Lorikeet *CORP.*

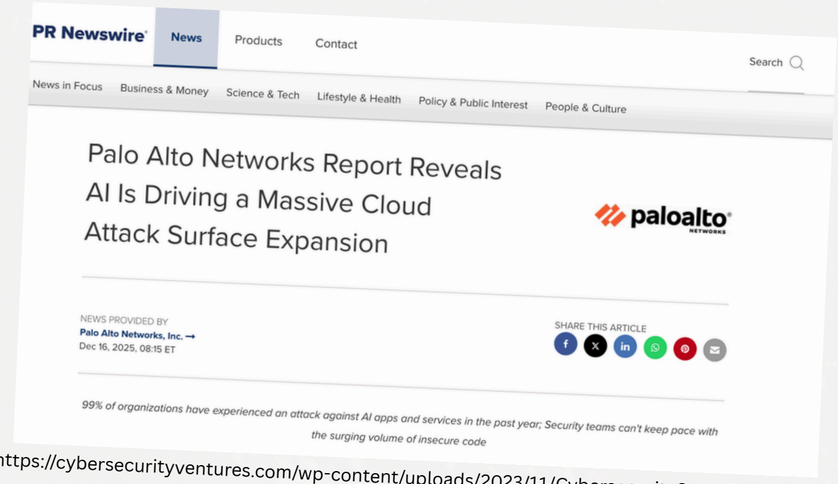
AI-ENABLED ATTACK SURFACE MANAGEMENT, FOR THE MODERN DAY

RYAN WILKE, CEO
JACOB MASSE, COO
19 JAN, 2026

The Problem.

1 You cannot secure what you cannot **see**.

- Organizations lack visibility into unknown assets
- Shadow IT and abandoned services expand exposure
- Orphaned domains and APIs remain live



https://cybersecurityventures.com/wp-content/uploads/2023/11/CybersecuritySpending2031.pdf

2 You cannot patch what you do not **understand**.

- Assets are poorly classified, misattributed, or completely unlabeled
- Security teams lack context around ownership, criticality, and exposure
- Findings are isolated, with no understanding of real attack paths

3 You cannot reduce risk you cannot **measure**.

- No consistent way to prioritize exposures across the attack surface
- Vulnerability data creates noise without business relevance
- Risk decisions rely on intuition instead of objective measures

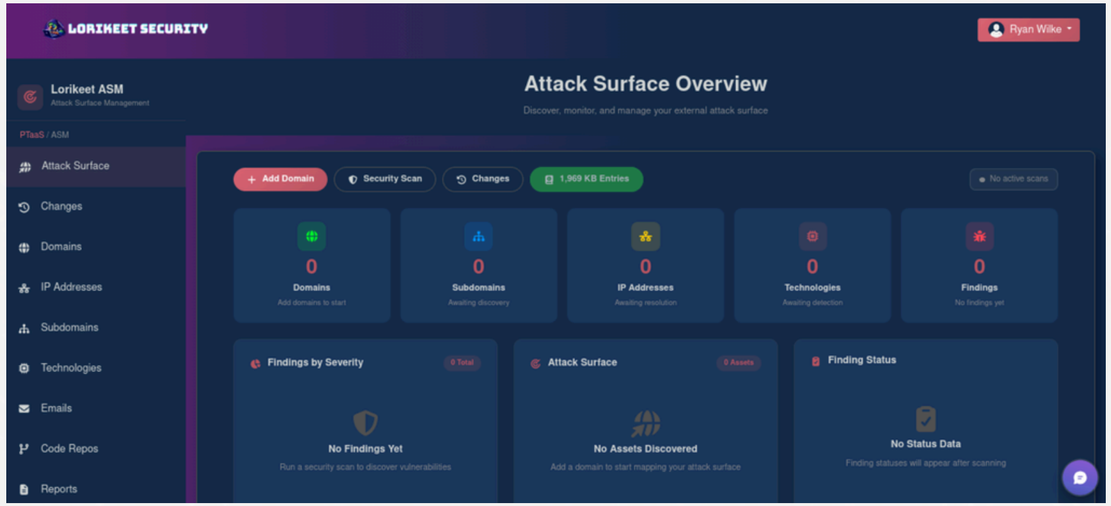
The Solution.

A continuously learning, AI-powered system for attack surface risk control.

Organization Asset Visibility

- Continuously discover the full external attack surface
- Expose shadow IT and forgotten assets
- Stay current as infrastructure changes

Outcome: Teams see what they actually expose.



Breakdown of Complex Findings with AI

- AI correlates assets and exposures into real attack paths
- Explains why findings matter and how they’re exploited
- Fewer alerts, higher confidence

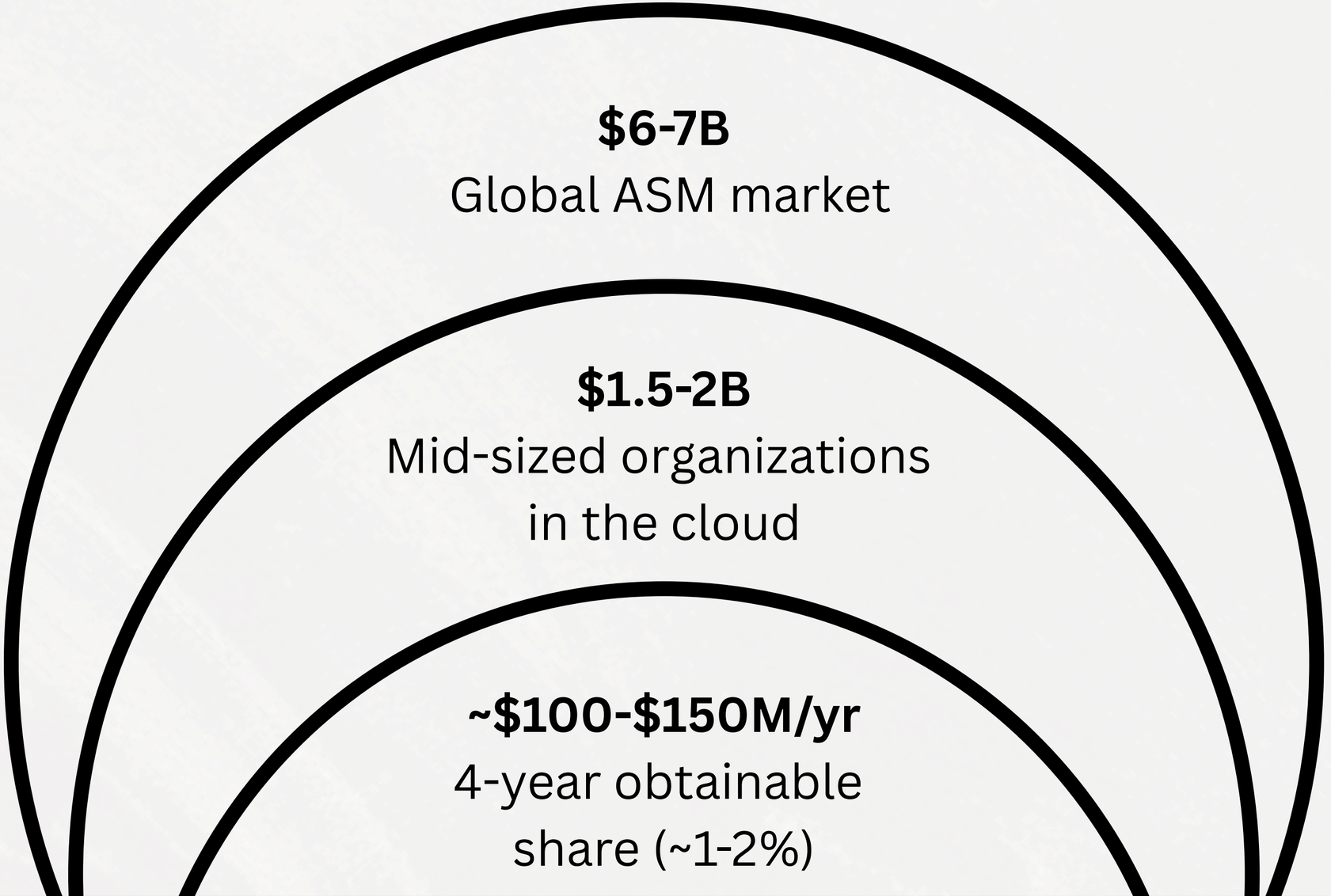
Outcome: Clear risk narratives and faster decisions.

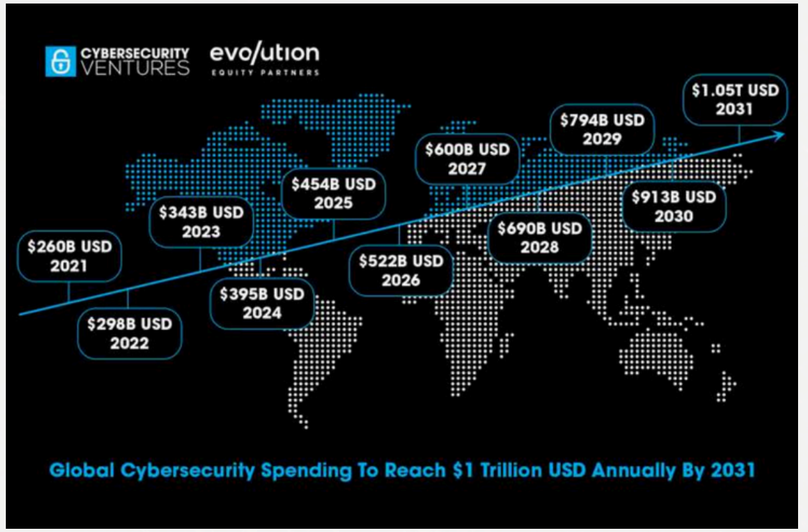
Objective Measuring of ANY Finding

- Score exposures by exploitability and business impact
- Normalize noise across vulnerabilities and misconfigurations
- Fixing top issues measurably reduces risk

Outcome: Teams fix what truly matters first.

Size of Market.





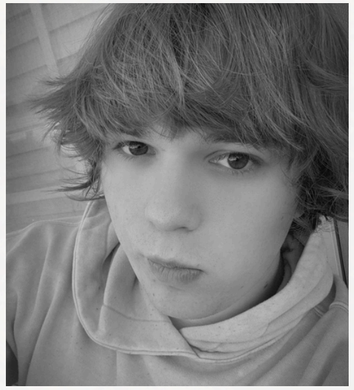
TAM: The global Attack Surface Management market driven by widespread cloud adoption, SaaS sprawl, and increasing external exposure.

SAM: Mid-sized, cloud-first organizations with complex internet-facing assets that require continuous discovery and monitoring.

SOM: A focused, attainable revenue segment representing $100–150M in ARR over four years through targeted enterprise adoption.

The Team.

“Builder of offensive security systems at scale, turning attacker behavior into practical defense intelligence.”



Ryan Wilke

Co-Founder
(eCPPT, eWPT, PCWPT)

- Founder of Parrot CTFs ($10k MRR) with 7 years of industry experience in global offensive security training and pentesting
- Built large-scale pentesting, red team, and SOCaaS infrastructures at Prescient Security & Cointelegraph
- Deep hands-on expertise across web, API, cloud, and offensive security/adversary simulation
- Designed technical hiring processes and security certification programs

“Operator who bridges product, engineering, and security to turn complex risk into scalable platforms.”

Jacob Masse

Co-Founder
(CySA+, eCPPT, Pentest+)

- Founder of traztech, building secure SaaS and automation systems for 5+ years.
- Offensive security engineer with 5+ CVEs (Mirai Botnet Killswitch), with extensive red-team background
- Scaled a bootstrapped server hosting startup to $13k in 1 Quarter
- Head of Operations at VC-backed startup, acquisition in progress by Cloudflare (Confidential)

The Ask: $885,000

Expand Expert Team

- Hire core engineers to build and scale the Lorikeet ASM platform
- Bring in security domain experts to guide detection and prioritization logic
- Add early go-to-market support to validate sales motion and customer fit

Expert hires require competitive salaries, and we need expert hires to stay on the edge of innovation.

Product Improvement

- Expand asset discovery, historical indexing, and monitoring coverage
- Improve AI-driven explanations, prioritization, and usability
- Harden the product for real-world customer environments
- Growing compliance (Vanta) and vCISO partnerships for client upsells (revenue source for Lorikeet)

We need to continually respond to the needs of early-stage users to win over business and snowball our growth.

Infrastructure & Research

- Scale scanning, data processing, and storage infrastructure
- Invest in internal security, reliability, and performance tooling
- Fund ongoing research into new detection techniques and data sources

Being able to scale our infrastructure is crucial to keep up with the scanning/asset profiling needs of our users.

Why Right Now?

AI Has Shifted from a “Feature” to Force Multiplier

- AI now makes large, noisy attack surfaces measurable and actionable
- What security teams couldn’t process manually is now automated and continuous

Security Spend Is Moving from Tools to Outcomes

- Security buyers care about risk reduction and outcomes, not more tools
- CISOs and boards want defensible, business-aligned decisions
- Platforms that reduce noise and prioritize action are replacing point solutions
- Attack Surface Management is becoming table stakes for SOC 2 and enterprise deals

The Problem's Scale.

Breach Cost
U.S. average breach cost:
> $10 M *(IBM 2025)*

The Target
Cloud and internet-exposed infrastructure are **top adversary targets** (*Crowdstrike*)

Asset Count
Average enterprise has **300+ internet-facing assets** *(Tenable market data)*

Market-Fit
[ASM] market is expected to grow to **USD 12.69 billion by 2033**... (*Straits Research*)

Over **80%** of data breaches result from **exploiting the attack surface** *(Cybersecurity Insiders, 2024)* with the average U.S. breach costing $10M per occurrence *(IBM, 2025)*

Future Opportunities

Services & Features

- Predictive exposure and risk insights
- Mandatory compliance asset mapping (SOC 2, ISO 27001)
- Deeper cloud and security integrations (AWS, GCP)
- Broader external risk visibility

Markets

- Expansion from mid-market to large enterprise
- Support for multi-region and regulated organizations
- Global market exposure as we scale (F100, Enterprise, Gov, FinTech, etc.)