WAVESTONE

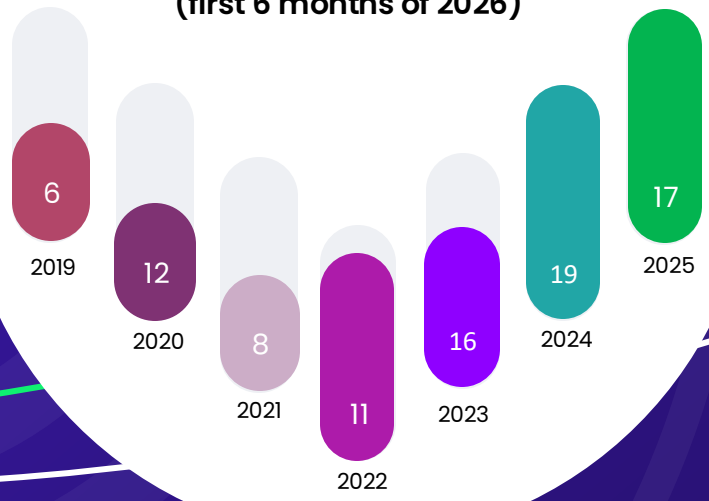
2026

GERMAN CYBERSECURITY STARTUP RADAR

In 2026, startup formation in Germany stabilizes at a solid level

106
Startups

+10
New players
(first 6 months of 2026)



Foreword

The German cybersecurity ecosystem is entering a decisive phase. Driven by increasing regulatory pressure, a rapidly evolving threat landscape, and the growing importance of digital sovereignty, a new generation of startups is reshaping how security is built, deployed, and managed.

This report highlights a selection of early-stage, product-driven cybersecurity startups headquartered in Germany. Rather than focusing on scale alone, the radar intentionally emphasizes innovation, specialization, and the ability to respond to emerging regulatory and technological challenges.
What becomes clear is that German cybersecurity startups are international by design. They address global markets from day one, align their solutions with European regulatory frameworks such as NIS2, DORA, and the Cyber Resilience Act, and increasingly position compliance as a core product capability rather than a constraint.
At the same time, the nature of cybersecurity innovation is shifting. Security is no longer treated as a standalone technical function. Instead, it is becoming deeply embedded in product development, business decision-making, and data governance. Topics such as AI security, product security, and automated compliance are gaining significant traction, reflecting both customer demand and regulatory momentum.
This radar aims to provide decision-makers with a structured and fact-based overview of this evolving landscape. It supports large organizations in identifying relevant partners, technologies, and trends, while also contributing to the visibility and growth of the German cybersecurity startup ecosystem.
We hope this report serves as a practical tool for navigating a market that is becoming increasingly complex, fast-moving, and strategically critical.

Selection criteria for the radar startups

This radar exclusively features startups operating in the cybersecurity domain.
The following eligibility criteria were applied to select the companies included in this analysis.

<7 years in the market

Only startups founded within the last seven years are considered. This threshold ensures the radar captures companies in their early growth phase, where innovation and agility are at their peak. It also reflects the fast-moving nature of cybersecurity, where recent entrants are more likely to address emerging threats and regulatory shifts.

<35 employees

Startups with fewer than 35 employees are included to maintain a focus on early-stage companies. This size constraint filters out more mature organizations and highlights lean, fast-moving teams. It ensures the radar surfaces emerging players that are still in their foundational phase of product development and market entry.

Headquartered in Germany

The startup must be headquartered in Germany. This geographic filter ensures the radar provides a focused view of the domestic cybersecurity innovation landscape. It captures companies that are building solutions within the German regulatory and market environment, including compliance with frameworks such as NIS2, DORA, and the EU Cyber Resilience Act.

<50% consulting activities

Startups must derive less than half of their revenue from consulting or professional services. This criterion ensures a focus on product-driven and technology-first business models. Companies that primarily sell consulting are excluded, as the radar aims to highlight scalable solutions rather than service-based offerings.

Methodology

The final dataset prioritizes quality over quantity, ensuring a clean, comparable, and innovation-focused startup set for further analysis.

Eligibility criteria

- German startup
- <7 years
- <35 employees
- Cybersecurity focus
- <50% consulting activities

The approach

A structured filtering approach was applied to refine a broad initial longlist of cybersecurity-related companies into a focused set of 106 relevant startups. Companies with a high share of consulting or project-based business models were excluded, as well as more mature players with over 35 employees. In addition, around 25 startups were removed due to insolvency or clear market exit. The resulting dataset focuses exclusively on active, product-centric and early-stage cybersecurity startups, ensuring a high-quality and comparable basis for further analysis.

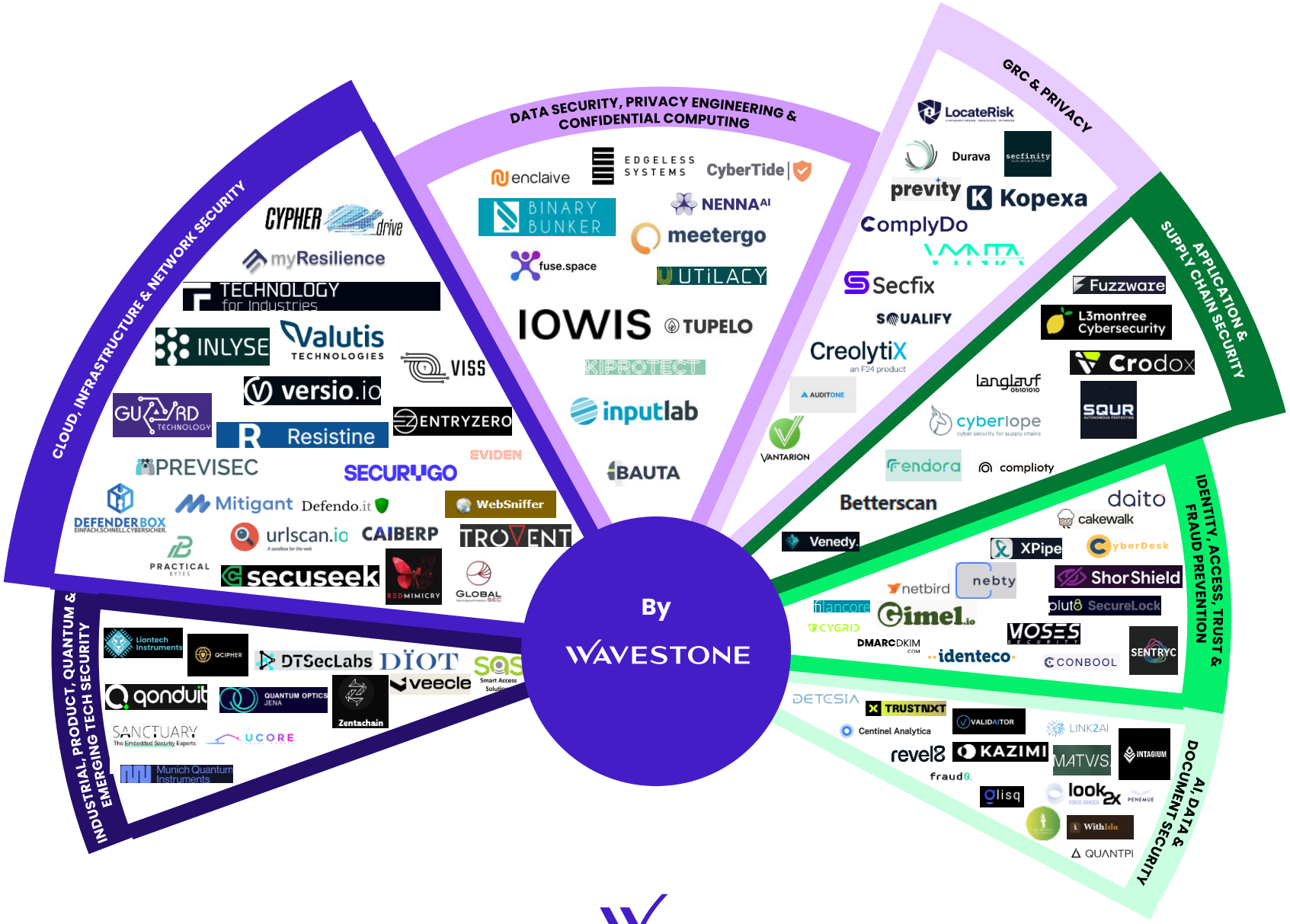
Results

> **300+**
> Cybersecurity startups

> **200+**
> Excluded due to mismatch with the criteria

> **106**
> Startups selected

The German Cybersecurity Startup Radar 2026



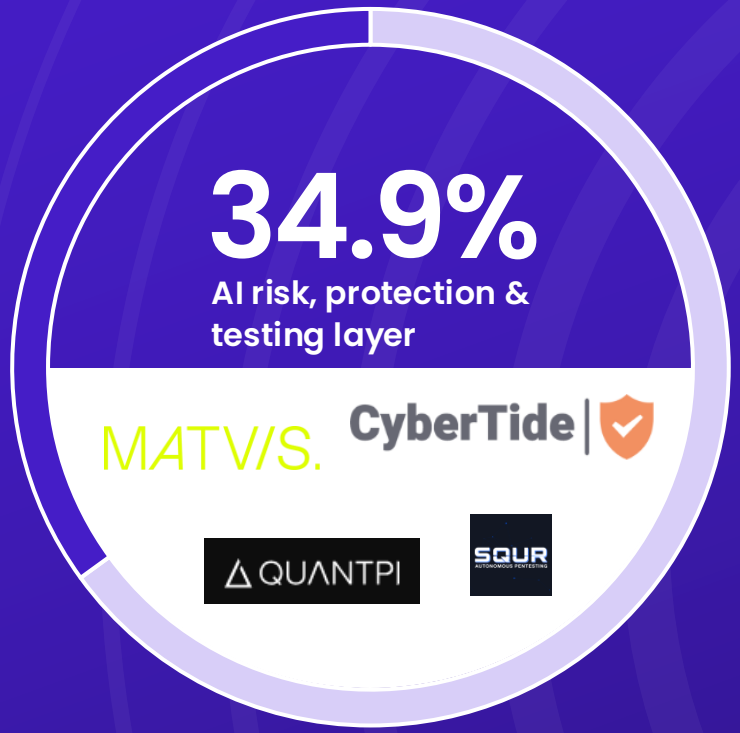
Market shift: regulation, AI, and product security now drive innovation

A clear pattern emerges among younger startups (2023–2026):

- Strong focus on GRC, NIS2, DORA, EU AI Act, Cyber Resilience Act (CRA)
- Security is no longer treated as an isolated technical discipline, but as:
  - a product development capability (CRA, Product Security, SBOM/HBOM),
  - a management and decision-support function (risk quantification, audit automation).

Innovation is increasingly driven by European regulation and operationalization of compliance, not primarily by new attack techniques.

Key segments drive the cybersecurity startup landscape



Rapidly growing segment addressing emerging risks from AI adoption

Driven by regulatory pressure and demand for automation

Critical layer securing access in increasingly complex environments

AI is present across the cybersecurity startup landscape

Solutions reimagined by AI

Startups that accelerate
security solutions using AI

AI-accelerated penetration testing

SQUR · DEFENDERBOX · REDMIMICRY · DTSecLabs

AI-accelerated resilience

CyberTide · ENTRYZERO · versio.io · GUARD TECHNOLOGY

AI-accelerated third-party management

CYGRID · VALIDAITOR · ComplyDo

AI-accelerated SOCs

CyberDesk · Resistine · DÏOT

Deep tech solutions

Deep tech companies building
core technologies for demanding environments

Data encryption

EDGELESS SYSTEMS · enclaive · qonduit · UTiLACY

Secure development

Fuzzware · Fendora · langlauf 0b101010 · ScanDog

Hardware-enforced runtime security

CYPHER drive · VISS · Valutis TECHNOLOGIES · Liontech Instruments

Identity Access Management

cakewalk · ShorShield · daito

AI is everywhere, but rarely truly “AI-first”

AI AS THE CORE

30% (32)
of startups
have AI as the core of their product

- **Use of AI for Security Automation & Threat Detection**
- **Protection of AI and LLMs with specialized AI models**
- **Managing Governance and Compliance**

AI AS SUPPORT

52% (55)
of startups
use AI in their products to accelerate and enhance the value of cyber activities

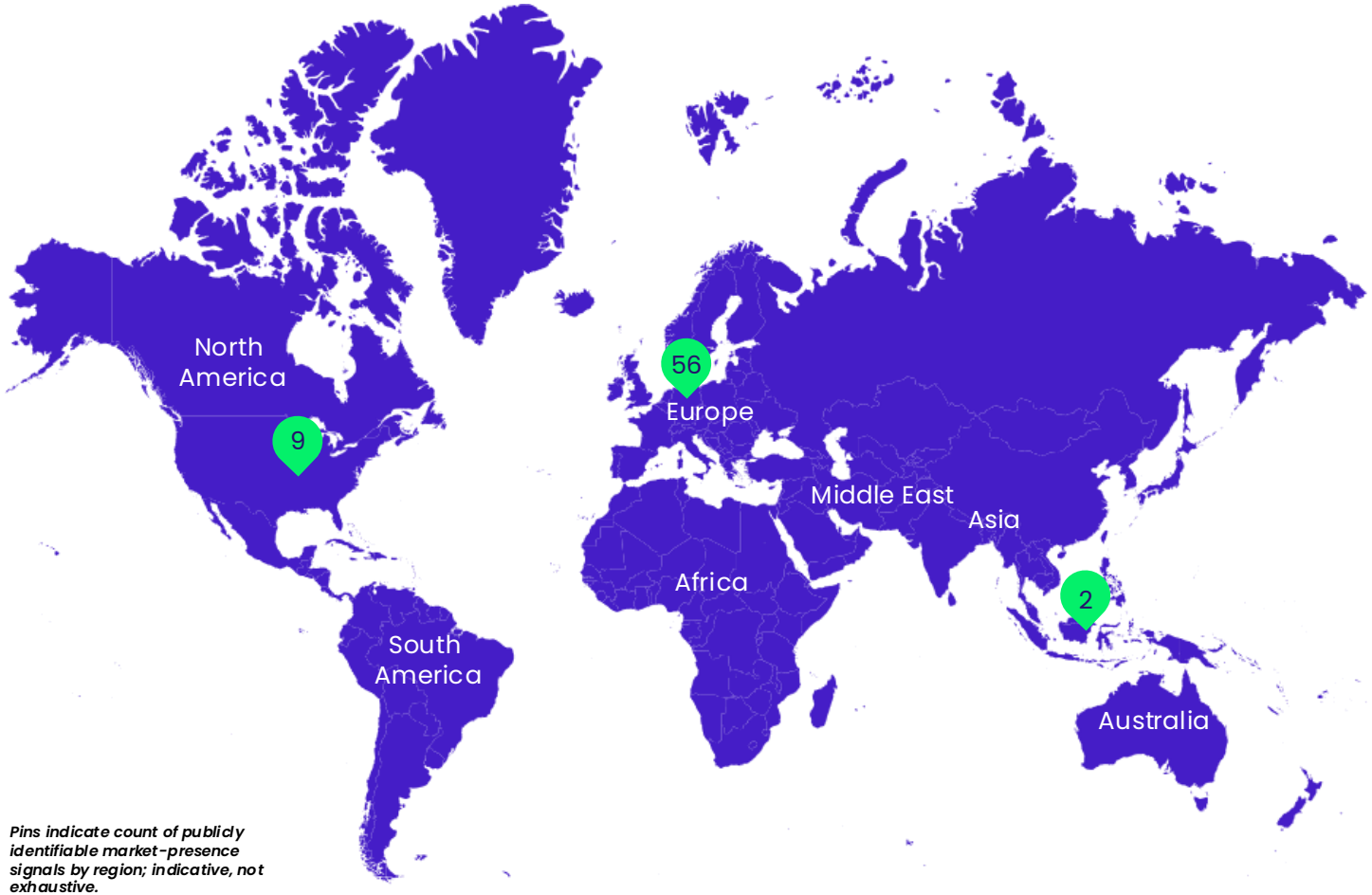
- **36% use Predictive AI**
- **46% use Generative AI**
- **11% of companies use AI Agents**

AI: between risk and opportunity for cybersecurity

AI is a major accelerator in cybersecurity, enhancing automation, productivity, and real-time threat detection. Nearly half of AI-driven solutions now rely on generative models and over one-third on predictive analytics. At the same time, AI enables faster and more sophisticated attacks, from deepfakes to automated exploits. This creates an “AI vs. AI” dynamic, where organizations must defend against increasingly advanced threats. AI is therefore both a critical opportunity to strengthen security and a source of new risks that must be actively managed.

Global footprint: German startups internationalize early

A screening of 106 German cybersecurity startups indicates early international go-to-market orientation.
Among the ~40 to 50 companies with publicly verifiable market signals, internationalization appears to be a core GTM pattern rather than a later scaling step.



Pins indicate count of publicly identifiable market-presence signals by region; indicative, not exhaustive.

~84%
of companies with public market signals target EMEA as primary market

~14%
show an active North America presence

~3%
show APAC expansion signals

~69%
reference international enterprise clients

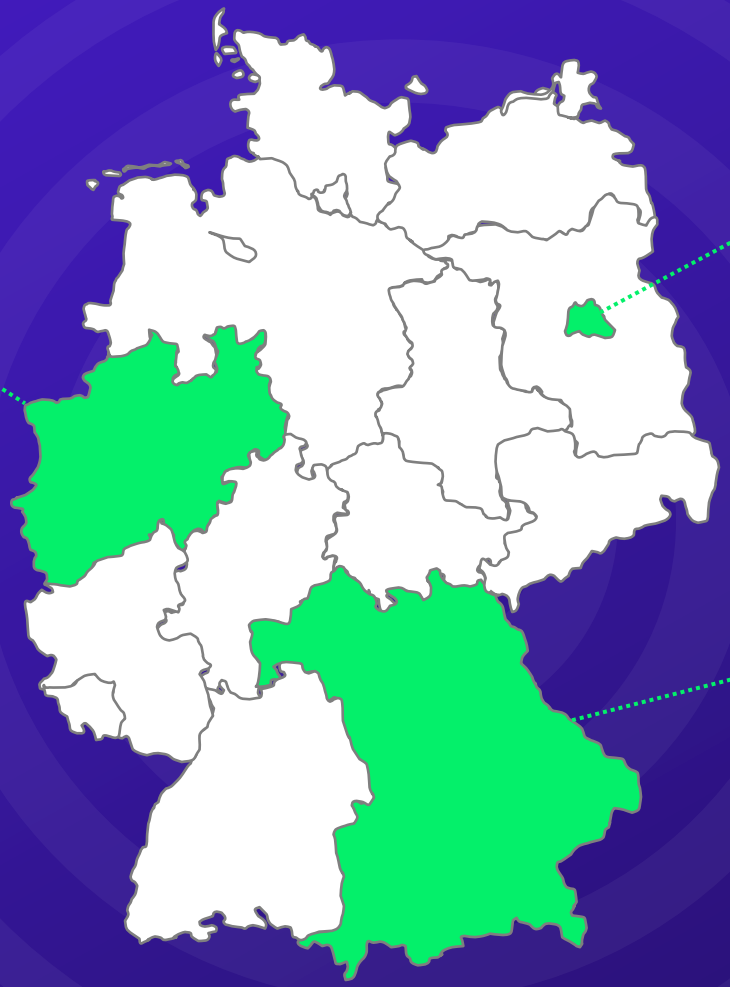
Three regions dominate Germany's startup ecosystem

15.1%

North Rhine-Westphalia

Large industrial base enabling practical B2B security solutions

Berlin, North Rhine-Westphalia, and the southern cluster around Bavaria and Baden-Württemberg stand out as the most active hubs in Germany's cybersecurity startup ecosystem.



24.5%

Berlin

Strong VC presence and startup density driving continuous growth

14.2%

Bavaria

Strong research ecosystem fueling deep-tech innovation

Three funding models clearly stand out

Based on interviews, we found that a significant share of startups relies on grants and bootstrapping, underlining the strong role of research-driven innovation and public support. At the same time, the presence of VC-backed and hybrid models indicates a clear progression toward scalability, with many companies transitioning from publicly funded development to growth-oriented private capital.

Bootstrapped/grants

40-60%

VC-backed

25-35%

Hybrid

15-25%

*Estimates based on publicly available funding data and expert interviews

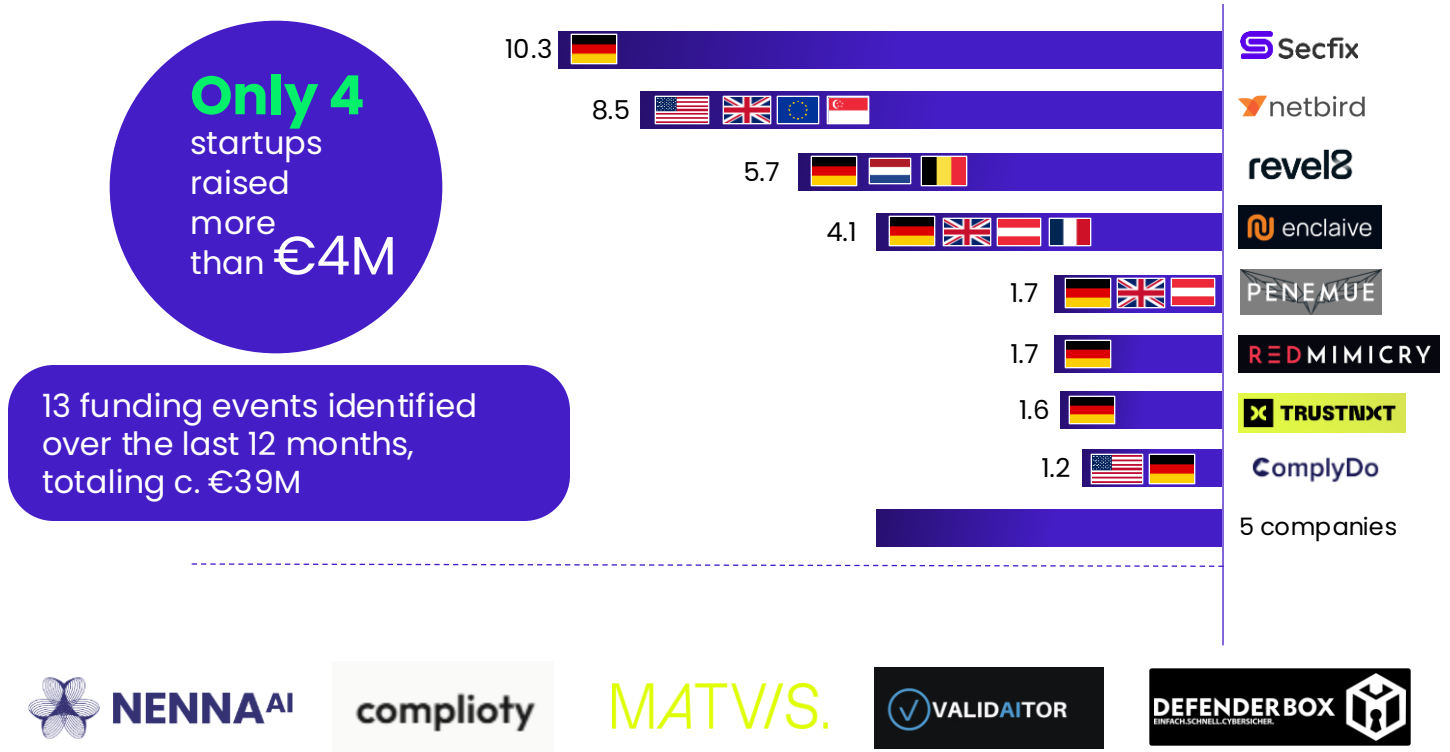
Funding momentum is visible, but highly concentrated

Publicly identifiable funding in the 106-company cohort is driven by a small set of larger seed and Series A rounds.

- Funding is no longer anecdotal: several in-scope companies raised institutional rounds in the last 12 months.
- The market is not yet broad-based: most capital is concentrated in a handful of clear category leaders.
- The disclosed funding base understates the market because several rounds are undisclosed or only reported as “seven-figure” rounds.

Only 4 startups raised more than €4M

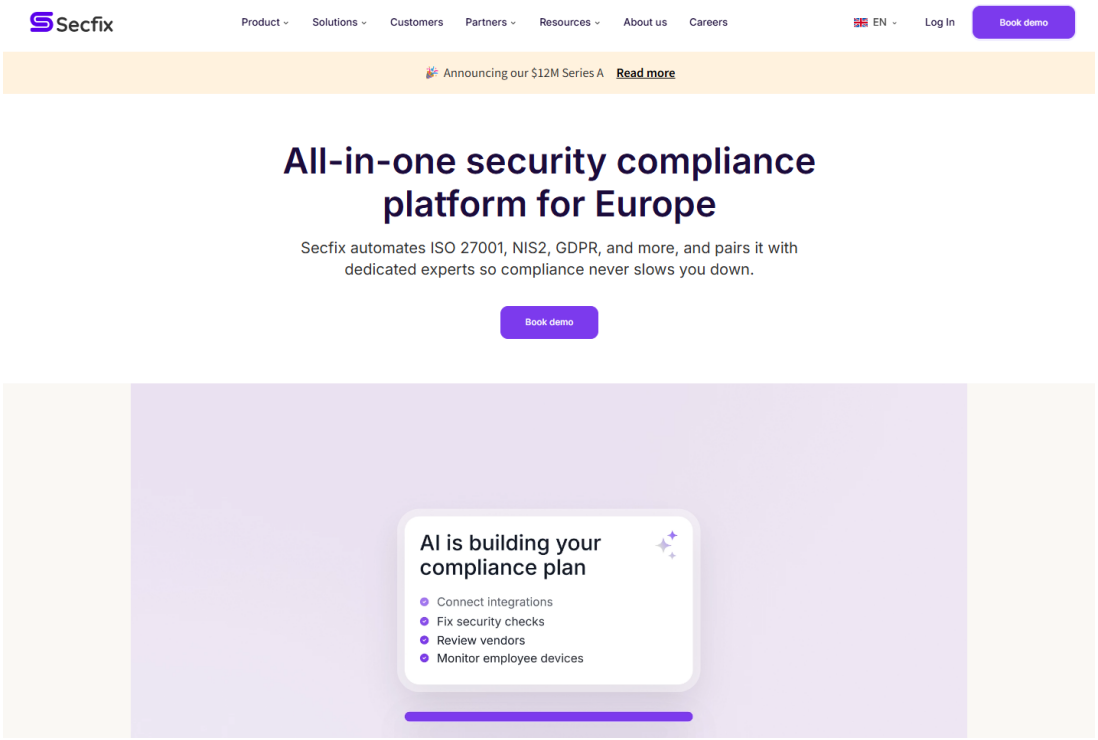
13 funding events identified over the last 12 months, totaling c. €39M



Distribution of fundraising

in €M, June 2025 to May 2026

Focus on Secfix



Objectives

Automate security and compliance processes (e.g., ISO 27001, SOC 2, TISAX). Reduce manual GRC workload for SMB/mid-market companies. Enable continuous compliance instead of point-in-time audits.

Resources

Strong early funding (~€15M). Lean, product-driven team (~35 FTE). Clear positioning in the compliance automation/GRC SaaS space. Focus on European regulatory environment (incl. GDPR alignment).

Ambition

Build the leading European platform for automated compliance. Standardize security programs for fast-growing companies. Expand from compliance automation to continuous security management.

Fundraising
~€15 million

Founded
2021

Employees
~35

Founders
Fabiola Munguia, Grigory Emelianov, Branko Džakula

Headquarters
Munich

Focus on NetBird

Objectives

Build an open-source Zero Trust networking platform to replace legacy VPNs and enable secure access to private infrastructure across remote, cloud, and hybrid environments.

Resources

NetBird has raised approximately €12.5–13.6M in disclosed funding. The company was founded in 2021/2022, has approximately 10–20 employees, and was founded by Mikhail Bragin and Maycon Santos.

Ambition

Become the European open-source alternative to legacy VPN and proprietary ZTNA providers, scaling from a developer-led open-source product into a global secure connectivity platform.

Fundraising
~ €13.6 million

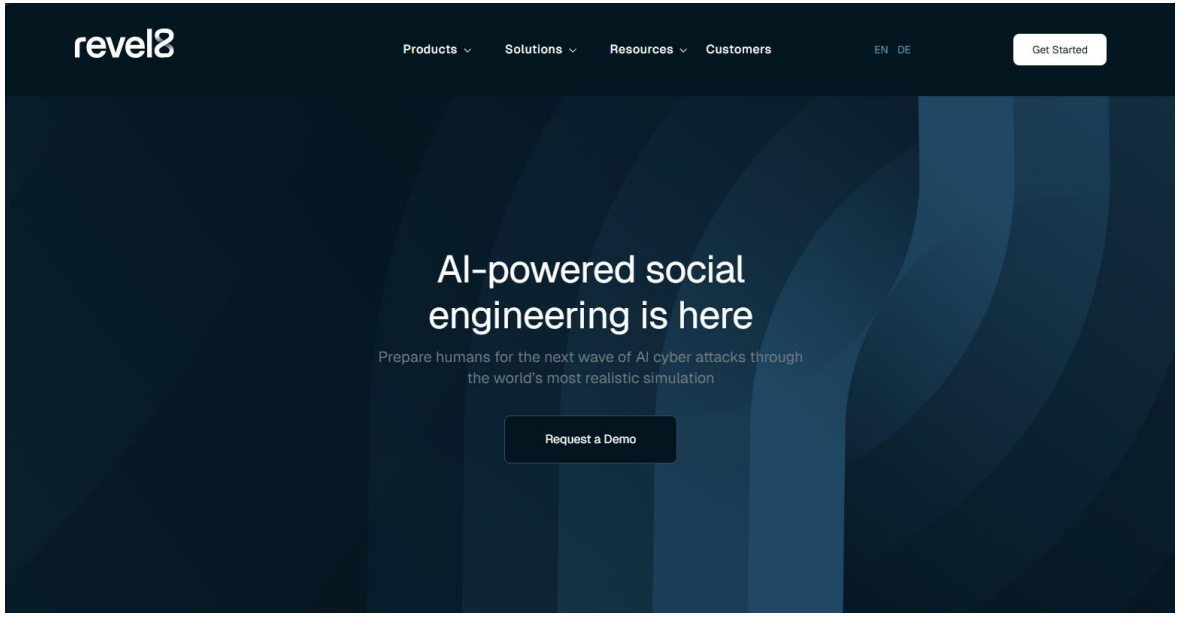
Founded
2021

Employees
~20

Founders
Mikhail Bragin
Maycon Santos

Headquarters
Berlin

Focus on revel8



Objectives

Build a cybersecurity awareness platform that prepares employees for AI-powered attacks through deepfake, phishing, and multi-channel attack simulations. The platform uses OSINT-based personalization and real-time micro-trainings to turn employees into an active "human firewall."

Resources

revel8 has raised €7.0M in total disclosed funding, including a €5.7M seed round led by Peak with participation from Fortino Capital, Merantix Capital, and business angels.

Ambition

Become Europe's category leader for AI-native human-risk cybersecurity by training 10 million "human firewalls" and helping enterprises defend against the next generation of GenAI-enabled impersonation, deepfake, and social engineering attacks.

Fundraising
~ €7.0 million

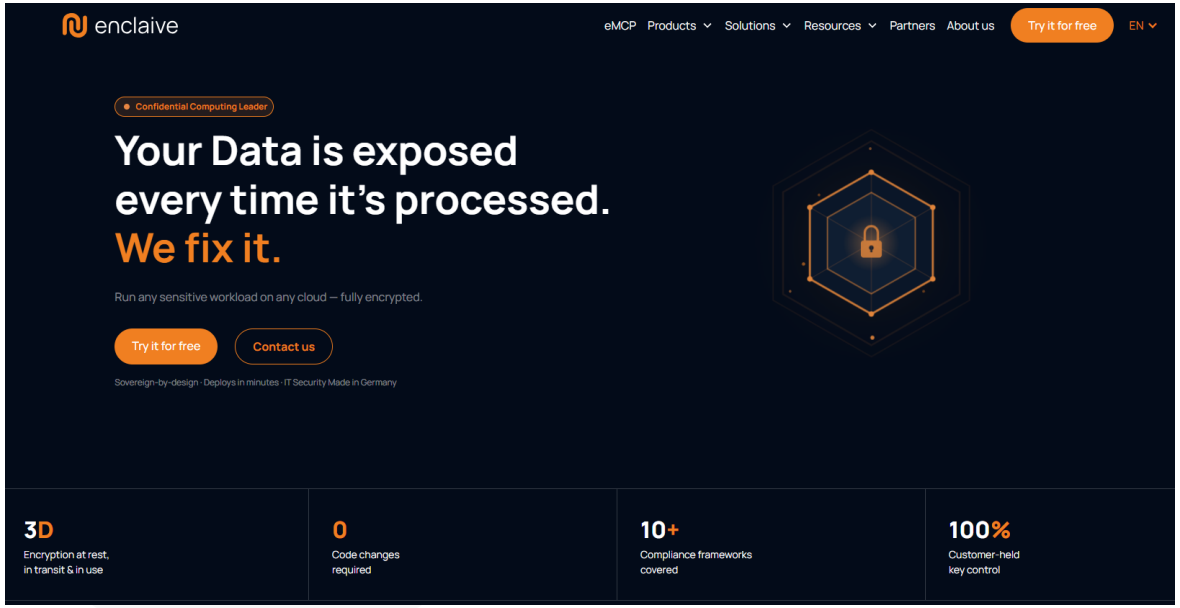
Founded
2021

Employees
~30

Founders
Julius Muth, Tom Müller, Robert Seilbeck

Headquarters
Munich

Focus on enclaive



Objectives

Build a confidential computing platform that protects sensitive data, applications and AI workloads during processing across multi-cloud environments.

Resources

enclaive has raised approximately €5.75M in disclosed funding. The company was founded in 2022 by Andreas Walbrodt and Prof. Dr. Sebastian Gajek and has around 20 employees.

Ambition

Become a leading European platform for confidential multi-cloud and confidential AI, enabling regulated enterprises to use public cloud infrastructure without exposing sensitive workloads or data.

Fundraising
~ €5.75 million

Founded
2022

Employees
~20

Founders
Andreas Walbrodt, Sebastian Gajek

Headquarters
Berlin

Questions?

Find out more about our 2026 radar on our website

Bernd WEGMANN
bernd.wegmann@wavestone.com
Senior Manager

Alexander GETTE
alexander.gette@wavestone.com
Senior Consultant

Kai KOPPER
kai.kopper@wavestone.com
Associate Consultant

With the operational support of:

Gabriela Celina LEMBKE

Kjell ZIEGERT

Poran BHUIYA

WAVESTONE

About Wavestone

Born from the rise of digital innovation, Wavestone has evolved into a leading consulting firm positioned at the convergence of business and technology. It helps the world's leading organizations scale new ways of working, transform operations and reinvent business models in the age of AI.

With 6,000 employees across Europe and North America, Wavestone combines business, transformation and technology capabilities to deliver end-to-end consulting services. AI has been embedded across the firm's expertise and ways of delivering services, enabling clients to translate its potential into tangible and sustainable value.

Wavestone is listed on Euronext Paris and has been certified as a Great Place to Work®.


WAVESTONE