liongard IQ

TOOLKIT

ATTACK SURFACE MANAGEMENT MONETIZATION TOOLKIT

Your Plug-and-Play Guide to Launching, Selling, and Scaling Proactive Security Services with LiongardIQ

Powered by Liongard

Why Attack Surface Management Is Critical

The Problem: Your Clients' Attack Surfaces Are Exploding

Cloud apps, remote work, shadow IT, misconfigured SaaS – your clients are adding new assets daily. Most go untracked.

82%
of organizations lack full visibility into their IT environment

(Bedrock Security)

76%
of breaches stem from misconfigured or unmonitored assets

(Verizon Data Breach Report)

$5M+
avg. cost of a data breach in 2024

(IBM Cost of a Data Breach Report)

Why You Must Shift Left of Boom

Attack Surface Management helps you shift left of breach, **before the damage is done**, with visibility, context, and control.

liongard

LiongardIQ Turns ASM Into a Scalable Service Model

Proactive Security with **LiongardIQ**	Legacy, Reactive Security
Continuous asset discovery	*Point-in-time scanning*
Always-on configuration monitoring	*No visibility between scans*
Unified identity + device visibility	*Siloed alerts with missing context*
AI-powered risk detection	*Static vulnerability reports*
Audit-ready documentation	*Scrambling for compliance*
Automated remediation for misconfigs	*Manual response required for known issues*

LiongardIQ = More Than Visibility, It's a Revenue Engine

- **Turn insight into income** with proactive security, compliance, and advisory services
- Enables compliance with frameworks: **CIS, NIST, SOC 2, HIPAA, GDPR**
- Helps clients **qualify for cyber insurance** by proving visibility and controls

The Bottom Line

You can't secure what you can't see.

ASM gives you that visibility—and turns it into MRR.

How To Should Position ASM for Customers

1 Visibility Isn't Optional, It's Foundational

You can't secure what you don't know exists.

Most organizations only protect the assets they're aware of, but it's the unknown, unmanaged, and misconfigured assets that open the door to breaches.

Real-World Examples:

- A forgotten cloud server exposed to the internet
- A misconfigured API leaking sensitive data

Key Message

We continuously monitor your IT environment, tracking users, devices, and configurations, to spot security gaps before attackers do. With AI-driven insights and prioritized alerts, we take action before small issues become serious risks.

Talk Track:

"Attackers are scanning for your vulnerabilities 24/7. Shouldn't you be doing the same?"

liongard

2 ASM for Compliance & Cyber Insurance Readiness

Modern compliance frameworks (SOC 2, HIPAA, CIS CSC, NIST) and cyber insurers now expect businesses to prove:

- They know what's on their network
- They're continuously monitoring and documenting changes

Key Message:

ASM supports both compliance and insurability. It's a critical component for passing audits and qualifying for lower cyber insurance premiums.

Talk Track:

"Cyber insurers are raising premiums – and denying claims – when you can't prove asset visibility. ASM ensures you're covered."

3 Attack Surface Management vs. Traditional Vulnerability Scanning

Many clients confuse ASM with point-in-time vuln scans. Here's how to clearly differentiate:

Vulnerability Scanning	Attack Surface Management
Scheduled snapshots	**Real-time monitoring**
Known assets only	**Finds shadow IT, misconfigs, & APIs**
One-time results	**Continuous discovery & risk detection**

Key Message:

ASM goes beyond scanning: it helps you uncover *what you don't even know to scan.*

Talk Track:

"Scanning tools check for weaknesses, ASM checks for *blind spots*. That's where attackers strike."

4 The Cost of Doing Nothing

Hidden Risk	What It Costs
Exposed API	Data leak, compliance fine
Untracked asset	Entry point for ransomware
Manual audits	Time + labor costs
Failed audit	Business disruption, lost trust

ASM automates the work, prevents the risk, and pays for itself.

- Helps avoid $100K+ in breach costs
- Keeps clients audit-ready for SOC 2, HIPAA, GDPR

5 Offer a Free Risk Visibility Assessment

"Let us scan your attack surface for free. We'll show you what attackers already see."
What the Free Assessment Could Include:

- Discovery of unknown assets (e.g., forgotten domains, shadow IT, orphaned cloud instances)
- Verification of key identity risks (e.g., inactive users, missing MFA)
- Configuration baseline audit (e.g., insecure settings, policy drift)
- SSL/TLS and external service checks
- Optional: Dark web scan for exposed credentials

Use the assessment to:

- Reveal unknown risks
- Build urgency
- Justify recurring ASMaaS service

Great for pre-sales, periodic business reviews, or cross-sell moments.

ASM Readiness Checklist

If you check 4 or fewer… ASM is not optional.

Use this checklist to assess whether your organization (or your client's) is ready for Attack Surface Management.

Do You Have Full Visibility Into…?

Area	What It Costs	[ ]
Identities & Privileged Access	Can you continuously track all users, admins, service accounts-across systems?	
Shadow IT & SaaS Apps	Are you aware of all cloud apps and services your team uses?	
Endpoint & Remote Devices	Can you identify every device accessing your network (on-site, remote, BYOD)?	
Configurations & Drift	Are you alerted when critical settings change across platforms?	
Public-Facing Assets	Do you monitor internet domains, SSL certs, and exposed services continuously?	
Access Controls & MFA	Can you verify MFA and region access settings across Microsoft 365, Google Workspace and others?	
Compliance Posture	Are you audit-ready with automated, up-to-date documentation for evidence?	
Change History	Do you have a timeline of changes to help with investigations or reviews?	

Score Yourself

- **0–4 boxes checked:** High risk. ASM is critical for visibility and protection.
- **5–6 boxes checked:** Progressing, but vulnerable to blind spots.
- **7–8 boxes checked:** Strong posture – ASM can help you maintain it automatically.

liongard

Turn ASM Into Revenue: 6 Ways to Monetize With LiongardIQ

LiongardIQ makes attack surface management a service you can sell: powered by real-time alerts, remediation, AI insights, and more. Use these six plays to package and price it as standalone, bundled, or tiered offerings across your client base.

1 Standalone ASM Service

- Offer as a subscription for continuous visibility and control
- Ideal for compliance-driven, cloud-heavy, or regulated clients
- Delivered with monthly or quarterly reports + real-time drift alerts

Why It Works
Easy to launch. Pairs well with vCISO or advisory services.

2 ASM + MDR/XDR Bundle

- Feed real-time asset data from directly into your detection stack
- Reduces false positives by providing complete, accurate context
- Create a premium security tier with this built-in

Pitch It Like
“Think of ASM as your always-on security scanner: paired with MDR, it’s total visibility + rapid response.”

3 ASM as an Add-On to Core Security Plans

- Include report dashboards, alerts, and automated config remediation
- Justifies price increases with visible outcomes
- Turns a service upgrade into a security maturity step

Revenue Play
$1–4 per user/month uplift on top of existing security stack

4 Cyber Risk Posture Assessment Service

- Offer as a one-time paid engagement or quarterly recurring
- Use LiongardIQ's report dashboards + config monitoring to assess gaps
- Tie findings to insurance controls, CIS, NIST, or custom frameworks

Deliverable
Executive-ready report + prioritized remediation list.

5 New Business Prospecting Toolset

- Use Liongard inspectors (DNS, TLS, Dark Web) to assess prospects
- Run free "exposure scans" and show real risks
- Generate tailored proposals from real data, not guesswork

Sales Boost
Better close rates. Shorter sales cycles.

6 Identify Additional Project Work

- Use asset insights to recommend hardware refreshes, cloud migrations, or compliance improvements
- Spot licensing waste, software drift, and unmanaged services
- Build a pipeline of upsell-ready initiatives from insights you already have

Examples
Replace outdated AV, upgrade endpoints, tighten IAM policies

Show the Value. Capture the Margin. Scale the Practice.

Flexible Pricing Models

LiongardIQ turns ASM into a high-margin, intelligence-driven service. Here's how partners can package and price it.

Model	Description	Example
Per Identity	Ideal for M365-heavy or compliance clients	$5–7/user/month
Tiered Bundle Add-On	Add ASM to Pro or Premium tiers	$500–$1,200 uplift/month
Standalone ASM	Premium core service (dashboards, alerts, compliance, AI)	$1,000+/month
Compliance Add-On	Bundled with insurance/ISO/GDPR services	$4–6/user/month
QBR-Based Assessment	Paid engagement or value-add with prioritized risk recommendations	$2,500/project or included

Tip: Use LiongardIQ to justify premium pricing, especially for compliance-heavy, regulated, or security-mature clients.

liongard

Revenue Model Snapshot: 1,000-User Example

ESTIMATED ROI - PERIODIC

LINE ITEM	ITEM	DESCRIPTION	PRICE	UNIT OF MEASURE	QTY	TIME PERIOD FREQUENCY	INCREASED REVENUE PER TIME PERIOD FREQUENCY	ANNUALLY INCREASED REVENUE
1	Managed Attack Surface	Cyber Risk Dashboard, Continuous Change Tracking/Documentation For Security Audits & Insurance Claims, Real-Time MFA Tracking & Daily Region Access Verification (US, CA EU) For Microsoft 365, Centralized Identity and Device Inventory, AI Powered Asset Intelligence, Automated M365 Remediation for Common Risks.	$7	Users	1000	Monthly	$7,000	$84,000
2	Monthly Billing Reconciliation	1,000 Active End Users – 10% Error Rate - $19.80 BP License	$19.80	Unbilled License	100	Monthly	$1,980	$23,760
3	Cyber Insurance Posture Alignment	$500 Per Assessment Done Quarterly	$500	Customer	25	Quarterly	$12,500	$50,000
4	Warranty Renewals	Dell/Lenovo – 1,000 Workstations With A 20% Past or Upcoming Expirations	$300	Renewal	200	Annually	$60,000	$60,000

ESTIMATED ROI - PER PROJECT

LINE ITEM	ITEM	DESCRIPTION	PRICE	UNIT OF MEASURE	QTY	TIME PERIOD FREQUENCY	INCREASED REVENUE PER TIME PERIOD FREQUENCY	ANNUALLY INCREASED REVENUE
1	Firewall Upgrades	Software Revenue + Project Work – Estimated 25% Out-of-Date 25 Firewalls under management	$500	Firewall Upgrade for Services & Software	5	Per Project	$2,500	$2,500

ESTIMATED ROI FOR SALES DEPARTMENT

Based on 25 Managed Customers & 1,000 Workstations & End Users

Total Combined 1st Year Revenue Generation Expectation	$220,260
Liongard Annual Investment	$41,880
RETURN ON INVESTMENT WHEN EXECUTED PROPERLY	426%

How ASM fuels revenue, retention, and growth

- High-margin, low-effort upsell to existing security clients
- Increased QBR value and stickiness
- Better compliance and audit outcomes = client retention
- Differentiator in a competitive market

liongard

Build a Stronger Practice with ASM – Powered by LiongardIQ

Why ASM Must Be in Your Stack

Attack Surface Management isn't just another service: it's a foundational capability for modern IT service providers. It's how you stay ahead of threats, prove compliance, and deliver proactive value clients can see.

With **LiongardIQ**, partners can:

Strengthen their security portfolio with proactive, always on visibility

Drive recurring revenue through through monthly deliverables and continuous monitoring

Improve client retention by reducing risk before incidents happen

Stand out in a crowded market with automation and AI-enhanced differentiation

liongard

Liongard: Your White-Labeled ASM Partner

You don't have to build it all yourself. LiongardIQ gives you the tools to deliver ASM under your brand complete with:

- 85+ integrations for full-stack visibility
- Multi-tenant support for scalable delivery
- Co-managed options for hybrid client relationships

Position it as your own.
Deliver it your way.
Let LiongardIQ power the back end.

Start offering ASM today by:

- Bundling it with your existing security packages
- Educating clients through risk assessments
- Operationalize at-scale with automation and insights

Let's make it real.
Ready to build your white-labeled ASM service?
Visit **www.liongard.com** to schedule a discovery call.

About Liongard

Liongard is redefining asset intelligence with its AI-powered platform built for modern IT and security operations. Trusted by organizations worldwide to protect complex environments, Liongard delivers unified, real-time visibility across users, systems, networks, and SaaS Applications. Liongard empowers teams to uncover hidden risks, enforce controls, and automate critical security outcomes. By combining deep asset intelligence with AI-driven insights and scalable remediation, Liongard helps organizations reduce risk, strengthen cyber resilience, and operate more efficiently.

For more information, visit www.liongard.com.

liongard