Lakera Guard:

Market Position, Strategy, and Product Leadership

Securing the AI-Powered Enterprise

By **Marcelo Caballero** , MSc AI, Senior Consultant

October 2025 | Confidential

My Journey to Lakera: The Right SC for Lakera's Next Chapter

Bridging Deep Tech Innovation with Enterprise-Scale Execution

Enterprise Productization in Regulated Markets

At Vorwerk and V-Zug I led the scaling of connected and AI enabled products across DACH and Europe. The work covered end to end delivery from roadmap to launch and support at scale.

This means I know how to:

- ☐ Build products that meet security privacy and compliance requirements for enterprise CISOs and regulators including GDPR.
- ☐ Translate a developer first product into a solution that works for risk averse decision makers and nontechnical users.
- ☐ Manage the full product lifecycle at scale from MVP to a supported global offering.

Deep, AI-Native Technical Foundation

My MSc in AI focused on AGI and limits of LLM evaluation. This provides a grounded view of model behavior and the attack surface you secure.

This means I can:

- ☐ Hold credible technical discussions with research and engineering teams.
- ☐ Analyze adversarial attacks and model vulnerabilities and explain the value of the Gandalf data asset.
- ☐ Turn complex technical work into clear product choices and customer narratives.

Navigating Platform Scale & GTM Integration

Experience at Siemens, Cisco and Swisscom taught me how to operate in large organizations and enable a global channel.

This means I will:

- ☐ Plan and deliver integration of Lakera Guard into Check Point Infinity with clear ownership milestones and risk controls.
- ☐ Equip sales and partners with use cases pricing and proof plans that improve conversion.
- ☐ Prioritize enterprise grade features such as RBAC audit and SIEM integration to move upmarket and increase deal size.

	Siemens AG	Cisco Systems	Incubator McKinsey	Swisscom	Vorwerk	Lufthansa Systems	V-Zug	Detecon	Schaerer AG	Now	Lakera
Nr. Employees FY2024	327,000	90,400	45,100	19,895	9,300	2,800	2,086	1,217	388		70

Defining AI Security

AI security encompasses five distinct but interconnected segments that address the unique challenges of securing AI systems throughout their lifecycle:

Runtime/LLM Firewalls

Real-time protection against prompt injection, jailbreaking, and data leakage during model inference.

Lakera Guard's primary domain

AI Supply Chain Management

Securing the provenance, integrity, and compliance of models, data, and dependencies.

Model/Data Security

Protecting training data and model weights from poisoning, theft, and unauthorized access.

Agentic Guardrails

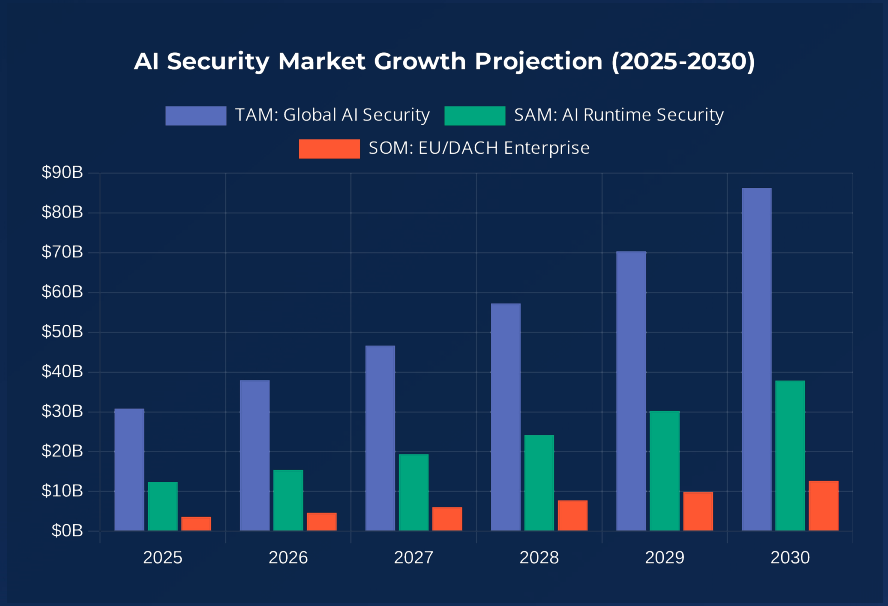
Safety mechanisms for autonomous AI agents to prevent harmful actions and ensure alignment with human values.

AI Governance

Policies, controls, and documentation to ensure responsible AI use and regulatory compliance (e.g., EU AI Act).

The AI security market is evolving rapidly, with runtime protection emerging as the most immediate need for enterprises deploying generative AI.

Market Size & Growth



Source: Mordor Intelligence, Grand View Research, Future Market Insights (2025)

Total Addressable Market (TAM)

$30.9B ↑ 22.8% CAGR

Global AI security market (2025)

Includes all AI security segments: runtime protection, model security, governance, and monitoring

Serviceable Available Market (SAM)

$12.4B ↑ 25% CAGR

AI runtime security & LLM firewalls (2025)

Focused on Lakera's core market of runtime protection and LLM security solutions

Serviceable Obtainable Market (SOM)

$3.7B ↑ 28% CAGR

EU/DACH enterprise AI security (2025)

Initial focus on EU/DACH region with strong regulatory drivers (EU AI Act)

Key Growth Drivers

- Enterprise AI adoption acceleration
- Rising AI security incidents
- EU AI Act compliance requirements
- Data privacy concerns

Market Drivers & Pressures

GenAI Adoption

- 78% of enterprises deploying GenAI in production by 2026
- Expanding attack surface with each new AI deployment
- Increasing complexity of AI supply chains
- Shift from experimental to mission-critical AI systems

Adversary AI Usage

- 300% increase in AI-powered attacks (2024-2025)
- Automated prompt injection at scale
- Sophisticated jailbreaking techniques
- Model poisoning and data extraction attacks

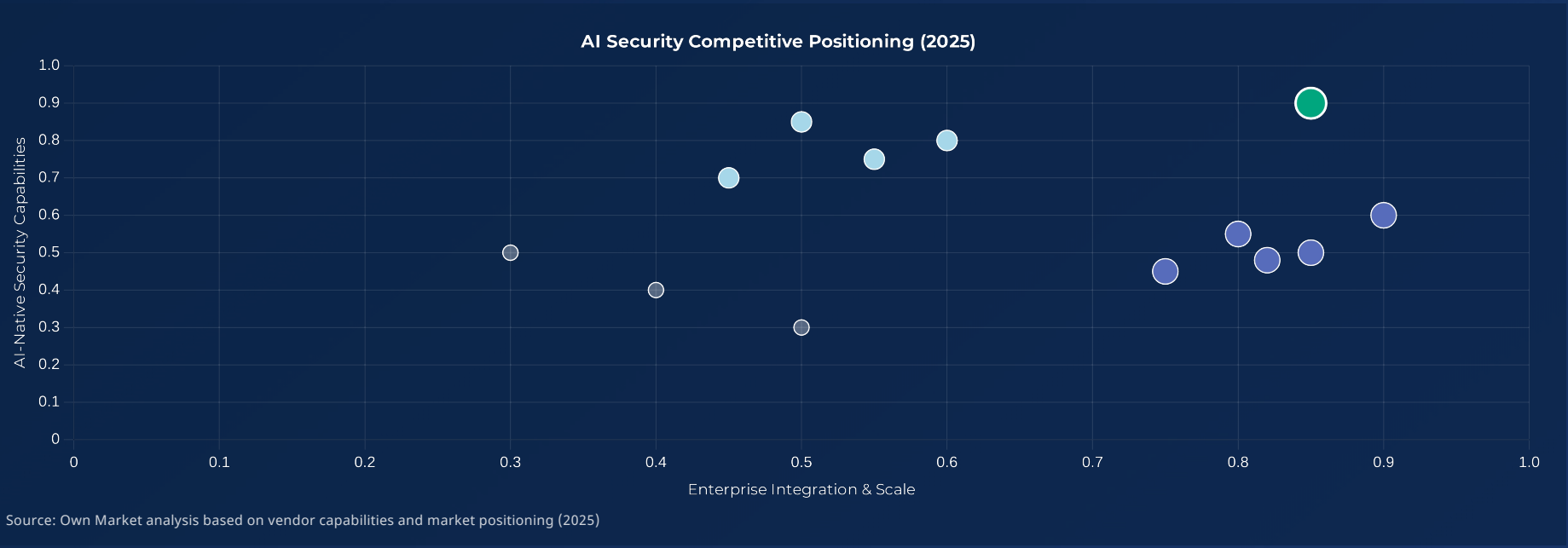
Regulatory Pressure

- EU AI Act enforcement Q2 2025
- Risk-based classification requiring security controls
- Mandatory risk assessments for high-risk AI systems
- Global regulatory convergence (US, UK, APAC)

Market Inflection Point

The convergence of these three forces is creating an unprecedented market opportunity for AI-native security solutions. Organizations must implement robust AI security measures now to protect their AI investments, comply with regulations, and defend against increasingly sophisticated threats.

Competitive Map



Source: Own Market analysis based on vendor capabilities and market positioning (2025)

Market Positioning

The AI security market is divided between specialized AI security vendors and established platform providers, with Lakera uniquely positioned at the intersection.

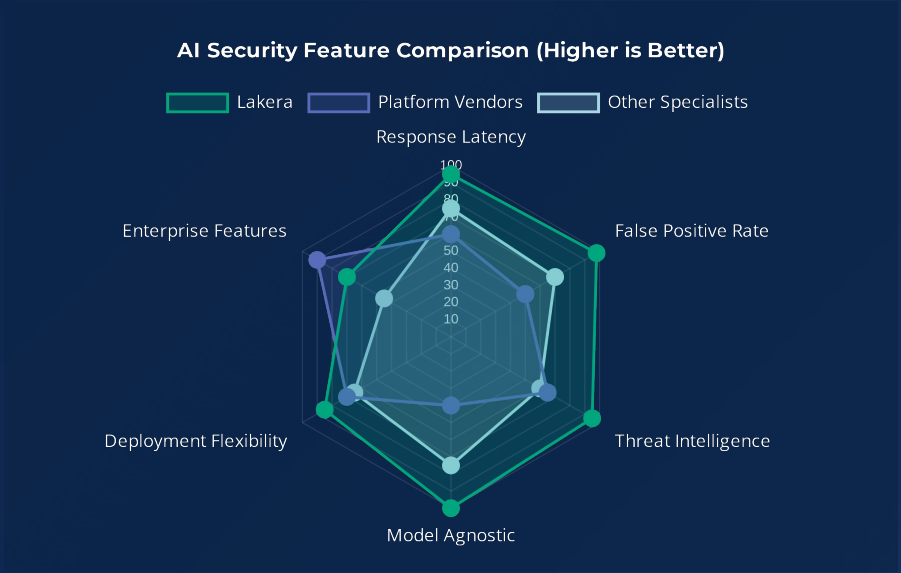
Vendor Categories

- **Leaders (Lakera)**
  High AI-native capabilities with enterprise scale
- **AI Security Specialists**
  Advanced AI security but limited enterprise scale
- **Platform Vendors**
  Strong enterprise integration but limited AI-native security
- **Challengers**
  Emerging solutions with limited capabilities

Strategic Advantage

The Check Point acquisition positions Lakera to combine best-in-class AI-native security with enterprise-grade distribution and integration capabilities.

Feature Benchmark



Source: own analysis (2025)

Competitive Advantages

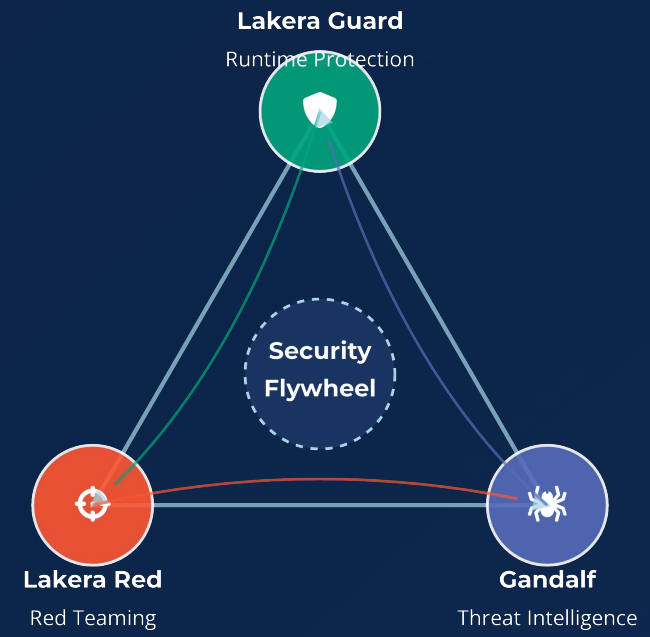
Lakera Guard outperforms competitors across key metrics that matter most to enterprise customers deploying AI at scale.

Feature	Lakera	Platform Vendors	Other Specialists
Response Latency	**<40ms**	100-250ms	75-150ms
False Positive Rate	**0.01%**	1-3%	0.5-2%
Threat Intelligence	**80M+ vectors**	Varies widely	10-30M vectors
Model Agnostic	✓	✗	◐
Deployment Options	SaaS & On-Prem	Platform-dependent	Mostly SaaS

Key Differentiators

- **Ultra-low latency:** Critical for real-time applications
- **Gandalf data moat:** Unmatched threat intelligence
- **Model agnostic:** Works with any LLM provider

Lakera Product Trinity



Source: Lakera Product Architecture (2025)

Integrated Security Ecosystem

Lakera's three core products work together to create a powerful flywheel effect, delivering comprehensive AI security across the entire lifecycle.

Lakera Guard (Shield)

Runtime protection for AI applications with ultra-low latency (<50ms) and industry-leading precision.

- Prompt injection defense
- Jailbreak prevention

Lakera Red (Sword)

Expert-led AI red teaming and penetration testing to identify vulnerabilities before exploitation.

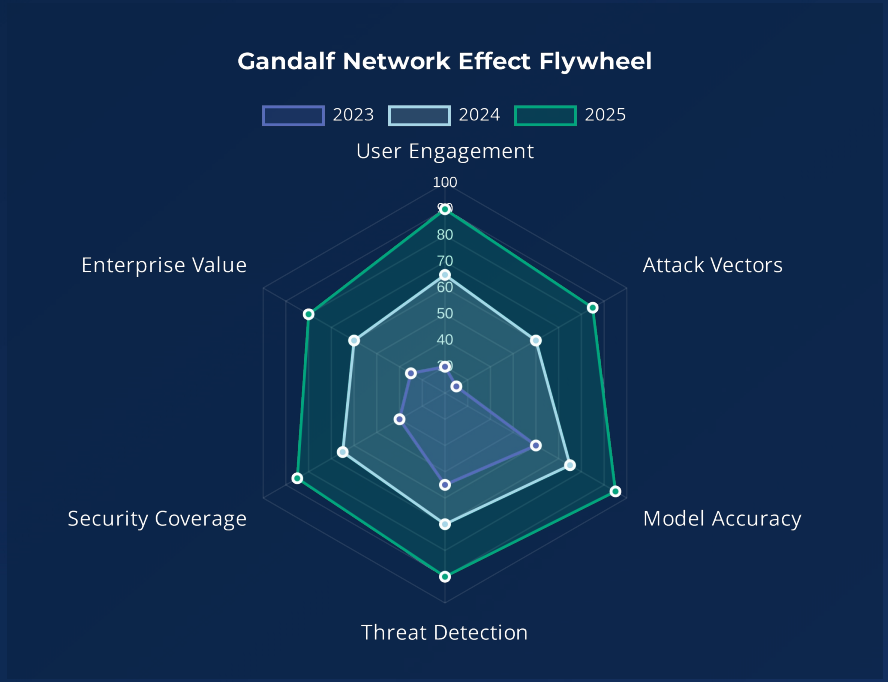
- Risk-based assessment
- Remediation guidance

Gandalf (Intelligence)

Viral threat intelligence platform with 1M+ users contributing 80M+ adversarial prompts.

- Continuous learning
- Novel attack detection

Gandalf Data Moat



Source: Own analysis, Lakera Gandalf Platform Analytics (2025)

Unique Competitive Advantage

Gandalf has created an unprecedented data moat that powers Lakera's AI security capabilities through continuous learning from real-world attack vectors.

Community Scale

1M+

Active users testing AI security boundaries

Attack Vectors

80M+

Adversarial prompts collected and analyzed

Daily Growth

150K+

New attack vectors added daily

Success Rate

99.7%

Attack detection accuracy

Strategic Value

- **Continuous Learning:** Real-time updates to security models based on emerging threats
- **Network Effects:** Value increases exponentially with each new user and attack vector
- **Defensibility:** Dataset cannot be easily replicated by competitors

Check Point Acquisition Context

2021
Lakera founded

2023-2024
Gandalf community grows to 1M+ users and 80M+ adversarial prompts

2024-06
Series A $20M / Total pre-acquisition funding $30M

2025-09-16
Check Point announces intent to acquire Lakera
Price undisclosed. Reputable media estimate ≈ $300M

Strategic Rationale

The acquisition creates significant value for both companies, positioning the combined entity as the leader in comprehensive AI security.

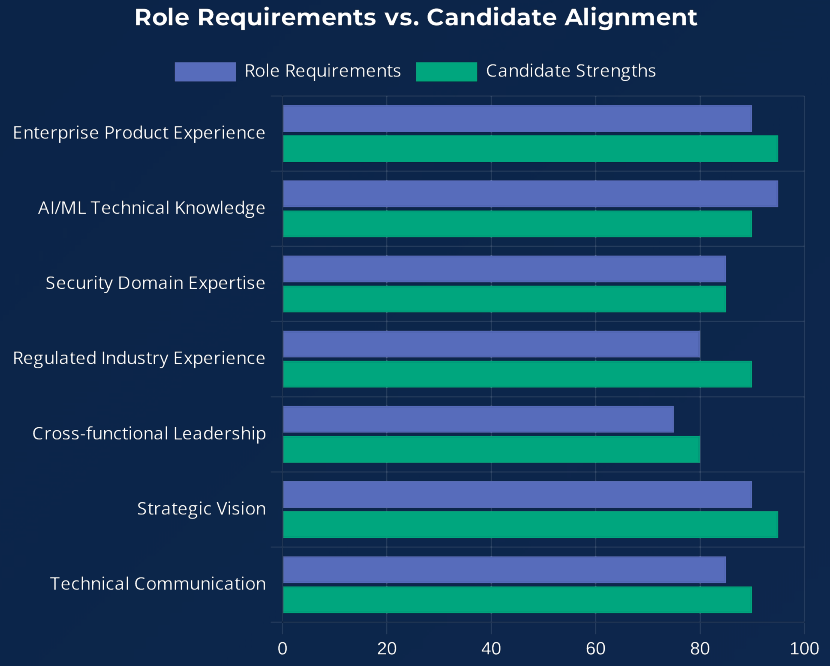
For Lakera

- Global enterprise distribution network
- Integration with broader security stack
- Resources to accelerate product roadmap

For Check Point

- Immediate AI security leadership position
- Integration with Infinity security platform
- Access to Gandalf's unique threat intelligence

Why the Role as Senior Product Manager Now?



Source: Lakera's Job Description/ own profile comparison (2025)

Critical Inflection Point

The Senior PM role is essential at this pivotal moment as Lakera transitions from startup to enterprise-scale following the Check Point acquisition.

Key Role Requirements

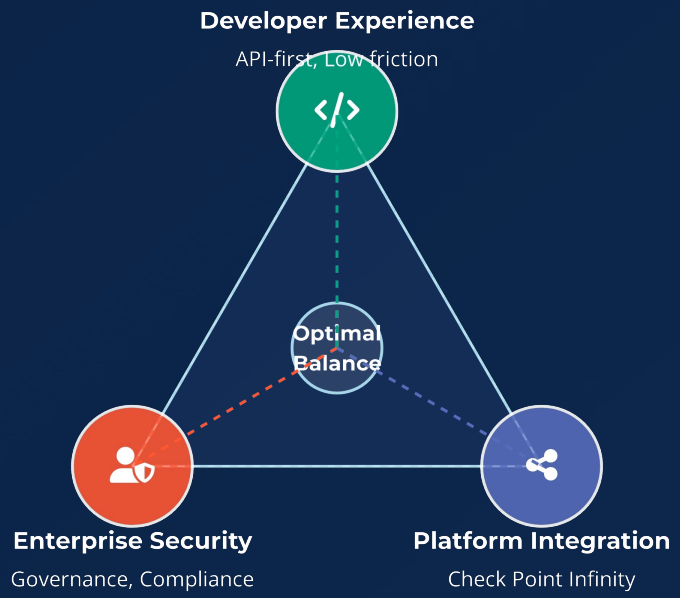
- **Enterprise Integration Expertise**
  Seamlessly integrate Lakera Guard into Check Point's Infinity platform
- **AI Security Domain Knowledge**
  Deep understanding of AI security challenges and solutions
- **Regulated Industry Experience**
  Navigate complex compliance requirements (EU AI Act)

Strategic Opportunity

This role represents a unique opportunity to shape the future of AI security at global scale through:

- Defining the product roadmap for enterprise AI security
- Building the foundation for Lakera as Check Point's AI Security Center of Excellence
- Creating a clear path to Head of Product leadership

Challenges to Solve



Source: Own Product Strategy Analysis (2025)

Key Product Challenges

The Senior PM role must navigate complex tensions between competing priorities while maintaining Lakera's core value proposition.

Developer-First vs. Enterprise CISO

Balancing the simplicity and flexibility developers demand with the governance and compliance requirements of enterprise security leaders.

Speed vs. Security

Maintaining ultra-low latency while expanding security coverage and detection capabilities to address emerging threats.

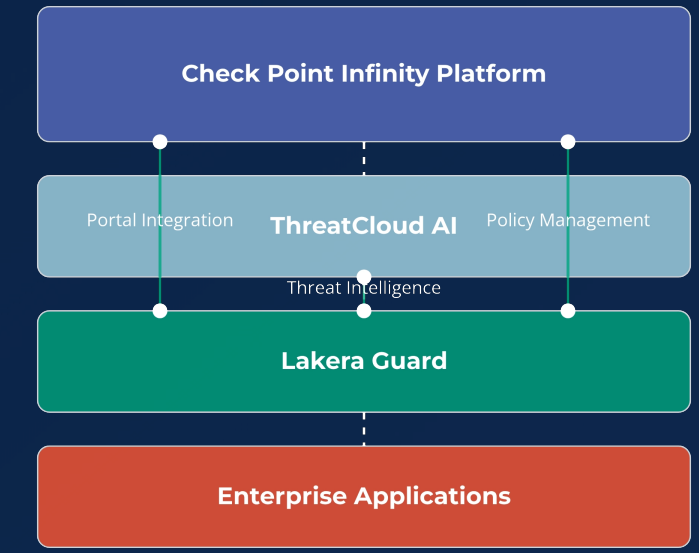
Integration vs. Independence

Integrating deeply with Check Point's Infinity platform while preserving Lakera's agility and AI-native innovation capabilities.

Strategic Opportunity

These challenges represent significant opportunities to create differentiated value by finding the optimal balance that serves both developer and enterprise needs.

Theme 1: Deep Infinity Integration



Source: Own analysis - Projection Lakera Product Roadmap

Strategic Integration

Seamlessly integrating Lakera Guard into Check Point's Infinity platform to deliver comprehensive AI security as part of a unified security architecture.

Q1 2026: Infinity Portal Integration

Single pane of glass management for AI security alongside other security controls.

- Unified dashboard
- Centralized alerts

Q2 2026: ThreatCloud AI Integration

Bi-directional threat intelligence sharing between Gandalf and ThreatCloud.

- Enhanced detection
- Shared IOCs

Q3 2026: Cross-Product Workflows

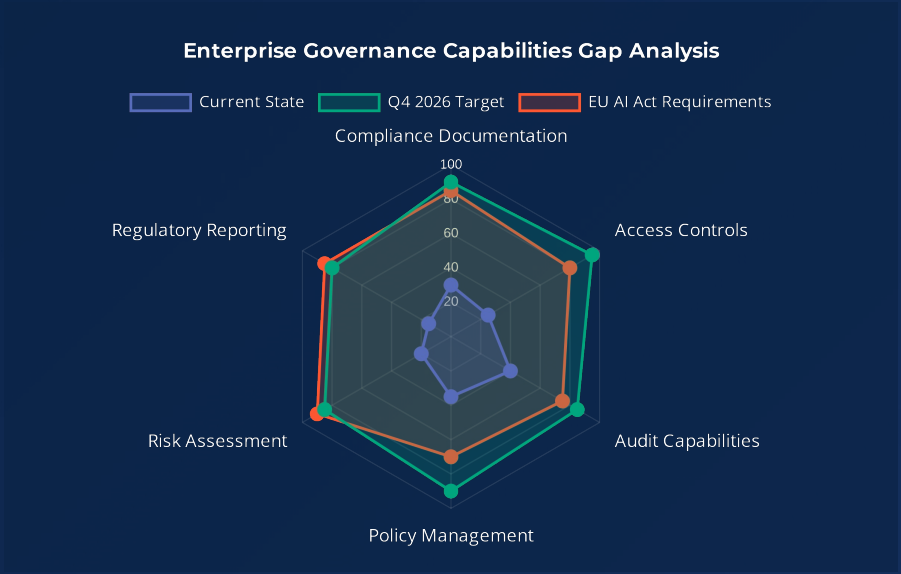
Automated response workflows across AI and traditional security controls.

- Automated remediation
- Policy enforcement

Integration Benefits

- **Enterprise reach:** Access to 100,000+ Check Point customers
- **Unified security:** AI security as part of holistic security strategy
- **Operational efficiency:** Single management console for all security

Theme 2: Enterprise-Grade Governance



Source: EU AI Act requirements analysis and preliminary targets (draft)

Strategic Rationale

Enterprise customers require robust governance capabilities to deploy AI securely at scale while meeting regulatory requirements. This theme positions Lakera Guard as the compliance solution of choice for regulated industries.

Key Governance Features

EU AI Act Compliance Dashboard

Automated risk assessment and documentation for high-risk AI systems under the EU AI Act, with pre-built templates for required technical documentation.

Role-Based Access Control (RBAC)

Granular permissions for AI security policies, allowing separation of duties between security teams, developers, and compliance officers.

Comprehensive Audit Trails

Immutable logs of all AI interactions, policy changes, and security events with advanced search and filtering capabilities.

Policy Templates & Versioning

Pre-built security policy templates for common use cases with version control and approval workflows.

Implementation Timeline (draft)

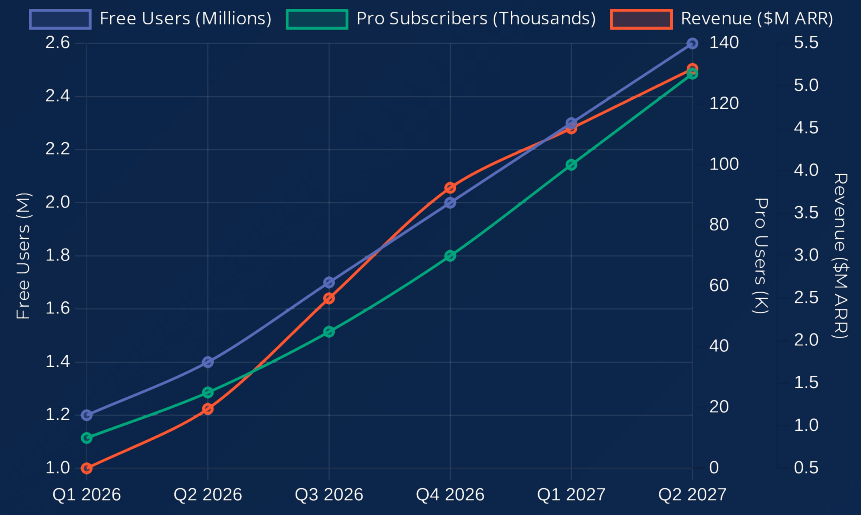
Q1 2026
RBAC and basic audit trails

Q2 2026
EU AI Act compliance dashboard

Q3 2026
Advanced policy templates and versioning

Q4 2026
Integration with Check Point Infinity governance framework

Theme 3: Monetizing the Gandalf Data Moat



Source: Lakera Gandalf Platform Analytics & Revenue Projections (draft)

Strategic Opportunity

Transform Gandalf from a viral marketing tool into a sustainable revenue stream while preserving its network effects and data collection capabilities.

Q1

Gandalf Pro Tier Launch

Premium subscription with advanced challenges, leaderboards, and exclusive content for security professionals and researchers.

Q2

Threat Intelligence API

Expose Gandalf's unique dataset as a commercial API for security vendors and enterprise security teams.

Q3

Enterprise Training Platform

Custom LLM security training environments for enterprise security teams based on Gandalf's challenge framework.

Q4

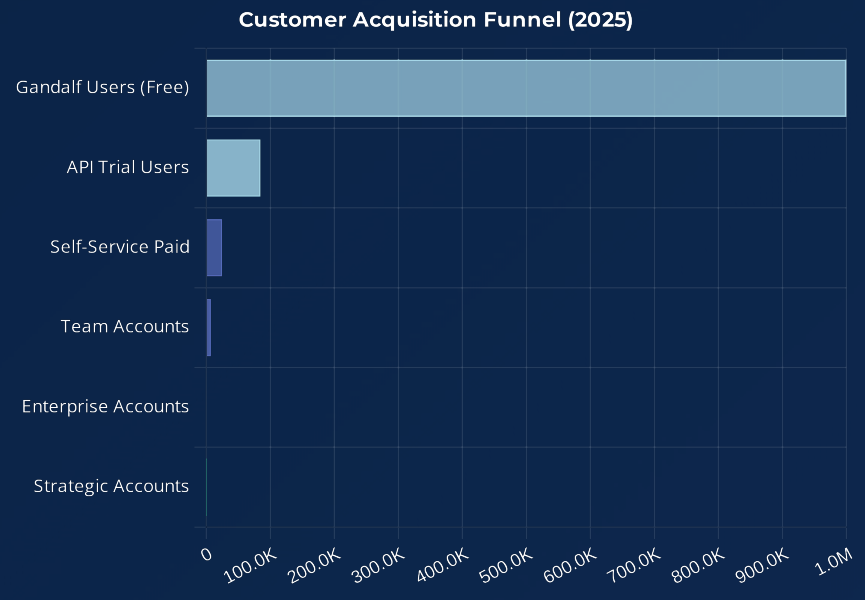
Gandalf Certification Program

Industry-recognized certification for AI security professionals, creating a talent pipeline for customers.

Key Success Metrics

- 10% Pro tier conversion rate
- $5M ARR by end of 2026
- 200M+ attack vectors
- 5,000+ certified professionals

Customer Acquisition Motions



Source: Lakera Go-to-Market Strategy (draft)

Dual-Channel Strategy

Lakera's customer acquisition leverages both bottom-up developer adoption and top-down enterprise sales, creating a powerful flywheel effect.

1

Developer-First Adoption

Free tier and self-service options drive initial adoption among developers and AI engineers, creating product champions within organizations.

2

Enterprise Conversion

As usage grows, security and compliance needs drive enterprise-wide adoption with governance features, SLAs, and support.

3

Check Point Channel

Leverage Check Point's global sales force and channel partners to accelerate enterprise adoption and expand into new markets.

Key Metrics

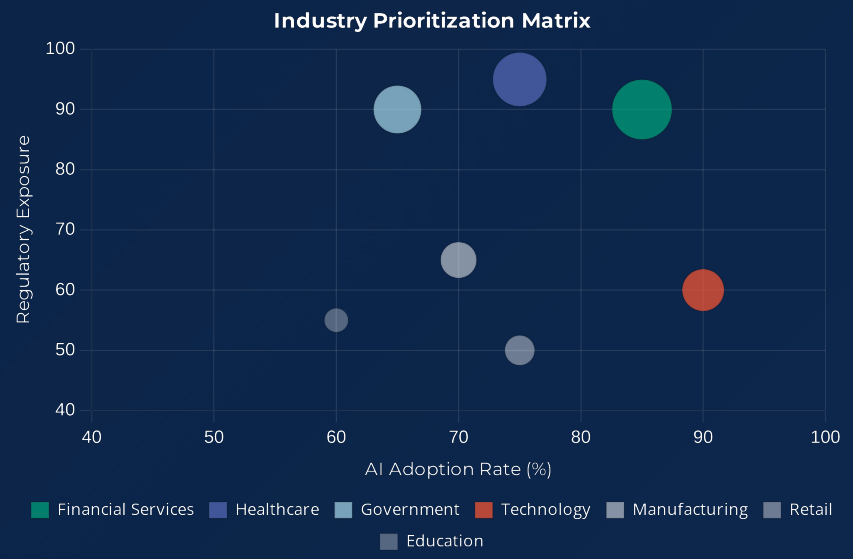
Developer Conversion
12% Free → Paid

Enterprise Expansion
3.5x Annual Growth

CAC Payback
8.2 Months

Net Revenue Retention
135% Annual

Target Verticals



Source: Market analysis based on AI adoption and regulatory exposure (projection)

Priority Industry Focus

Lakera will focus on highly regulated industries with both significant AI adoption and stringent security requirements.

Financial Services

Banks, insurance, and fintech companies with strict regulatory requirements and high AI adoption.

- Sensitive customer data protection
- Compliance with GDPR, GLBA, PCI-DSS

Healthcare

Hospitals, pharma, and health tech with strict patient data protection needs.

- HIPAA compliance requirements
- Patient data confidentiality

Government

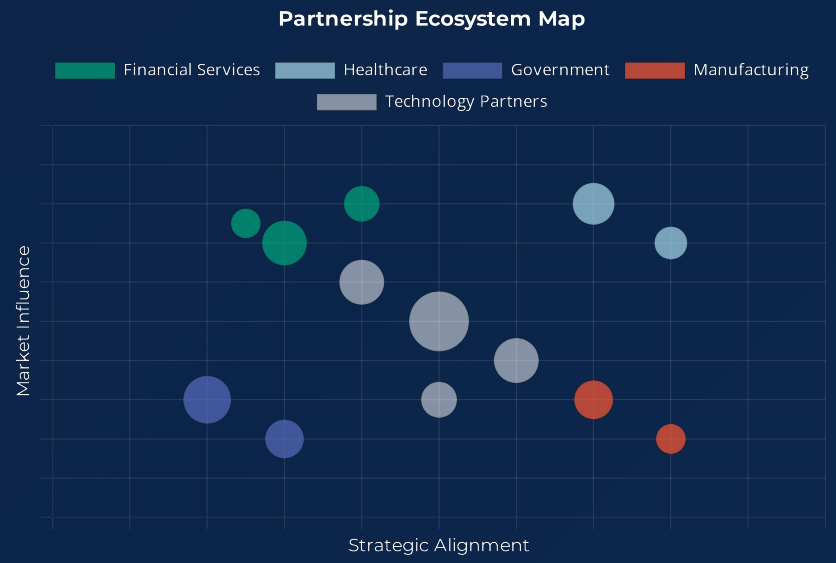
Public sector agencies with high security standards and growing AI adoption.

- Classified information protection
- Critical infrastructure security

Vertical Strategy

Develop industry-specific templates, compliance documentation, and reference architectures to accelerate adoption in target verticals. Partner with industry-specific system integrators and consultancies to expand reach.

Lighthouse Accounts & Partnerships



Source: Lakera Partnership Strategy (projection)

Strategic Partnership Approach

Building a robust ecosystem of reference customers, technology partners, and channel relationships to accelerate market adoption and establish Lakera as the AI security standard.

Lighthouse Accounts

Financial Services
Credit Suisse, Deutsche Bank

Healthcare
Roche, Novartis

Government
EU Commission, Swiss Gov

Manufacturing
Siemens, ABB

Technology Partners

Cloud Providers
AWS, Azure, GCP

LLM Providers
OpenAI, Anthropic, Cohere

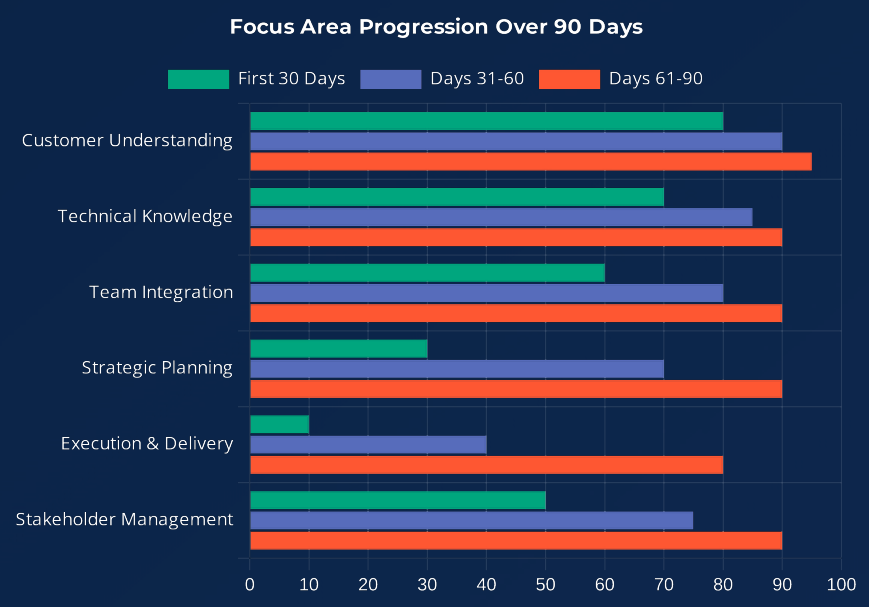
DevOps
GitHub, GitLab, Atlassian

Security
CrowdStrike, Palo Alto

Partnership Goals

- 10 reference case studies
- 5 technology integrations
- 3 marketplace listings
- 20 channel partners

30-60-90 Day Plan



Source: Senior PM Onboarding Framework (draft)

First 30 Days: Learn

Stakeholder Mapping
Build relationships with key stakeholders across Lakera and Check Point teams

Customer Discovery
Interview 15+ customers to understand pain points and requirements

Technical Deep Dive
Understand Lakera Guard architecture and Infinity integration points

Days 31-60: Analyze

Metrics Framework
Establish key product metrics and measurement framework

Roadmap Prioritization
Refine product roadmap based on customer insights and business goals

Integration Strategy
Define detailed integration plan with Check Point Infinity platform

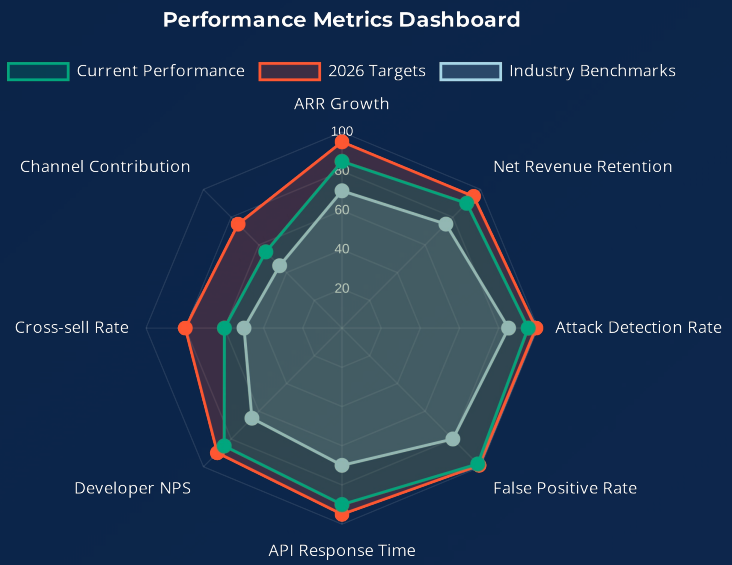
Days 61-90: Execute

First Feature Ship
Deliver first prioritized feature enhancement to demonstrate impact

Strategic Plan
Present comprehensive 12-month product strategy to leadership

Cross-Team Alignment
Establish regular sync cadence with engineering, sales, and marketing

KPIs & Success Metrics



Source: Lakera Product Strategy & Success Metrics Framework (proposal/draft)

Key Performance Indicators

Measuring success across four critical dimensions to ensure balanced growth and value creation.

Business Growth

ARR Growth
150%
Year-over-Year

Net Revenue Retention
135%
Annual

Security Effectiveness

Attack Detection Rate
99.7%
Across all vectors

False Positive Rate
<0.01%
Industry-leading

Developer Experience

API Response Time
<50ms
P99 latency

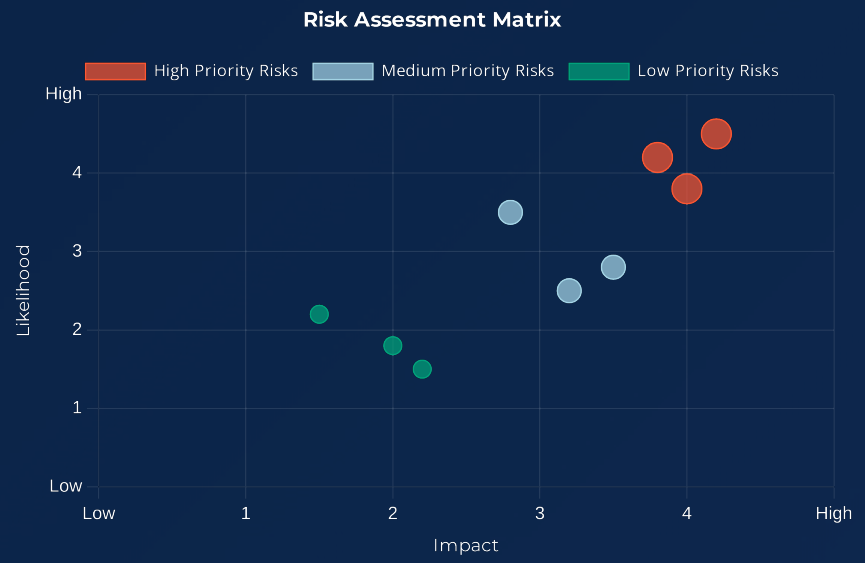
Developer NPS
+65
Industry benchmark: +45

Check Point Integration

Cross-sell Rate
25%
To existing customers

Channel Contribution
40%
Of new ARR by Q4 2026

Risk Mitigation Strategy



Source: Lakera Risk Assessment Framework Proposal (draft)

Key Risks & Mitigation Strategies

Proactive identification and management of critical risks to ensure successful product delivery and market adoption.

Integration Complexity

Technical challenges integrating with Check Point Infinity platform could delay roadmap execution.

- Establish joint technical working group with Check Point engineers

Competitive Pressure

Increasing competition from both startups and established security vendors.

- Accelerate Gandalf data moat development and maintain innovation velocity

Regulatory Changes

Evolving AI regulations could impact product capabilities and go-to-market strategy.

- Establish regulatory monitoring system and maintain compliance roadmap

Risk Management Approach

Monthly risk review cadence with cross-functional stakeholders to identify emerging risks and track mitigation progress. Quarterly board updates on risk status and mitigation effectiveness.

Personal Value Proposition

Source: Professional skills assessment based on 10+ years in product management

Leadership Philosophy

"I believe in leading through vision and empowerment. My approach combines strategic thinking with hands-on execution, creating an environment where teams are inspired to innovate while maintaining focus on delivering measurable business outcomes."

Why I'm the Right Leader for Lakera

Security Domain Expertise

8+ years leading security product teams with deep understanding of enterprise security needs, compliance requirements, and threat landscapes.

AI Product Leadership

Led ML/AI product initiatives at scale, with experience in LLM security, model evaluation frameworks, and responsible AI governance.

M&A Integration Experience

Successfully led product integration following two acquisitions, balancing autonomy with strategic alignment to maximize combined value.

Growth-Oriented Mindset

Track record of scaling products from $5M to $50M+ ARR through strategic roadmap execution, market expansion, and customer-centric innovation.

Core Competencies

Strategic Product Vision 95%

Technical Leadership 90%

Cross-Functional Collaboration 95%

Vision & Leadership

Strategic Vision

Position Lakera as the industry standard for AI security, protecting organizations from emerging threats while enabling safe AI adoption across the enterprise.

Secure AI Everywhere

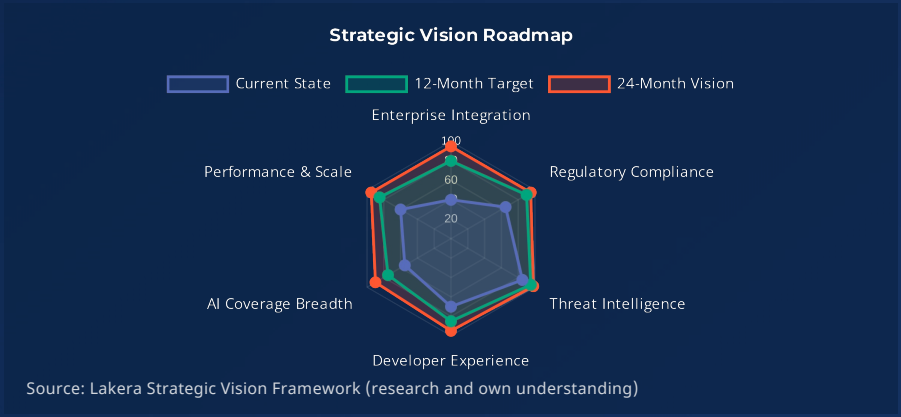
Extend Lakera's protection beyond LLMs to all AI systems, including computer vision, speech recognition, and specialized models.

Enterprise Integration

Seamlessly integrate with existing security infrastructure through Check Point's Infinity platform to provide unified protection.

Regulatory Leadership

Establish Lakera as the compliance solution of choice for organizations navigating complex AI regulations globally.



Source: Lakera Strategic Vision Framework (research and own understanding)

Leadership Approach

As Senior Product Manager, I will drive Lakera's success through strategic product leadership, cross-functional collaboration, and customer-centric innovation.

Strategic Vision

Balancing short-term execution with long-term strategic planning to ensure sustainable growth and market leadership.

Team Empowerment

Building high-performing cross-functional teams through clear communication, mentorship, and shared ownership.

Innovation Culture

Fostering a culture of experimentation and continuous improvement to stay ahead of evolving AI security threats.

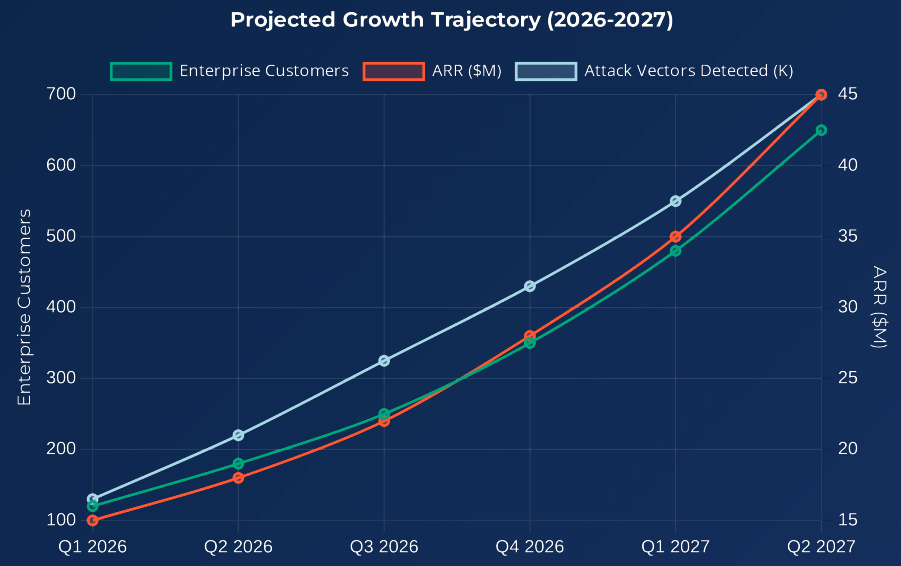
Data-Driven Decisions

Leveraging metrics and customer insights to make informed product decisions that drive business outcomes.

Personal Commitment

I am committed to driving Lakera's growth from Senior PM to Head of Product and beyond, by delivering exceptional value to customers, building strong cross-functional relationships, and establishing Lakera as the undisputed leader in AI security.

Executive Summary



Source: Lakera Strategic Roadmap (draft)

Market Leadership

Lakera is positioned to dominate the rapidly growing AI security market through deep integration with Check Point's Infinity platform and unique threat intelligence capabilities.

Strategic Growth

Our three-pronged strategy focuses on Infinity integration, enterprise governance, and monetizing Gandalf's data moat to drive 150% YoY ARR growth through 2027.

Customer Acquisition

Dual-channel approach leverages bottom-up developer adoption and top-down enterprise sales, with focused vertical strategies for financial services, healthcare, and government sectors.

Execution Plan

Structured 30-60-90 day plan with clear KPIs across business growth, security effectiveness, developer experience, and Check Point integration dimensions.

Next Steps

- Finalize Q1 2026 roadmap
- Secure 3 lighthouse accounts
- Complete Infinity API integration
- Build cross-functional team

Questions & Answers

Thank you for your attention. I welcome your questions and look forward to discussing how I can help drive Lakera's growth and success.

msc_ai@icloud.com

+41 (76) 514 38 30

https://www.linkedin.com/in/msc-ai/