liongard

MONETIZING YOUR INVESTMENT IN LIONGARD

A COMPREHENSIVE GUIDE FOR MSPs

MSP GUIDE

Purpose of the Guide

This guide is designed to help MSPs take full advantage of the increasing cybersecurity risks faced by customers by providing the most effective prevention and protection services. By incorporating Liongard into all your customer service offerings, you can maximize your monthly recurring revenue (MRR) and create numerous stand-alone engagements that significantly add to your income. Additionally, this guide will help you attract and retain customers with your ability to help them sleep better at night, knowing their IT environments are secure.

Who is this Guide Designed For?

This guide is intended for MSPs who are already familiar with Liongard's products and services. While we will discuss the key monetization opportunities Liongard enables, a more comprehensive education can be obtained through Liongard Academy and our weekly Continuing Education Webinars. For those who need to learn a few key points to support their proposals, please consult the Liongard Platform FAQ.

By following this guide, you will learn how to integrate Liongard into your business strategy, offering comprehensive, value-added services that drive revenue growth and enhance customer satisfaction.

A PRIMER FOR MSPS

Attack Surface

at·tack sur·face | \ə-'tak 'sər-fəs\

noun

Any person, process, or technology a threat actor exploits to achieve their objectives on a target.

Fundamentals of Attack Surface Management and Key Business Drivers for enabling a Managed Attack Service Offering.

What is Attack Surface Management?

When discussing cybersecurity breach events, the pivotal moment isn't necessarily when the attack occurs, but often lies within the realm of what could have been done well before the incident to make the initial access by a threat actor irrelevant or at least less impactful through reduction of the blast radius.

The act of hardening the attack surface refers to enforcing an environment grounded in cyber resilience practices. Continuous monitoring for policy change, under deployed policies or gaps in policies recognizes that software, users, and systems are in constant flux, necessitating vigilant configuration change detection and responsive insights.

The reality is that the game has changed.

The tools required to efficiently manage and secure a client's IT infrastructure has sprawled - today's landscape demands integrated IT and security strategies. Historically, their separation has led to gaps and alignment issues. IT drives security posture improvements by reducing misconfigurations, while security possesses the expertise to detect and respond to intrusions. **They should operate in synergy, not isolation.**

Liongard's extensive partner base has identified several critical pain points they are chal-

MARKET LANDSCAPE

lenged with regularly.

Visibility Gaps

Customers often lack comprehensive visibility into their IT environments, leading to unmanaged risks and inefficiencies.

Security Vulnerabilities

The complexity of modern IT environments makes it difficult to identify and mitigate security risks effectively.

Manual Processes

Many organizations rely on manual processes for IT management, which are time-consuming and prone to errors.

Compliance Challenges

Ensuring compliance with various regulations is a major concern, especially for businesses without dedicated compliance teams.

CHALLENGES IN SELLING NEW SERVICES

MSPs encounter specific challenges when introducing new services to their clients.

Value Articulation
Clearly communicating the value of new services to clients can be difficult, especially when clients are focused on cost.

Service Integration
Integrating new services into existing offerings without causing disruptions is challenging.

Client Resistance
Clients may resist changes due to perceived risks or a lack of understanding of the benefits.

Pricing Strategy
Setting the right price for new services to ensure profitability while remaining competitive is complex.

Understanding the drivers for revenue generation is crucial for MSPs looking to grow their businesses.

These statistics underscore the importance of focusing on cybersecurity, managed services, and compliance as key areas for revenue generation.

Here are some important industry statistics:

$150
Billion by 2025
in Cybersecurity Spending

Cybersecurity Spending
Global spending on cybersecurity is expected to exceed $150 billion annually by 2025. This presents a significant opportunity for MSPs to offer security services.

17.5%
CAGR from 2021 to 2026 in Cloud Services Growth
(Forrester)

Cloud Services Growth
The cloud services market is projected to grow at a compound annual growth rate (CAGR) of 17.5% from 2021 to 2026, highlighting the demand for cloud expertise.

$356
Billion 2025 Managed Services Market

Managed Services Market
The global managed services market size is expected to reach $356.24 billion by 2025, driven by the increasing adoption of outsourcing IT services.

$5.5
Million Annually on compliance activities

Compliance Costs
Companies spend an average of $5.47 million annually on compliance activities, indicating the need for efficient compliance solutions.

5 WAYS TO MONETIZE

The following guide aims to provide five options to monetize Liongard's platform and enable you to identify and assess misconfiguration and weaknesses in your clients' systems, networks, or applications, and alert administrators so you can take the necessary measures to address critical issues. In turn, reducing risks and prevent potential cyberattacks and exploits.

1. Enhance Existing Service Offerings or Develop Premium Offering
2. Cyber Risk Posture Assessment and Management
3. Microsoft License Reconciliation
4. Use Liongard for Informed Sales Engagements
5. Identifying Additional Project Work

1 ENHANCE EXISTING SERVICE OFFERINGS OR DEVELOP PREMIUM OFFERING

TACTIC

Bundling Liongard's Attack Surface Management (ASM) in Service Packages

Integrating Liongard's Attack Surface Management (ASM) into your service packages involves incorporating this advanced security feature into your existing offerings. By charging an additional $3-$5 per endpoint/user, you can provide a comprehensive managed attack surface service to your clients, enhancing their security posture and increasing your revenue.

Implementation Steps

Enhance Existing Packages

- ☐ Integrate ASM as a standard feature in your service offerings.
- ☐ Consider premium offering or add-on Managed Attack Surface service.

Highlight Key Features

- ☐ Educate your clients on the benefits of ASM, such as its ability to identify and mitigate risks including misconfigurations, outdated software, over-privileged user accounts, unnecessary services, unpatched assets, internal and external threat actors, old devices, inadequate access controls, supply chain threats, and third-party software vulnerabilities.
- ☐ Use client-facing materials to explain how ASM adds value to their security strategy.

Implement Real-Time Monitoring

- ☐ Liongard is deployed ASM to provide continuous visibility into clients' IT environments.
- ☐ ASM actively identifies and addresses potential threats, misconfigurations, vulnerabilities, and weaknesses.

Automate Security Processes

- ☐ Utilize ASM's automation capabilities to continuously monitor changes, additions, and removals within the IT environment.
- ☐ Ensure security tools are fully deployed and correctly configured, reducing manual efforts and human error.

EXPECTED RESULTS

Constant Threat Awareness

- ASM provides real-time visibility, allowing you to proactively identify and tackle potential threats, ensuring you stay ahead of disruptions.

Fortified Cybersecurity

- By monitoring for unexpected gaps in the attack surface, ASM helps harden defenses against unauthorized changes and potential breaches, enhancing overall security.

Streamlined Compliance & Audits

- ASM's comprehensive timeline history and reporting capabilities ensure seamless navigation of industry regulations and audits, simplifying compliance management.

Efficient Incident Resolution

- Proactively addressing minor issues before they escalate, ASM enables swift and efficient problem resolution, minimizing downtime and impact on clients.

Security Automation Integration

- Automating cybersecurity posture monitoring ensures continuous protection and optimal configuration of security tools, increasing operational efficiency.

By bundling ASM into your service packages, you can offer a robust, proactive security solution that enhances your value proposition, improves client satisfaction, and generates additional revenue. This approach not only strengthens your clients' cybersecurity posture but also positions your MSP as a trusted partner in managing their IT security needs.

2 CYBER RISK POSTURE ASSESSMENT AND MANAGEMENT

DRIVE GROWTH WITH LIONGARD'S CYBER RISK MONITORING

TACTIC

Cyber Risk Posture Assessment and Management

Understanding and managing the cyber risk posture of your customers is critical in today's threat landscape. Liongard's Cyber Risk Monitoring provides a comprehensive view of your customer's cybersecurity posture, tied directly to cyber insurance controls. This tactic ensures that your clients comply with security frameworks and cyber insurance requirements, providing a proactive approach to managing their cybersecurity risks.

Implementation Steps

Enhance Existing Packages

- ☐ Access Liongard's Cyber Risk Dashboard to gain an instant overview of your customer's cybersecurity posture.
- ☐ Ensure the dashboard is configured to align with relevant security frameworks and cyber insurance requirements.

Monitor Configuration Changes

- ☐ Use Liongard's Configuration Change Detection to monitor and alert on any configuration drifts that may impact the customer's cyber risk posture.
- ☐ Set up automated alerts to notify you of any significant changes that could indicate a potential security threat or non-compliance.

Implement the Cyber Risk Alert Template

- ☐ Deploy the new Cyber Risk Alert Template to track and monitor key security-related configuration settings across various systems.
- ☐ Regularly review and update the template to ensure it covers all critical aspects of your customer's IT environment.

EXPECTED RESULTS

Improved Cybersecurity Posture

- By leveraging Liongard's Cyber Risk Dashboard and Configuration Change Detection, you'll provide your clients with a clear and actionable view of their cybersecurity posture, enhancing their overall security.

Enhanced Compliance and Insurance Alignment

- Ensuring compliance with security frameworks and cyber insurance requirements helps your clients meet regulatory obligations and qualify for better insurance premiums.

Proactive Risk Management

- The Cyber Risk Alert Template allows for continuous monitoring of key security settings, enabling proactive identification and remediation of potential vulnerabilities.

Increased Client Trust and Retention

- Providing a robust cyber risk posture assessment and management service demonstrates your commitment to your clients' security, fostering trust and long-term relationships.

Revenue Growth

- By offering comprehensive cyber risk management services, you can drive growth for your MSP business, attracting new clients and upselling to existing ones.

3 MICROSOFT LICENSE RECONCILIATION

STREAMLINE MANAGEMENT AND MAXIMIZE VALUE

TACTIC

Microsoft 365

Microsoft License Reconciliation

Microsoft License Reconciliation involves auditing and managing your clients' Microsoft licenses to ensure they are correctly allocated and utilized. This tactic helps MSPs optimize license usage, reduce unnecessary costs, and ensure compliance with Microsoft licensing agreements. By offering this service, you can provide added value to your clients and create new revenue streams.

Implementation Steps

Conduct a License Audit

- ☐ Use Liongard's platform to perform a comprehensive audit of your clients' Microsoft licenses. Identify all active licenses, their allocation, and their usage across the client's organization.

Analyze and Optimize License Usage

- ☐ Compare the current license allocation with actual usage to identify underutilized or unused licenses.
- ☐ Recommend adjustments to optimize license usage, such as reallocating licenses to match usage patterns or downgrading unnecessary premium licenses.

Ensure Compliance

- ☐ Verify that all licenses are compliant with Microsoft licensing agreements to avoid potential fines or penalties.
- ☐ Provide clients with detailed reports on their license usage and compliance status.

Implement Ongoing Monitoring

- ☐ Set up Liongard to continuously monitor license allocation and usage. Provide regular updates and recommendations to clients to ensure they remain compliant and optimized.

EXPECTED RESULTS

Cost Savings

- By identifying and eliminating underutilized or unused licenses, clients can reduce unnecessary costs and maximize their IT budget.

Improved Compliance

- Ensuring that all licenses are compliant with Microsoft licensing agreements helps clients avoid potential fines and legal issues

Enhanced License Utilization

- Optimizing license allocation ensures that clients are making the most of their purchased licenses, improving overall efficiency.

Proactive Management

- Continuous monitoring and regular updates help clients stay on top of their license usage, preventing issues before they arise and maintaining compliance.

Increased Client Satisfaction

- Providing a detailed and proactive approach to license management demonstrates your commitment to your clients' success, fostering trust and long-term relationships.

By offering Microsoft License Reconciliation as part of your service portfolio, you can help clients optimize their license usage, ensure compliance, and reduce costs. This service not only adds significant value to your offerings but also positions your MSP as a proactive and trusted advisor in managing their IT resources.

4 USE LIONGARD FOR INFORMED SALES ASSESSMENTS

TACTIC

New Business Prospecting

New business prospecting involves using Liongard's powerful tools to gather critical information about potential clients' websites and email systems without needing on-site access. By leveraging the Internet Domain & DNS Inspector, Identity Monitoring (Dark Web) scan, and TLS/SSL Certificates inspector, you can quickly assess a prospect's security posture and provide valuable insights during sales discussions. This tactic enables you to create tailored proposals that address specific security concerns, enhancing your sales efforts and demonstrating your expertise.

Implementation Steps

Gather Website and Email Information

- ☐ Use the Liongard Internet Domain & DNS Inspector to collect critical information about the prospect's website and email systems.
- ☐ Identify potential vulnerabilities and areas for improvement without requiring on-site access.

Assess Security Practices

- ☐ Utilize the TLS/SSL Certificates inspector to evaluate the prospect's security practices, including the validity and configuration of their TLS/SSL certificates
- ☐ Identify any issues or gaps that could be addressed to improve their security.

Run Identity Monitoring (Dark Web) Scan

- ☐ Conduct an Identity Monitoring (Dark Web) scan to check if any of the prospect's email addresses have been involved in data breaches.
- ☐ Use this information to provide insights into the prospect's security posture and potential risks.

Prepare Tailored Proposals

- ☐ Use the gathered data to create tailored proposals that address the specific security concerns of the prospect.
- ☐ Highlight the benefits of using Liongard's tools to enhance their security posture and protect their business.

Offer Free Assessment Period

- ☐ Inform prospects that the first month of using Liongard for prospect assessments is free with an active subscription.
- ☐ Inform prospects that the first month of using Liongard for prospect assessments is free with an active subscription.

Automated Weekly Dark Web Health Check

- ☐ Implement Liongard's automated weekly Dark Web health check, providing ongoing monitoring of any compromised credentials related to the prospect's domain.
- ☐ Offer this service as part of a comprehensive dark web monitoring package, driving MRR through continuous monitoring and proactive alerts on potential security vulnerabilities.

EXPECTED RESULTS

Informed Sales Discussions

- Gathered data provides valuable insights that can be used to have informed and impactful sales discussions with prospects, increasing the likelihood of conversion.

Enhanced Credibility

- Demonstrating your ability to identify and address specific security concerns builds credibility and positions you as a trusted advisor.

Tailored Proposals

- Creating proposals that directly address the prospect's security needs increases the relevance and appeal of your offerings, improving your chances of winning new business.

Early Risk Identification

- Identifying potential security risks early in the sales process allows you to offer proactive solutions, showcasing the value of your services.

Increased Conversion Rates

- Offering a free assessment period encourages prospects to try Liongard's tools, increasing the likelihood of converting them into paying clients.

Increased MRR through Dark Web Monitoring

- The weekly Dark Web health check offers an automated monitoring service that can be bundled into your recurring revenue model, providing continuous value to your clients.

By leveraging Liongard's Internet Domain & DNS Inspector, Identity Monitoring (Dark Web) scan, and TLS/SSL Certificates inspector for new business prospecting, you can provide valuable insights, create tailored proposals, and enhance your sales efforts. This approach not only helps you win new business but also demonstrates your expertise in managing and improving cybersecurity for potential clients.

5 IDENTIFYING ADDITIONAL PROJECT WORK

MONETIZING DEEP SYSTEM VISIBILITY

TACTIC

New and Existing Business Prospecting

Liongard's deep visibility into clients' systems allows you to uncover additional project work, creating new revenue streams. By automating asset discovery and monitoring, Liongard identifies opportunities for upselling and ensures that your clients' systems are always optimized and compliant. This tactic empowers MSPs to expand service scopes, streamline project scoping, and protect their bottom line.

Implementation Steps

Identify New Line Items for Service Scopes

- ☐ Leverage Liongard's comprehensive system visibility to identify areas where clients require additional services, such as hardware refreshes, system optimizations, or enhanced security solutions.
- ☐ Use this information to introduce new line items in your service agreements, expanding your revenue opportunities while delivering value to clients.

Quickly Find Systems Needing Updates or Upgrades

- ☐ Automate the identification of systems that require updates, upgrades, or replacements. Liongard's monitoring capabilities allow you to spot outdated hardware, expired software, or unpatched vulnerabilities without needing on-site visits.
- ☐ Use this insight to proactively recommend projects that will enhance your clients' IT environment, ensuring continued security and operational efficiency

Conduct Billing Reviews to Spot Discrepancies

- ☐ Run automated billing reviews to identify discrepancies in user counts, licenses, or services that may have changed over time.
- ☐ This can uncover opportunities for billing corrections, license optimization, and additional services, providing transparency to clients and ensuring you're billing accurately.

Detect Expiring Certifications

- ☐ Utilize Liongard's monitoring to detect when important certifications, warranties, or licenses are about to expire.
- ☐ Turn this into an opportunity to upsell clients on renewal services, license management, or compliance support, keeping their systems up-to-date and secure.

EXPECTED RESULTS

Increased Revenue from New Project Work

- Expanding service scopes through Liongard's deep visibility provides a steady flow of new project work, driving additional revenue from existing clients.

Improved Client Systems

- Proactively identifying and addressing outdated systems, expiring certifications, and discrepancies ensures your clients' IT environments are optimized, reducing downtime and increasing their satisfaction with your services.

Streamlined Operations and Project Scoping

- Automated asset discovery saves time and effort in identifying potential project opportunities, enabling you to scope and deliver work more efficiently without manual inspections or on-site visits.

Enhanced Upsell Opportunities

- By detecting certifications and licenses that are about to expire, you can engage clients with timely upsell opportunities, ensuring continuous revenue from renewals and compliance services.

Optimized Billing Accuracy

- Conducting regular billing reviews helps ensure accuracy in your invoicing, identifying any discrepancies that may have gone unnoticed, and helping you maintain transparent client relationships.

By monetizing Liongard's deep system visibility, MSPs can uncover new project opportunities, streamline operations, and maximize revenue from their client base. This approach not only protects your bottom line but also enhances your reputation as a proactive, value-driven MSP that delivers consistent results.

REVENUE OPPORTUNITY EXAMPLE

ESTIMATED ROI - PER RECURRING

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**	Access To Cyber Risk Dashboard, Change Tracking/Documentation For Security Audits & Insurance Claims, Daily Verification Of MFA Enablement & Region Access Verification (US, CA EU) For 365, Automated Monthly Report Of Changes Across Stack.	$3	Users	1000	Monthly	**$3,000**	**$36,000**
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	**$172,260**
Liongard Annual Investment	**$14,850**
RETURN ON INVESTMENT WHEN EXECUTED PROPERLY	**1060%**

CONCLUSION

By incorporating these tactics, MSPs can fully leverage Liongard's capabilities to enhance their service offerings, improve client satisfaction, and drive revenue growth. Each tactic is designed to address specific challenges and opportunities within the MSP landscape, providing actionable steps to optimize operations and deliver exceptional value to clients.

Liongard's comprehensive platform empowers MSPs to proactively manage cybersecurity, streamline operations, and provide tailored solutions that meet the evolving needs of their clients. By following the strategies outlined in this guide, you can differentiate your services, enhance your value proposition, and achieve sustainable business growth in a competitive market.

Embrace these tactics to transform your service offerings, drive new business, and secure your position as a trusted advisor in the IT and cybersecurity landscape.

Your investment in Liongard is not just a toolset but a pathway to greater success and profitability.

liongard

www.liongard.com