTELLIGENCE

System Inspections	Perform automated inspections of integrated systems to collect structured configuration, operational, and security data directly from authoritative platforms.
Configuration Sync	Synchronize collected configuration data with external documentation platforms to ensure documentation systems remain aligned with live environment data.
Pre-built Metric Queries	Access a library of predefined queries that retrieve configuration, operational, and security data collected through Liongard inspections across integrated systems.
Custom Metric Queries	Use JMESPath-based queries to extract additional configuration or operational data from inspection results. Queries can be created manually or generated with AI assistance to quickly retrieve specific data points beyond the predefined query library.
Configuration Change Detection	Identify configuration drift by comparing inspection results across historical inspection runs to detect changes in system configuration and operational state.
Historical Configuration Timeline	Maintain a historical record of configuration states and inspection results to support auditing, troubleshooting, and operational analysis.
Automated Documentation	Generate documentation directly from inspection and configuration data to maintain continuously updated records of systems, settings, and operational details.
Custom Alerts	Define alert conditions based on inspection results or configuration changes to notify teams when meaningful operational or security changes occur.
Global Asset & Configuration Search	Instantly search across collected asset, configuration, and inspection data to locate systems, users, settings, and operational intelligence across the entire environment.
Risk Scoring & Prioritization <i>*ThreatImpactIQ Add-On</i>	Analyze asset intelligence and configuration data to identify and prioritize security exposures based on operational and security impact.

VULNERABILITY INTELLIGENCE

Configuration-Based Vulnerability Detection	Identify security exposures caused by misconfigurations, risky permissions, insecure system settings, and outdated software versions discovered through continuous system inspections.
--	--

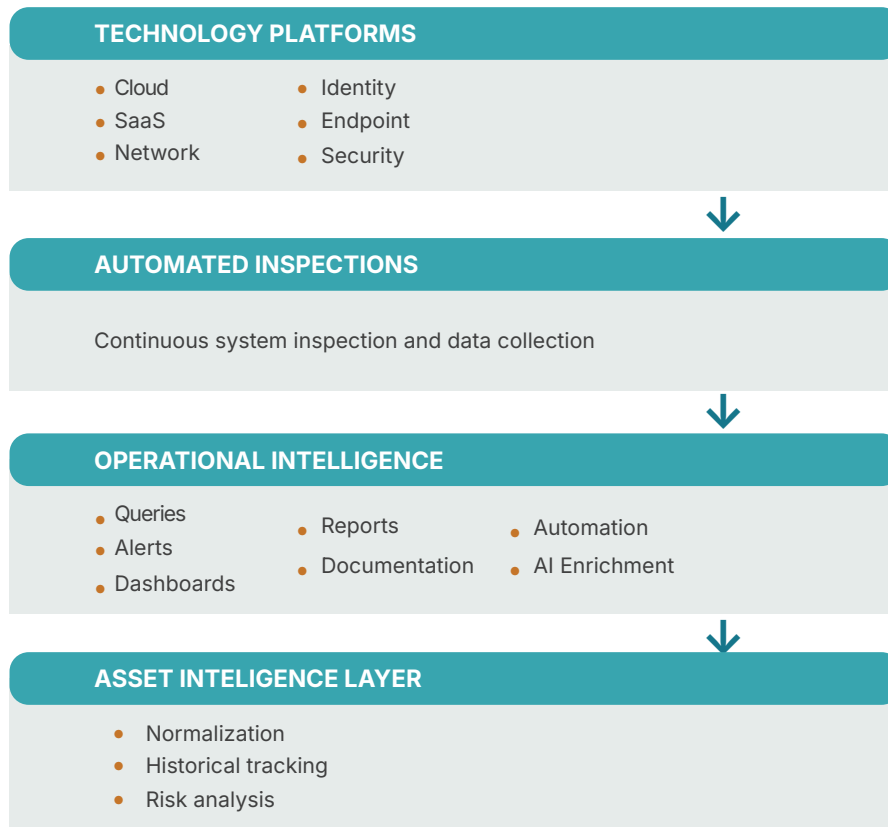
Vulnerability Risk Correlation <i>*ThreatImpactIQ Add-On</i>	Correlate asset intelligence with vulnerability data and threat intelligence sources to identify exposures across the environment.
Risk Scoring & Prioritization <i>*ThreatImpactIQ Add-On</i>	Prioritize vulnerabilities based on exploit likelihood, severity, and potential business impact to focus remediation efforts.
Remediation Workflow Coordination <i>*ThreatImpactIQ Add-On</i>	Initiate remediation actions and coordinate mitigation efforts across teams and systems.
Risk & Vulnerability Reporting <i>*ThreatImpactIQ Add-On</i>	Generate structured reports summarizing vulnerability posture and remediation progress across the environment.
REPORTING & DATA VISUALIZATION	
Cyber Risk Dashboard	Provide a centralized view of security posture aligned to foundational cyber insurance readiness controls. The dashboard highlights configuration conditions that impact insurability and supports exportable reporting for internal assessments and external validation.
Prebuilt Dashboards	Access prebuilt dashboards that visualize operational and security insights derived from Liongard inspection and asset intelligence data with Visual Insights.
Custom Dashboards	Create custom dashboards to visualize configuration data, inspection results, and operational metrics relevant to specific teams or workflows with Visual Insights.
Tabular Reports	Generate structured tabular reports from inspection data to support operational reviews, compliance assessments, and documentation. Reports can include asset inventories, identity and account audits, devices security posture assessments, configuration audits, licensing summaries, and compliance-aligned reports such as CIS Controls and cyber insurance evaluations.
Unified Asset Inventory Reporting	Generate exportable device and identity inventories built from LiongardIQ's normalized asset intelligence model. Assets discovered across multiple integrated systems are automatically correlated and deduplicated into centralized inventories for reporting, operational analysis, and audit workflows.
Cross-Platform Reporting <i>*Visual Insights Pro Add-On</i>	Combine LiongardIQ inspection data with information from external operational platforms such as Autotask, ConnectWise, QuickBooks, and other business systems to create unified dashboards, analytics, and operational reports.
Compliance Evidence Collection	Generate exportable reports and system intelligence that support compliance reviews, cyber insurance assessments, and security audits. Liongard provides evidence of asset inventories, configuration states, and historical system activity, including up to 18 months of visual change history.
Security Posture Reports <i>*ThreatImpactIQ Add-On</i>	Generate structured reports that summarize configuration risk and security posture across systems for operational reviews, cyber insurance defensibility, and audit workflows.
AI & INTELLIGENCE CAPABILITIES	
AI Conversational Enriched Search	Interact with LiongardIQ using natural language to explore environment data, assets, and configuration intelligence. Ask questions about systems, users, configurations, and risk exposure, and receive contextual insights that can be refined through follow-up queries with Roar Assistant.
AI Query Companion	Use AI to assist with building and refining structured queries (metrics) across LiongardIQ inspection data. AI helps generate queries, interpret results, and accelerate investigation without requiring manual query construction.

AI Asset Summaries	Automatically generate contextual summaries of systems, assets, and environments using LiongardIQ's inspection and configuration data. These summaries help teams quickly understand system health, security posture, and operational context without manually reviewing raw configuration data.
MCP Server Access <i>*Paid Add-On</i>	Access LiongardIQ asset intelligence through the Model Context Protocol (MCP) server, enabling partners to securely connect Liongard data to AI agents, automation workflows, and developer tools.
PLATFORM INTEGRATIONS & EXTENSIBILITY	
System Integrations	Connect LiongardIQ to cloud, SaaS, identity, endpoint, and network platforms to collect inspection and asset intelligence across the environment.
API Access	Programmatically access Liongard data to build custom integrations, reporting pipelines, and automation workflows. This gives access to LiongardIQ's data lake and cached queries (metrics).
Core Configuration & Flexible Asset Sync	Synchronize configuration and asset intelligence data to external documentation systems.

Platform Architecture

LiongardIQ functions as an intelligence layer across the IT environment. Through automated inspections and integrations, the platform collects, normalizes, and analyzes configuration and asset data to create a continuously updated operational view.

Architecture flow



Platform Coverage

Liongard integrates with more than 100 products across cloud infrastructure, SaaS applications, identity providers, endpoints, network devices, and operational systems. Through these integrations, LiongardIQ continuously collects configuration, identity, and asset intelligence to maintain an accurate operational view of the environment.

105+ Integration Partners Across The Stack



Security & Data Protection

LiongardIQ is built with a multi-layered security architecture designed to protect customer data and ensure platform reliability. The platform follows industry best practices for encryption, infrastructure security, secure development, and operational governance.

Data Encryption

All data is encrypted in transit using HTTPS. Encryption controls ensure that only authorized users can access collected system intelligence.

Secure Platform Architecture

The LiongardIQ platform operates on a hardened Linux environment with no open ports or listening services, reducing attack surface and strengthening platform resilience.

Network & Infrastructure Protection

The platform is protected by advanced firewalls, intrusion detection and prevention systems (IDS/IPS), and secure cloud infrastructure designed to prevent unauthorized access.

Compliance & Independent Audits

LiongardIQ undergoes regular third-party audits and maintains SOC 2 Type 2 compliance, with controls aligned to frameworks such as HIPAA and PCI.

Secure Development Practices

The LiongardIQ platform operates on a hardened Linux environment with no open ports or listening services, reducing attack surface and strengthening platform resilience.

Secure AI Processing

AI-powered capabilities such as Roar Assistant and Enriched Search operate using secure processing through AWS Bedrock. Data used to generate AI responses is encrypted in transit, processed within secure AWS infrastructure, and is not retained or used to train external AI models. AI responses follow LiongardIQ's existing permission model and can be enabled or disabled at the Environment level.

Operational Resilience

Business continuity planning, incident response procedures, and vendor risk management practices help ensure platform availability and operational integrity.

Deployment & Implementation

LiongardIQ is designed for fast deployment and immediate operational visibility.

Organizations connect LiongardIQ to systems across their technology stack through secure integrations. Once connected, LiongardIQ begins collecting configuration, identity, and asset intelligence directly from integrated platforms.

As systems are connected, LiongardIQ continuously builds an understanding of the environment, providing visibility into assets, configurations, and system changes over time.

This approach allows teams to quickly establish operational insight without requiring significant infrastructure changes or manual documentation efforts.

LiongardIQ can be deployed across environments of any size and begins delivering value shortly after systems are connected.

Establish Your System of Authority for Asset Intelligence

Liongard enables organizations to operate complex technology environments with greater visibility, automation, and confidence. By continuously collecting and analyzing configuration, identity, and asset intelligence across systems, LiongardIQ provides the trusted operational foundation teams need to manage risk, streamline operations, and scale efficiently.

With LiongardIQ, organizations can:

- Establish a trusted source of asset intelligence
- Detect configuration drift and operational risk earlier
- Reduce manual operational work and documentation
- Improve the effectiveness of security and automation tools
- Operate complex environments with confidence

Learn More

To learn more about how Liongard can help your organization improve visibility, automation, and operational intelligence across the technology stack, visit liongard.com or schedule a demo with the Liongard team.

[Schedule your discovery call now!](#)

