weagle

Protection across Browser, Search and LLM

The browser-centric web ecosystem has become fertile ground for invisible attacks across everyday browsing, search and GenAI tools

1

Work, search, GenAI, SaaS and personal life have collapsed into a single browser, so corporate data, private accounts and everyday browsing are mixed in the same sessions

2

The ad- and tracking-driven model constantly injects third-party code into pages, creating a dense supply chain that gives attackers cheap reach and fast-rotating infrastructure

3

Modern browsers run rich, active code alongside user credentials and data, so a single compromised script or extension can quickly turn a normal session into an entry point

4

User habits normalise risky behaviour, as mixed logins, stored passwords and permissive extensions quietly turn everyday browsing into an attack path that users do not perceive as risk

weagle

As a result, a trusted site can flip from news to ransomware with a single click, with no clear warning

Behind a single harmless click, web-based attacks use the full delivery chain to silently deploy malicious content

weagle

weagle

The blind spot of cybersecurity is in the browser and AI, Weagle stops invisible web attacks leveraging its patented approach

New attack surface

- Search, AI prompts and browser activity expose enterprises to hidden cybersecurity threats and data leakage

Traditional defenses fail

- Firewalls, endpoint security tools and modern browsers don’t stop data leakage and hidden threats in web activities

Weagle closes the gap

- Patented technology intercepts and sanitizes company data, blocks invisible web attacks and delivers enterprise control

The browser and AI layer has become the critical frontline where traditional defenses are not effective

Expanded threat vectors

Malvertising, browser-in-the-browser, malicious extensions, AI poisoning and data leakage originate in web and AI activities

Inside enterprise perimeter

These new and advanced threats operate natively in the web browser and AI layer, bypassing network and endpoint visibility and thus security controls

Escalating enterprise risk

These risks span financial, operational and regulatory domains, making protection at the browser and AI layer a strategic priority

weagle

Traditional defenses were not designed for attacks inside the browser and AI and expose companies to hidden threats

Network security stops at the perimeter

Firewalls, SWG and SASE inspect traffic in transit but cannot detect attacks that materialize inside the browser

Endpoint tools miss user-driven risk

EDR focus on device processes, blind to AI prompts, search queries and malicious browser extensions

Secure browsers protect from outside-in

They don’t prevent sensitive data exposure, malvertising or advanced attacks like browser-in-the-browser

DLP coverage incomplete

Traditional DLP fails with AI chat, copy-paste and browser-based data flows.

weagle

Weagle stops hidden browser and AI attacks with a patented protection layer for browser and AI activities

Protection where attacks emerge

Operates directly in the browser and AI layer, intercepting threats that bypass network, endpoint and secure browsers

Patented prevention technology

Blocks malicious content, sanitizes inputs and prevents sensitive data exposure before it could harm the companies

Comprehensive cyber threat coverage

Stops malvertising, browser-in-the-browser, malicious extensions, AI poisoning and data leakage at the source

Enterprise grade governance

CISO dashboard provides visibility, policy control and SIEM/SOC integration for enterprise grade unified security operations

weagle

Weagle is redefining browser and AI security by building a comprehensive enterprise protection layer

2023

Establish the foundation

Browser Plugin | Confidential search | AI chat | Anonymization engine | Mobile

2024

Enable enterprise governance

CISO dashboard | Policy control | SIEM/SOC integration | ISO Certifications

2025

Strengthen runtime protection

Revamped Browser plugin | Malvertising block | Browser in the Browser defense | Extension control | Technology patent

2026

Lead with predictive intelligence

Threat intelligence | Private AI | Extended mobile | Enterprise standard

Advanced enterprise data protection across web search, AI and internet browsing

Advanced protection for hidden attacks targeting web search, AI and browsers

weagle

Advanced attacks in 2025/2026 run in the browser, beyond the reach of network, endpoint, and traditional security tools

Jan 2025

Extension Compromise

A supply-chain attack pushed a malicious update to legitimate extensions, exfiltrating data including cookies and session

Mar 2025

Browser-in-the-Browser

Browser-in-the-Browser overlays to phish steam credentials with realistic fake login pop-ups

Jun 2025

Malicious Browser Extension

A malicious Campaign in LATAM infected users with Chrome, Edge and Brave browsers extension to siphon authentication data

Jul 2025

SEO Poisoning

A threat actor compromised an organization through a SEO poisoning campaign to deliver Akira ransomware

Jul 2025

Malicious Browser Extension

18 malicious extensions in Chrome/Edge, with more than 2.3 million installs, tracked users and hijacked browsing sessions

Aug 2025

Malvertising/SEO Poisoning

Malvertising delivered “PS1Bot,” a modular malware used for info-steal, keylogging and persistence

Sept 2025

Browser-based intrusion

Scattered Spider targeted the browser runtime with Browser-in-the-Browser, session-token theft and malicious extensions

weagle

Weagle would have stopped those attacks with its patented enterprise protection layer, blocking them in the web browser

Malvertising and fake installers

Blocks malicious ads, validates landing pages, enforces download provenance and file reputation, stops drive-by scripts before execution

Browser-in-the-browser attacks

Detects full-screen overlays and window-context anomalies, enforces domain-bound login, blocks credential submission to untrusted origins

Malicious or hijacked extensions

Enforces enterprise allowlist and install control, prevents permission escalation, monitors runtime behavior and auto-disables suspicious extensions

SEO Poisoning

Filters poisoned results and fake pages, prevents malicious installers, blocks command-and-control beacons at the browser layer

Fake browser updates chains

Identifies “update now” kits and redirect patterns, blocks forced downloads, neutralizes injected scripts on compromised sites

AI prompt leakage and poisoning

Redacts secrets and PII in prompts and uploads, anonymizes queries, blocks outbound to untrusted AI endpoints, sanitizes model inputs

Session and token exposure

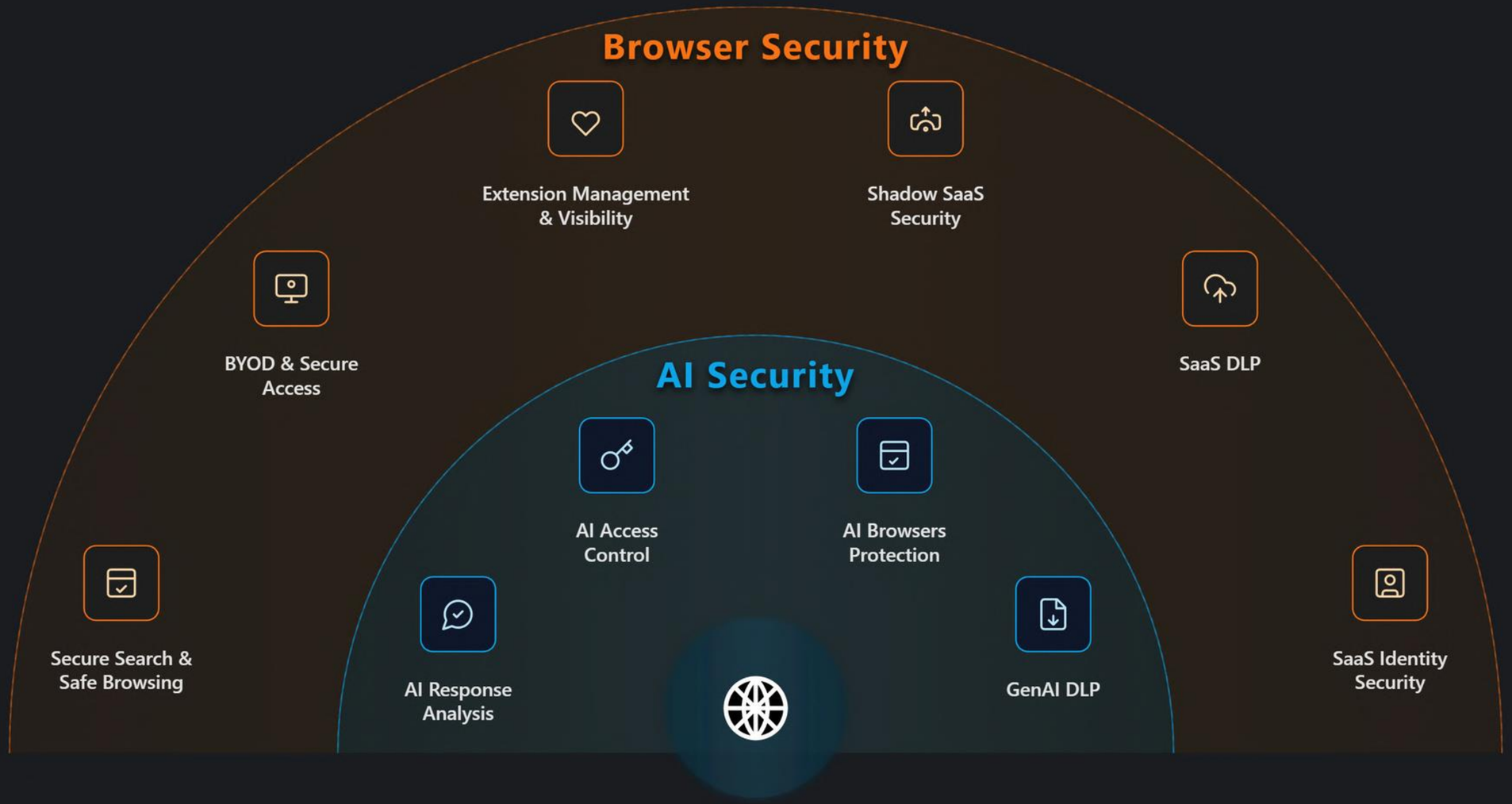
Prevents credential and session data exfiltration via forms, scripts and extensions, enforces policy on session artifacts, alerts SOC in real time

In-browser payload reassembly

Detects and blocks reassembly patterns in WASM/JS/DOM, isolates suspicious execution paths invisible to network and endpoint tools

weagle

Weagle **Unified Security Platform**



weagle

weagle

WEAGLE TEAM

Founders

Lorenzo Cerrone
CEO & Sales
Serial entrepreneur

Andrea Marchica
CTO
Pursuing excellence

Executive team

Massimo Schiattarella
Executive Partner & ex CEO
Unicredit Bank Business Services
Sales Mastery

Pietro Terraneo
COO & Finance
The wise guy

Tommaso Barbacci
R&D & UXUI
The ultimate team player

CISO Advisors

William Harmer
CISO advisor Craft Ventures,
Ex USA CISO Zscaler

Itzik Menashe
CISO Telit,
Ex Talon advisor

Prashant v Jethwa
CISO Bank of Dubai
Ex CISO Lloyds Bank

Advisors

Piero Molino
AI
Ex Uber

Leandro Agrò
Design & Ethics
Ex NTTData

Pancrazio Auteri
Product &
Go-to-market
x3 Exits

TRACTION (Co-design)

We Co-Design our Security Dashboard with these CISOs:

Roberto Barbieri

Head of Cybersecurity @Eni

Oil & Gas

82,000 Employees

Mkt Cap: 47 Bln

Luca Dozio

Head of ICT Security @Illimity

Bank

1,200 Employees

Mkt Cap: 382 Mln

Simone Rizzo

CISO @Haier Europe

Consumer electronics

10,000 Employees

Mkt Cap: 222 Bln

Designed by
Built for CISOs

weagle

weagle

TRACTION (Pipeline)

Qualified

- CSI Piemonte
- Enel
- Robin Hood
- KCB Bank
- Bper Banca
- Banca di Asti
- Unipol
- Wipro
- Corner Bank
- BPS Swiss
- Nestlè Italia
- Withers Worldwide
- Novartis
- F.C. Internazionale
- Gucci
- Etro

Seats: 55,000
ACV: $5.6M

Discussion

- Banco BPM
- Sterling
- Credem Banca
- Moncler
- BNP Paribas UK
- CNP Assurances
- Banca Intesa San Paolo
- Banca Mediolanum
- Banca Sella
- Crypto.com
- Fastweb
- Vittoria Assicurazioni
- Gruppo 24Ore
- Choose Paris Region
- Swisscom
- Ministero MiMiT
- Ministero di Giustizia
- Ministero Finanze MEF
- Ministero Cultura
- Autostrade per l'Italia
- Prada
- AON
- ACI

Seats: 45,500
ACV: $5.5M

Evaluation/PoC

- Eni
- Leonardo
- Lamborghini
- Haier Europe
- Illimity bank spa
- Acea
- Amplifon
- De Nora
- Interpol
- Bologna Airport

Seats: 28,000
ACV:$2.9M

Quote

- Haier Europe
- Illimity bank
- Telecom Italia
- Poste Italiane
- Automotive Cells Company (ACC)
- Impact Advisor
- Iren
- Arera
- Elesa
- A2A
- Maggioli Group
- NLB Bank
- Law Firm Bonelli Erede
- Nexi
- Italgas
- Sumitomo Chemical America
- Unicredit
- Facile.it
- Benelli

Seats: 525
ACV: $130,000

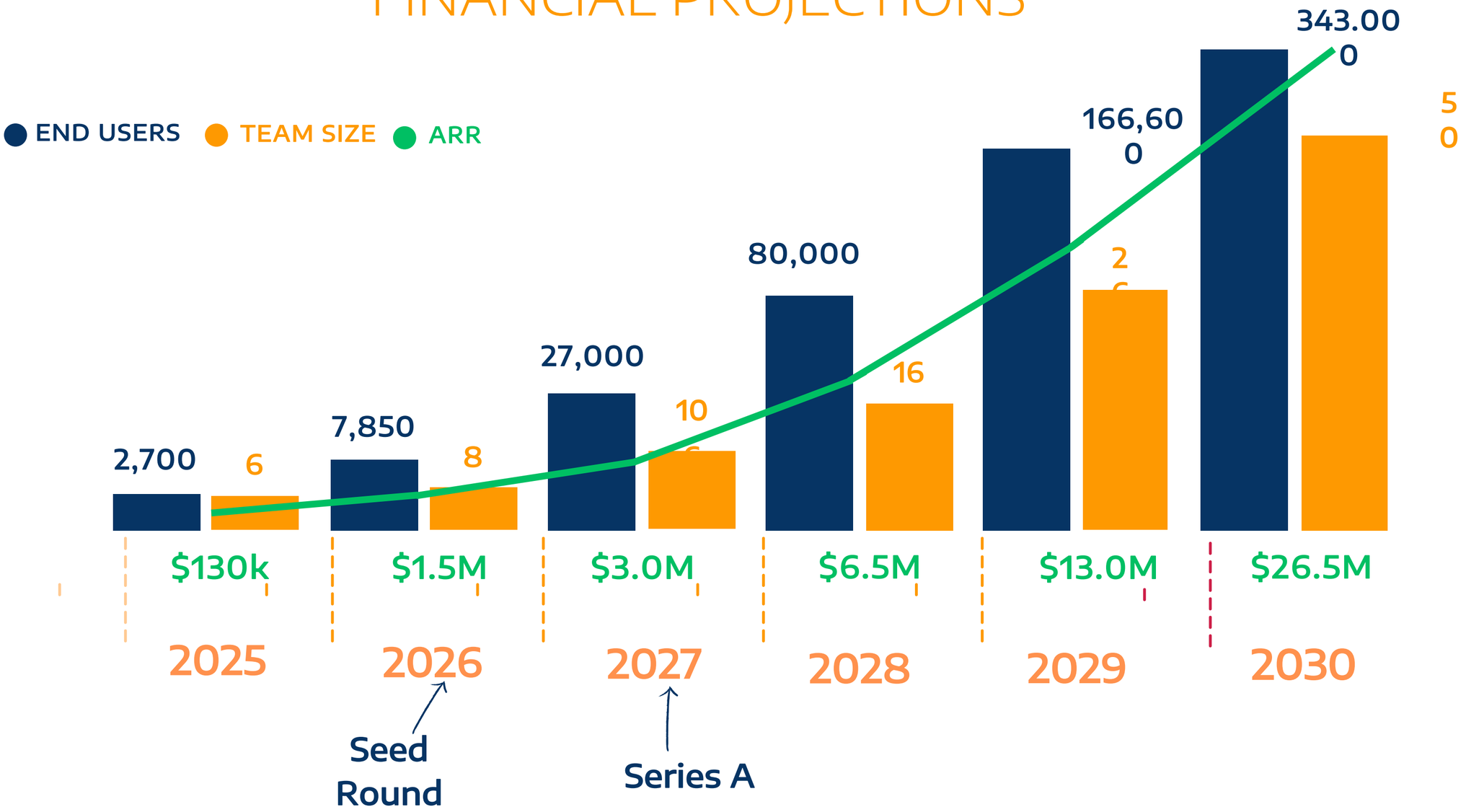
***Most # of Seats and ACV refer to a starting pack on a small % of employees**

TOTAL PIPELINE
ACV:$14.13M

SASE/SSE INTEGRATIONS

FEATURE	Weagle	Talon	Zscaler	Netskope	Symantec (Broadcom)
Primary Focus	Enterprise-grade meta-search engine and AI suite with full data anonymization and privacy controls	Cloud-integrated secure browser with Zero Trust and SASE	Secure access service edge (SASE) platform with zero trust browsing and private app access	SASE solution with integrated secure browser, DLP, and SaaS protection	Legacy DLP solution extended with secure browser features
Security	End-to-end privacy: encrypted search, data masking on AI inputs, data isolation and 24h deletion	SaaS visibility, extension control, and native Zero Trust protections	Inline Zero Trust access, private app segmentation, strong SSL inspection	Deep inspection engine, DLP, CASB, behavior analytics	Focused on advanced DLP, threat detection, and SEP integration
Management	Central CISO Dashboard with risk scoring, KPI visualization, and threat detection insights	Managed via Palo Alto Cortex XDR for unified monitoring	Strong policy engine, identity-driven access controls, and global network enforcement	Admin interface supports SIEM/SOAR; detailed control options	Comprehensive but complex for medium/small orgs
User Experience	Chrome-compatible extension, no ads, clean AI/search interface, customizable dashboard	Chrome-like UI, seamless for end users	Consistent experience across devices; browser agent required	UX varies by org setup; not always intuitive	Designed around compliance, limited flexibility in UX
Best Use Cases	High-privacy industries (finance, legal, pharma), sensitive teams, hybrid workforces	Remote access, secure SaaS workflows, BYOD	Zero Trust access to private apps, hybrid cloud, global distributed teams	SaaS risk management, secure browsing, DLP enforcement	Large-scale legacy deployments, strict regulatory needs
Key Strengths	Only platform combining search, AI, and browsing with full anonymization, CISO controls, and fake news filtering	Tight Palo Alto integration, strong UX, built for Zero Trust from day one	Global SASE infrastructure, mature policy engine, identity-first model	Strong SaaS coverage, multi-layered DLP, cloud-native integrations	Enterprise-grade DLP, trusted compliance framework
Limitations	New market category – requires client education but offers first-mover advantage in enterprise search security.	Tied to Palo Alto environment; less flexible with third-party stacks	Requires full Zscaler deployment for best value; less suited to niche tools	Part of a larger suite, not ideal if browser is the only concern	Outdated interface, high overhead for evolving tech stacks

FINANCIAL PROJECTIONS



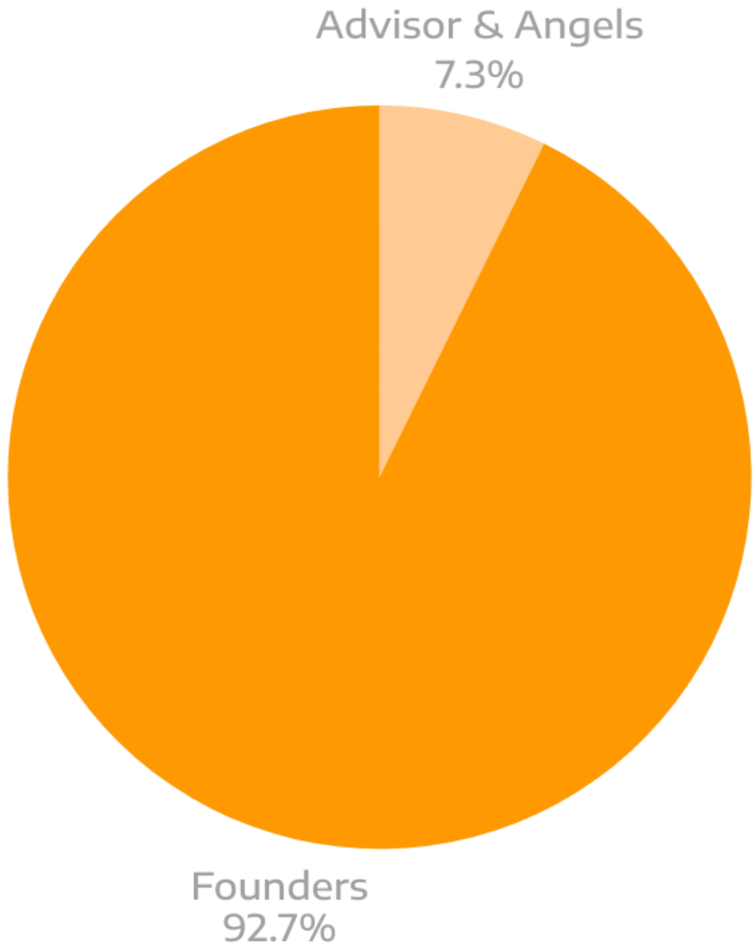
weagle

weagle

WHAT WE ASK

SEEKING $7.000.000

$1.400.000
funds raised to
date



MILESTONES

- Rev target: $1.5M (EoY 2026)
- Integrate with security policy systems, secure browsers (Zscaler, Palo Alto, Netskope...)

USE OF FUNDS

- Hire one sales rep. from industry
- Hire Devs for upgrading product
- find industrial partners
- Marketing for CISOs
- Expand in US, UK and Canada markets

Weagle Flip

Weagle INC. is an incorporated company in Delaware, USA.

CONTACTS

Lorenzo Cerrone, CEO

lorenzo.cerrone@weagle.it

+ 39 333 139 5989

www.weagle.ai

weagle

weagle