

The European TrustTech Report

2024 | G+D Ventures

This report delves into the European TrustTech startup ecosystem. TrustTech refers to technologies dedicated to securing digital ecosystems and fostering trust across various digital interactions and transactions.

What you can expect in this report:

Investment Landscape: Insights into venture capital activities, funding rounds, and the overall growth of investments in TrustTech companies.

Regional Analysis: Geographical distribution of TrustTech initiatives and funding across Europe, showcasing where the most significant developments and investments are happening.

Exits: Review of the major exits in the TrustTech space.

Deepfake Detection Searchfield: An analysis and segmentation of the deepfake detection market.

G+D Ventures

Backed by the G+D Group and the European Investment Bank, G+D Ventures is a financially-oriented VC, focusing on early-stage TrustTech companies.



G+D Ventures

G+D Ventures is active since 2018 and founded by experienced Venture Capitalists. We are a theme-driven investor focusing on growth-oriented companies, whose innovations promote and protect trust in our society. With this goal in mind, we established a €50m co-investment vehicle with the European Investment Bank and G+D, dedicated to investing in early-stage European TrustTech startups. We designed this fund to move quickly, driven by financial returns, while leveraging the support of G+D's business units. With the G+D Group's backing and decades of venture capital investing experience in both financial and corporate settings, we leverage our unique, global trust network to open doors for our portfolio companies.



Michael Hochholzer
Managing Director



Assaf Shamia
Investment Partner



Andreas Barthelmes
Investment Manager



Alberto Pérez Arranz
Investment Manager



Ena Uffelmann
Investment Analyst

TrustTech secures the digital ecosystem across four layers

TrustTech is framework of technologies designed to **establish, secure, and restore trust** in digital and real-world interactions. At its core, TrustTech ensures that digital environments are safe, transparent, and reliable, addressing risks such as cyber threats, data breaches, fraud, identity theft, misinformation, and regulatory non-compliance.



Ethical

Addressing digital trust challenges beyond compliance by embedding ethical safeguards. Solutions detect and mitigate fake news, online abuse, counterfeiting, and others to uphold the integrity of digital interactions and prevent manipulation.

Regulatory

Ensuring compliance with existing regulatory frameworks to protect the rights of transacting parties. Solutions for anti-money laundering, fraud detection, automated compliance, and others are on this layer.

Identity

Ensures that only verified and authorized entities participate in digital interactions through KYC solutions, self-sovereign identity, biometric authentication, security identity management and others...

Digital Infrastructure

The backbone of digital trust, ensuring secure and resilient systems for data, transactions, and communications using encryption, secure computing, AI-driven threat detection among other technologies.

The World Economic Forum ranked disinformation in the **top five** global risks for 2025 and for the next 10 years.⁴

An estimated **\$52.3 Bn** of cryptocurrency was received by illicit addresses in 2024, involving business with sanctioned entities, scams...³

Deepfakes account for **40%** of all biometric fraud cases. In 2024 digital document forgeries spiked by **244%** year-over-year.²

Expected cost of cybercrime for 2028¹ is estimated at **\$13.8 Tn**, driven by AI-powered attacks.

1 Statista, 2 Entrust 3 Deloitte, 3 Chainalysis, 4 WEF

Notable European TrustTech startups

€ xx m Total raised

quantexa
 AI-driven decision intelligence platform
 HQ: London, UK
€472m

copper
 Digital asset custody and management
 HQ: Zug, Switzerland
€313m

SHIFT
 AI-powered insurance decision automation
 HQ: Paris, France
€266m

UAWULT
 Secure multi-cloud data storage solutions
 HQ: Lisbon, Portugal
€215m

immersive
 Cybersecurity skills development platform
 HQ: Bristol, UK
€172m

Aztec
 Decentralized privacy network (Ethereum)
 HQ: London, UK
€121m

COMPLY ADVANTAGE
 Anti-money laundering & compliance solutions
 HQ: Zug, Switzerland
€119m

ZAMA
 Fully homomorphic encryption solutions
 HQ: Paris, France
€112m

IDnow. GDV Exit
 Identity-verification-as-a-service
 HQ: Munich, Germany
€111m

SEON
 Anti-money laundering & compliance solutions
 HQ: Budapest, Hungary
€97m

DataGuard
 Data protection and compliance
 HQ: Munich, Germany
€81m

INFOSUM
 Privacy-first data collaboration platform
 HQ: Hampshire, UK
€79m

DataDome
 Cyberfraud and bot protection solution
 HQ: Paris, France
€71m

sosafe
 Cybersecurity awareness training
 HQ: Cologne, Germany
€64m

eye
 SME cybersecurity solutions
 HQ: The Hague, Netherlands
€57m

G+D Ventures | The European **TrustTech** Report

European **TrustTech**

Deals | Companies | Investors | Exits



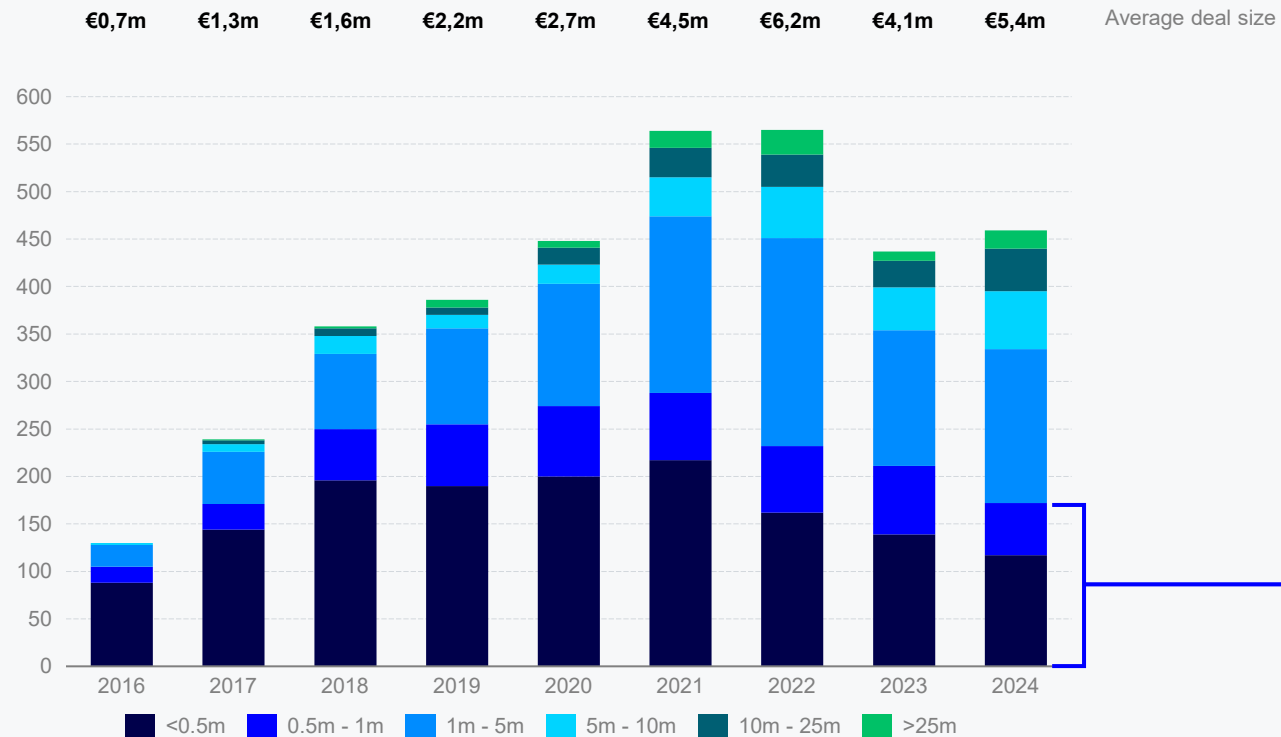
Ena
Uffelmann

Damla
Üstündag

The next wave of TrustTech startups is focusing heavily on agentic AI-enabled solutions

Number of deals¹ per deal category and overall average deal size per year

Source: PitchBook Data, Inc.



¹ Only known deal sizes

Data has not been reviewed by PitchBook analysts.

An analysis of the **accelerator-backed and pre-seed** deals uncovers a new wave of startups tackling TrustTech challenges. These companies mark the start of a new innovation cycle and shed light on the **upcoming TrustTech trends**.

~22% of pre-seed TrustTech startups focus on **AI-driven enterprise search and workflow automation**, streamlining operations, enhancing decision-making, and ensuring compliance.

Close behind is **autonomous cybersecurity** at 16%, with startups using agentic AI for threat detection and monitoring, predictive analytics and response.

Nearly 14% are building solutions for **financial compliance automation**, leveraging automated risk assessment to enhance trust, efficiency, and regulatory adherence. Another 14% are using AI agents to automate the **software development and testing process**.

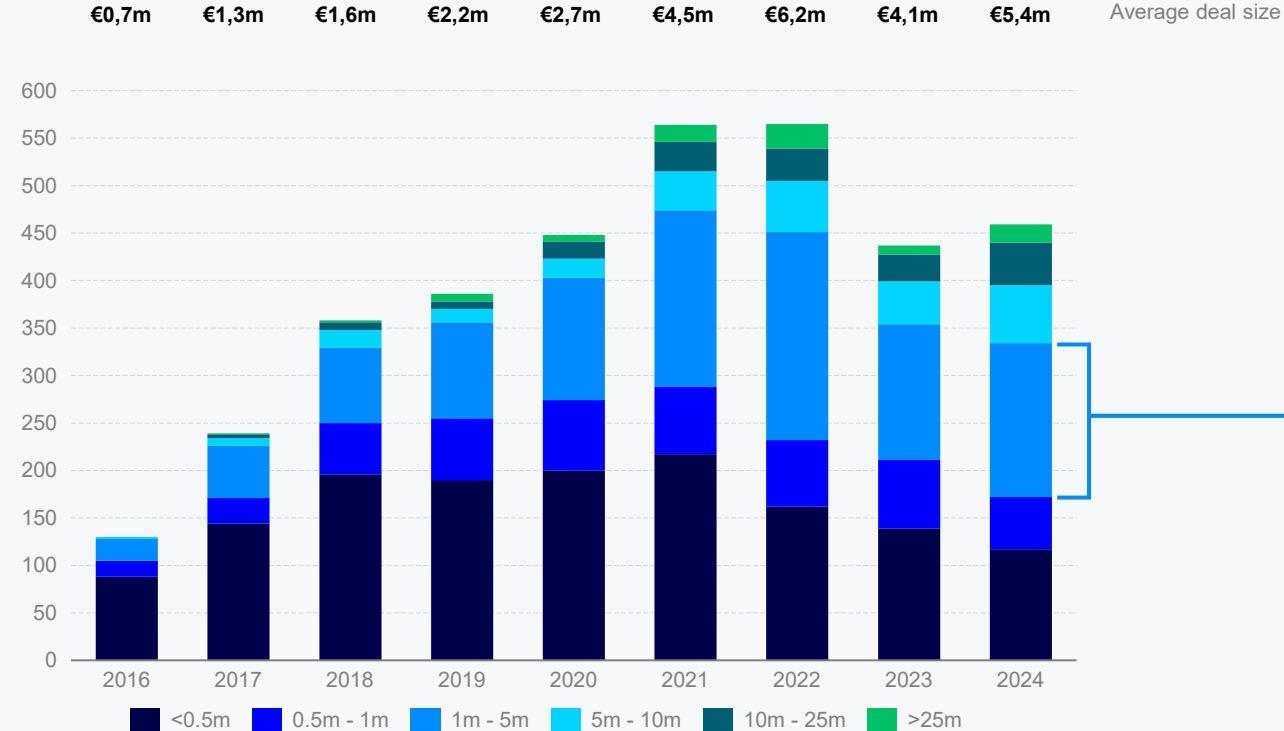
Privacy and digital identity (~11%) remain core pillars of TrustTech, aligning with regulatory shifts and consumer demand for secure authentication. Deals in **GenAI governance** (~8%) point to rising concerns about AI safety and transparency.

Meanwhile, **AI infrastructure and compute marketplaces** (~5%) suggest a growing need for scalable AI resources. At the fringe, **Space Tech and other emerging industries** (10%) signal exploratory investment beyond traditional TrustTech applications.

The **current early-stage TrustTech** ecosystem is dominated by cybersecurity and privacy-enabling solutions

Number of deals¹ per deal category and overall average deal size per year

Source: PitchBook Data, Inc.



¹ Only known deal sizes

Data has not been reviewed by PitchBook analysts.

Looking more closely at the **seed-stage** deals reveals the current state of the early-stage TrustTech ecosystem. An analysis of these companies shows the sectors that have been attracting the most early-stage funding until now.

Over 22% of seed-stage startups are tackling **cybersecurity and threat** intelligence, with a strong focus on AI-powered security, DevSecOps, encrypted network protection, and cyber risk management, highlighting the industry's shift towards proactive, AI-driven defense strategies against evolving cyber threats.

With 17% of the deals, **privacy-first approaches for AI and data** are a growing priority. Focus on technologies like fully-homomorphic encryption, confidential computing, and multi-party computation indicates a need to process data securely without compromising privacy.

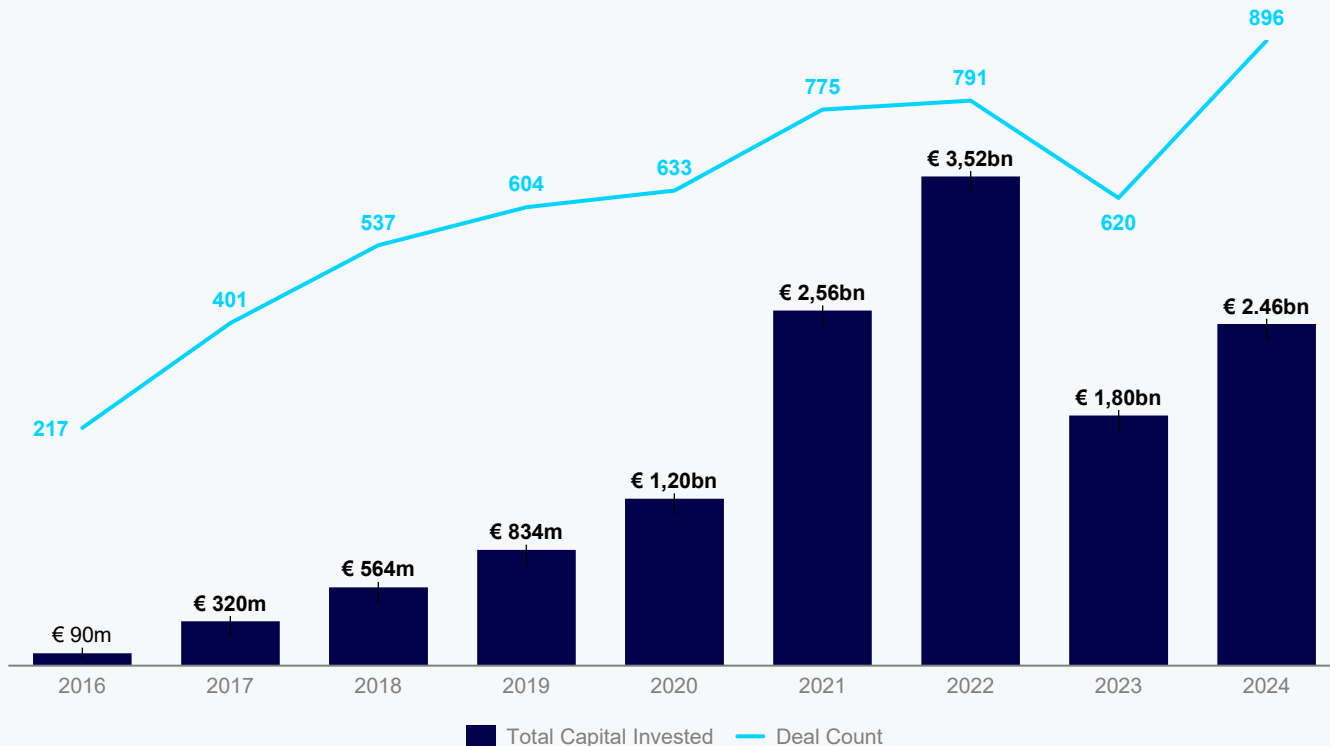
12% of startups in the seed stage focus on **fraud prevention and identity verification**, whereas another 12% offer solutions for broader **regulatory compliance and risk management**.

One in ten seed-stage TrustTech startups focus on **blockchain security, decentralized finance and institutional digital asset management**, indicating the need to address blockchain adoption in enterprise environments.

The TrustTech funding landscape is stabilizing after the 2023 downturn, with investment activity rebooting in 2024

Capital invested and deal count¹ per year

Source: PitchBook Data, Inc.



¹ Also includes deals for which the deal size is unknown.

Data has not been reviewed by PitchBook analysts.

With €13.5bn invested since 2016, the TrustTech startup ecosystem shows stable growth across the last 10 years.

The significant drop in both deal count and capital in 2023 aligns with broader VC market trends, where rising interest rates and risk aversion led to a funding pullback. However, the 2024 rebound shows promise towards a market recovery, and indicated that TrustTech remains a resilient sector benefiting from continued innovation and regulatory drivers.

The 2024 recovery in TrustTech funding is stronger compared to the overall European funding landscape, as Atomico shows funding levels in 2024 almost reaching, but not exceeding those of 2023.

Most notable deals in 2024 include:

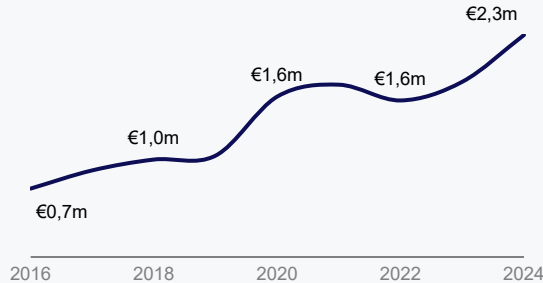
- Vawlt (PT, €215m) – Secure multi-cloud storage
- Tessel (UK, €92m) – AI-native development platform
- Zama (FR, €68m) – Fully-homomorphic encryption
- Prewave (AT, €63m) – Supply chain risk intelligence
- Napier (UK, €52m) – Financial crime compliance

Early-stage pre-money valuations remain stable

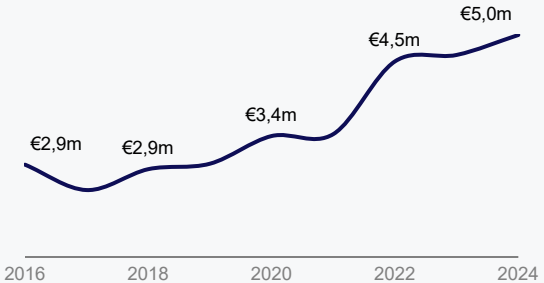
Median pre-money valuations

Source: PitchBook Data, Inc.

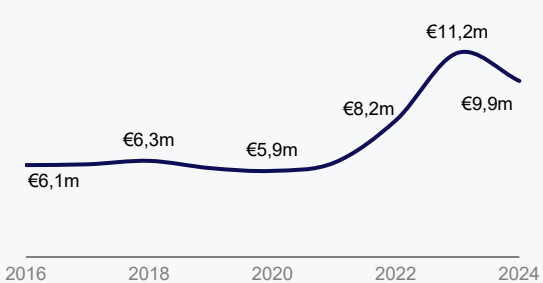
Deal sizes €<0.5m



Deal sizes €0.5m – €1m



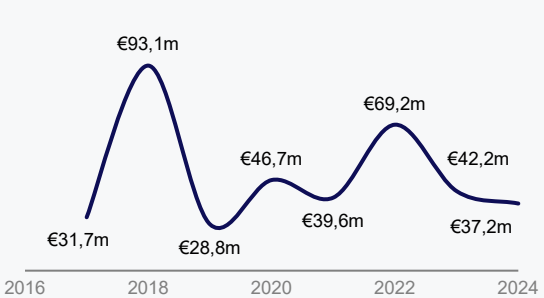
Deal sizes €1m - €5m



Deal sizes €5m - €10m



Deal sizes €10m - €25m



Deal sizes >€25m



Data has not been reviewed by PitchBook analysts.

The rising early-stage pre-money valuations suggest that despite market fluctuations investors remain confident in the growth potential of TrustTech startups.

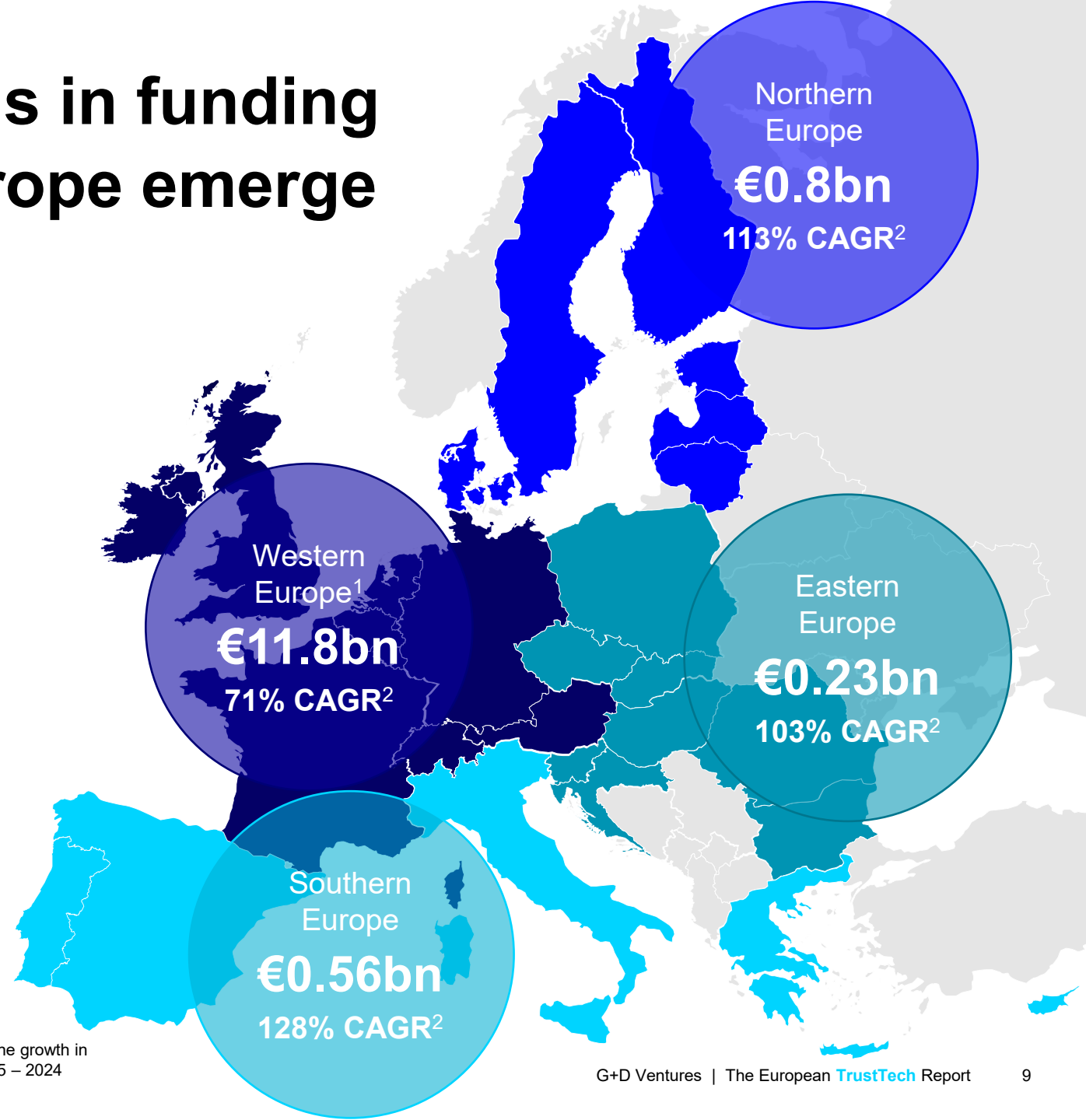
The later-stage deals show more volatility in their pre-money valuations. This indicates that market conditions and investor sentiment play a larger role in pricing at this stage, with valuations fluctuating based on macroeconomic factors, exit opportunities, and shifting risk appetites. It also suggests that later-stage investors are more cautious, prioritizing profitability and sustainable growth over aggressive scaling.

While Western Europe leads in funding Northern and Southern Europe emerge as high-growth hubs

Western Europe remains the dominant hub for TrustTech funding, reflecting its established ecosystem, strong investor networks, and concentration of mature startups. However, the most dynamic growth is occurring in Northern and Southern Europe, signaling a shift in where new opportunities are emerging.

Northern Europe's high growth suggests that existing innovation hubs, such as Sweden and Estonia, are scaling rapidly. According to the Startup Ecosystem Report 2024 by StartupBlink, **Sweden is ranked as EU's top startup ecosystem (6th globally) with Estonia not far behind (12th globally)**. In fact, out of the 8 countries in the Nordics and Baltics combined, **5 make it to the global top 20 list** – no small feat! These ecosystems benefit from a strong digital infrastructure, progressive regulation, and government-backed tech initiatives, making them attractive for TrustTech startups as well.

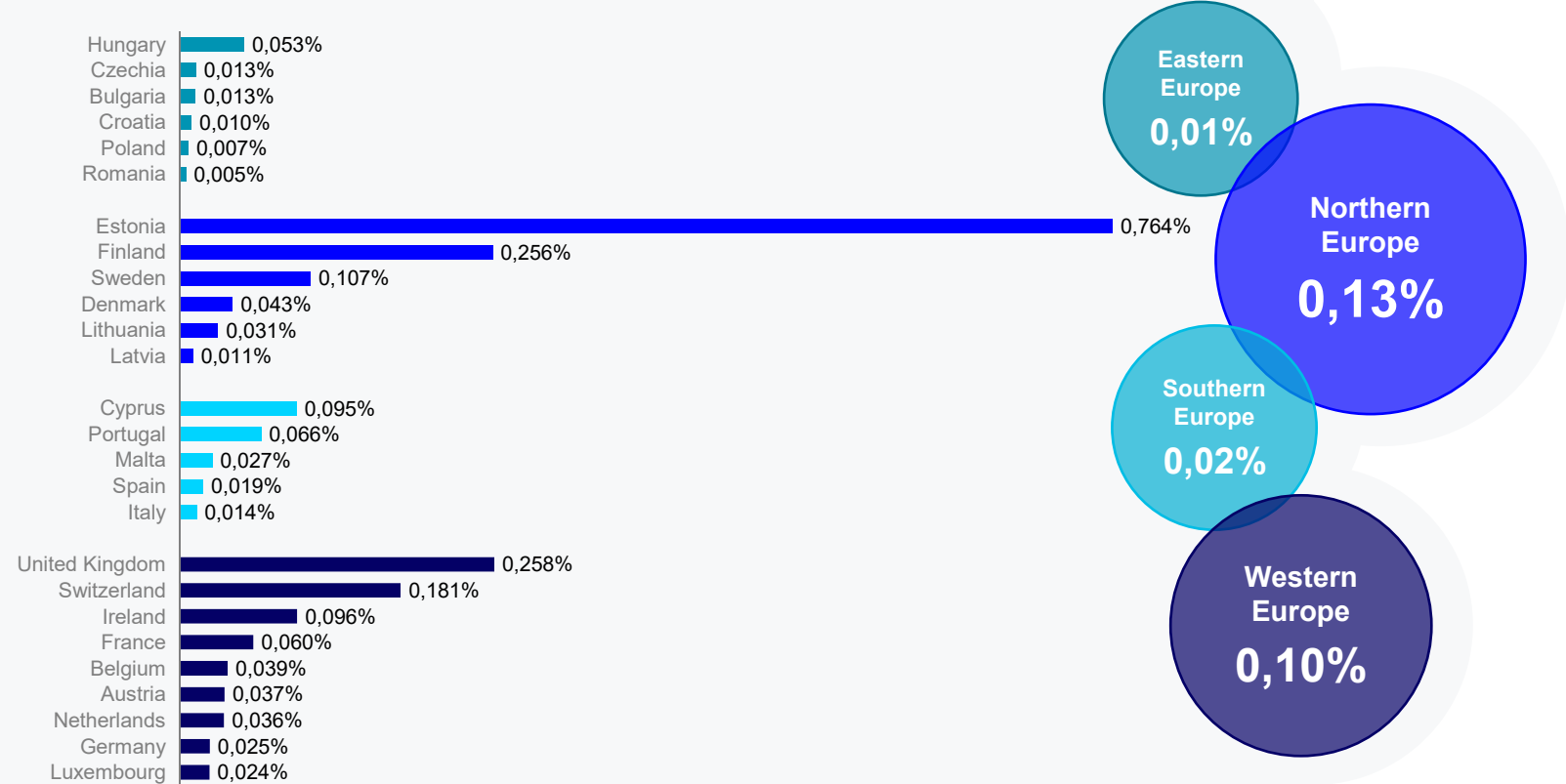
In the sunny Southern Europe, **Spain is becoming the region's strongest TrustTech player, while StartupBlink ranks it 15th worldwide**. The country benefits from strong university research, a vibrant fintech sector, and growing investor interest in regulatory-driven solutions. With the cost of scaling a startup lower than in Western Europe, Southern Europe is an attractive ecosystem for founders and investors alike.



Estonia outperforms in investment intensity relative to GDP, while larger economies lag

Capital invested since 2014, normalized for GDP

Source: PitchBook Data, Inc., The World Bank



Data has not been reviewed by PitchBook analysts. Countries with less than 0,005% are excluded.

Estonia stands out by a wide margin, attracting far more TrustTech investment relative to its GDP than any other European country. This solidifies its standing as one of the top 20 global startup ecosystems and reflects Estonia’s strong digital-first economy.

Ranked 2nd in the global startup ecosystem index, the United Kingdom also takes second place in TrustTech funding relative to GDP.

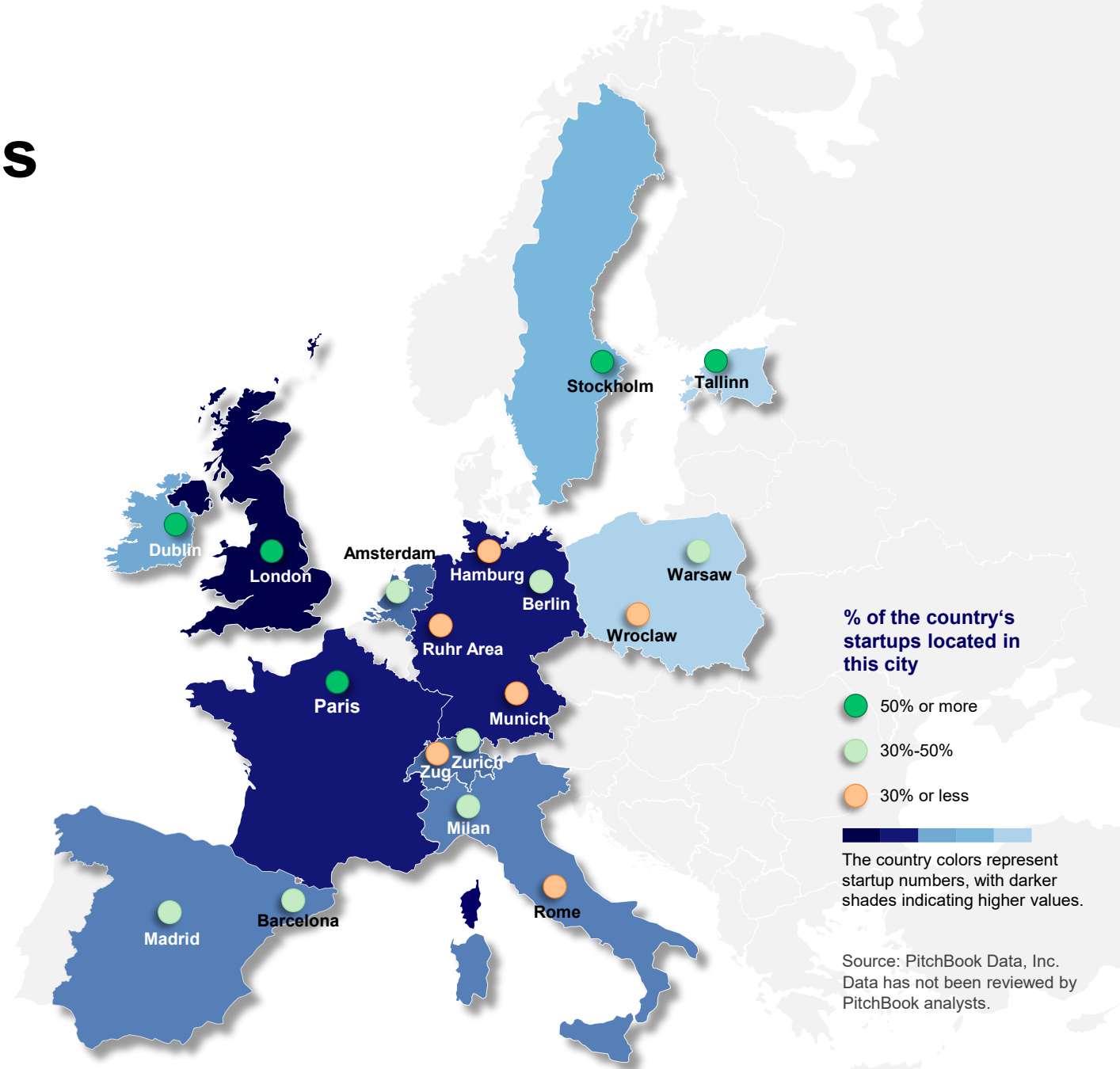
Despite sitting comfortably among the top 10 global startup ecosystems, Germany (7th), France (8th), and The Netherlands (9th) lag in TrustTech investment relative to their GDP. This suggests that while these countries dominate in absolute funding, their ecosystems are more diversified, meaning TrustTech does not take up as large a share of investment activity as in smaller, specialized ecosystems.

Most active TrustTech hubs

London and Paris stand out as major TrustTech hubs, each with a high absolute number of startups (1035 and 277 respectively) and significant regional influence. StartupBlink ranked Paris as EU's top ecosystem and Europe's second-best ecosystem, preceded by London, ranked 3rd overall.

Germany, Switzerland, Spain, Italy and Poland have multiple TrustTech hubs, suggesting that innovation in these countries is more evenly spread. Germany's TrustTech hubs are well distributed across the country, with Berlin taking the lead. Interestingly, nearly 15% of the country's startups are based in the Ruhr area, matching Munich's startup share. The region has cultivated a strong cybersecurity ecosystem, supported by multiple universities with dedicated cybersecurity programs, specialized research centers, and incubators driving innovation.

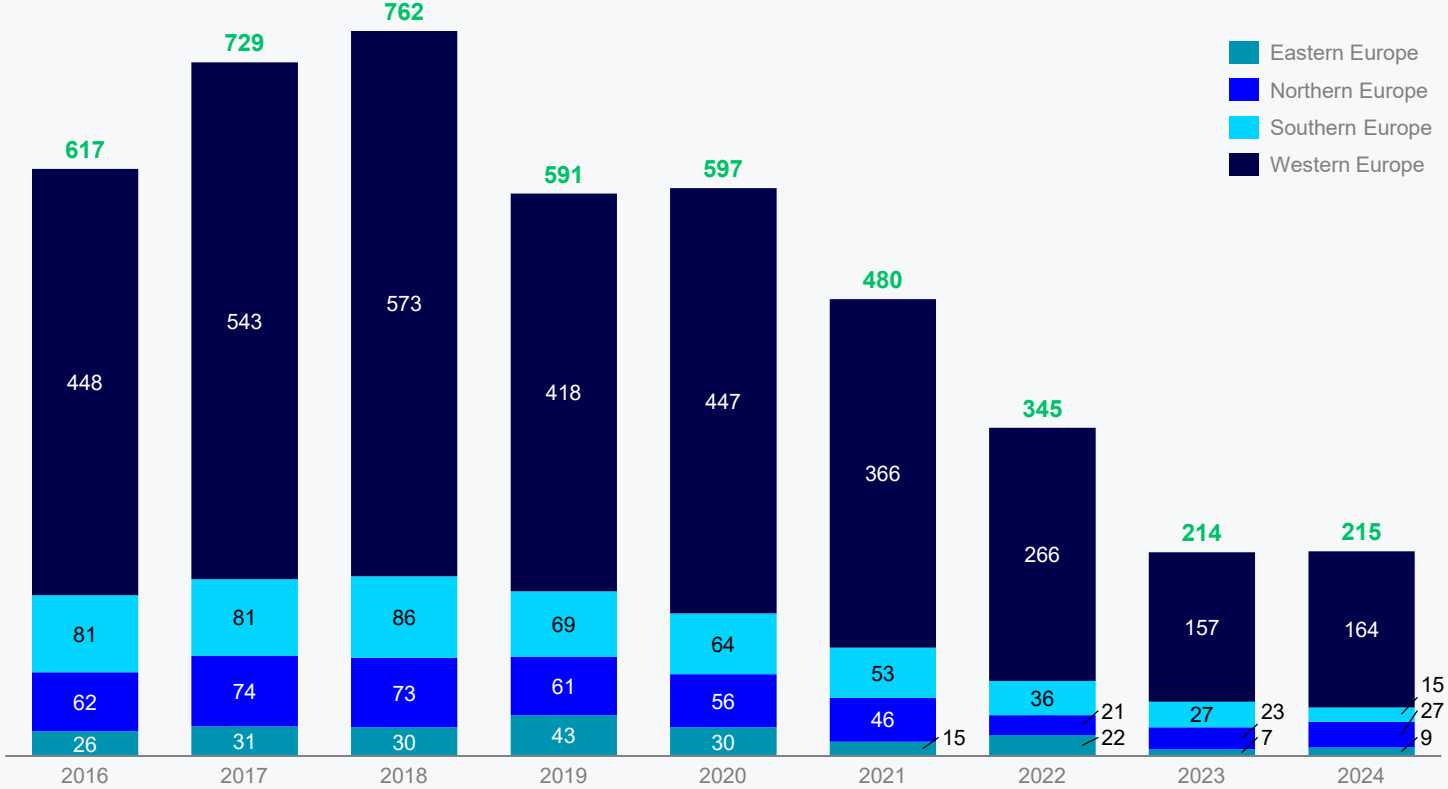
In Spain, Madrid and Barcelona are neck to neck with a combined 70% of the country's startups founded in either city. A similar situation can be found in Italy, where Milan and Rome account for ~60% of the company's startups.



Potential first signs of recovery in YoY growth in TrustTech startups founded

Newly founded¹ startups per year in each European region

Source: PitchBook Data, Inc.



¹ Only known deal sizes.

Data has not been reviewed by PitchBook analysts.

For the first time since 2020, the number of newly founded startups in 2024 did not sharply decrease compared to the previous year.

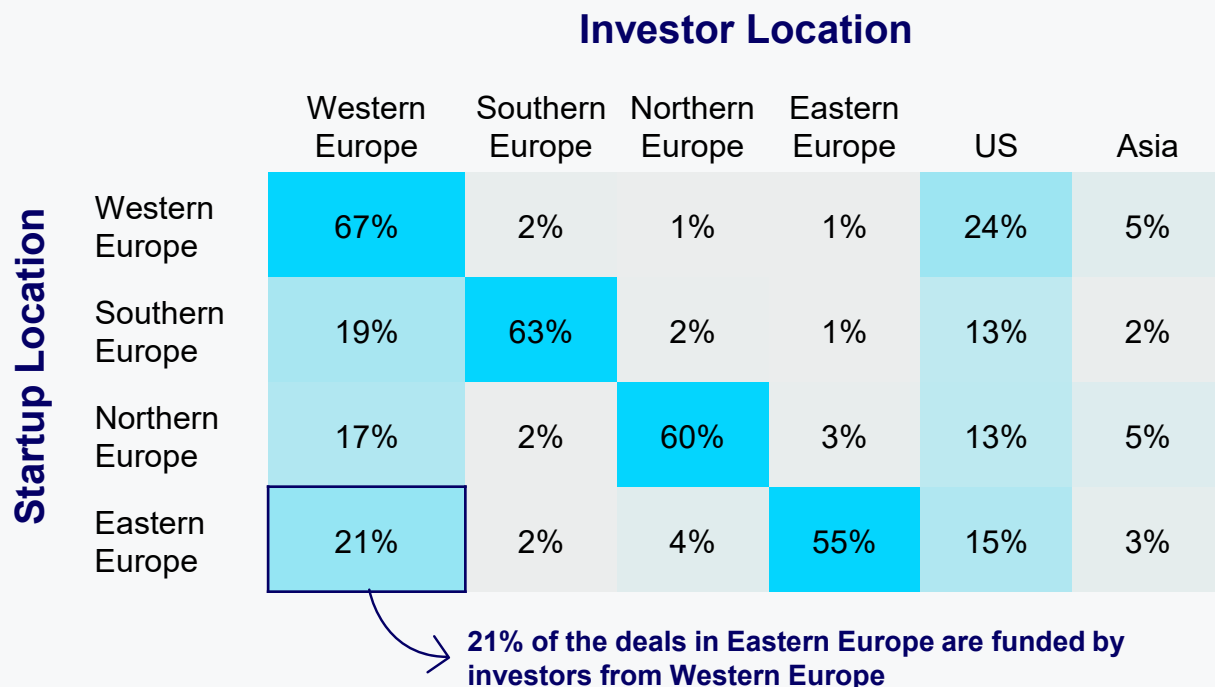
The stabilization suggests that the TrustTech ecosystem is entering a new innovation cycle likely driven by recent technological breakthroughs and stricter regulation.

Emerging capabilities in Agentic AI, privacy-enhancing technologies, decentralized security and others are likely driving this change. Furthermore, AI's soaring compute and energy demands is also fueling this growth, contributing to innovation in high-performance and quantum computing, edge AI, AI compute marketplaces and decentralized compute networks and AI governance.

While some international investment exists, the European TrustTech funding landscape remains highly localized

Origin of TrustTech funding across investor regions

Source: PitchBook Data, Inc.



Data has not been reviewed by PitchBook analysts.

Western European investors are leading capital providers. 67% of Western European deals are funded by domestic investors, showing a strong, self-sustaining investment ecosystem. However, Western European investors also contribute significantly to other regions, particularly Eastern Europe (21%) and Southern Europe (19%), reinforcing their role as the primary external backers of European TrustTech startups.

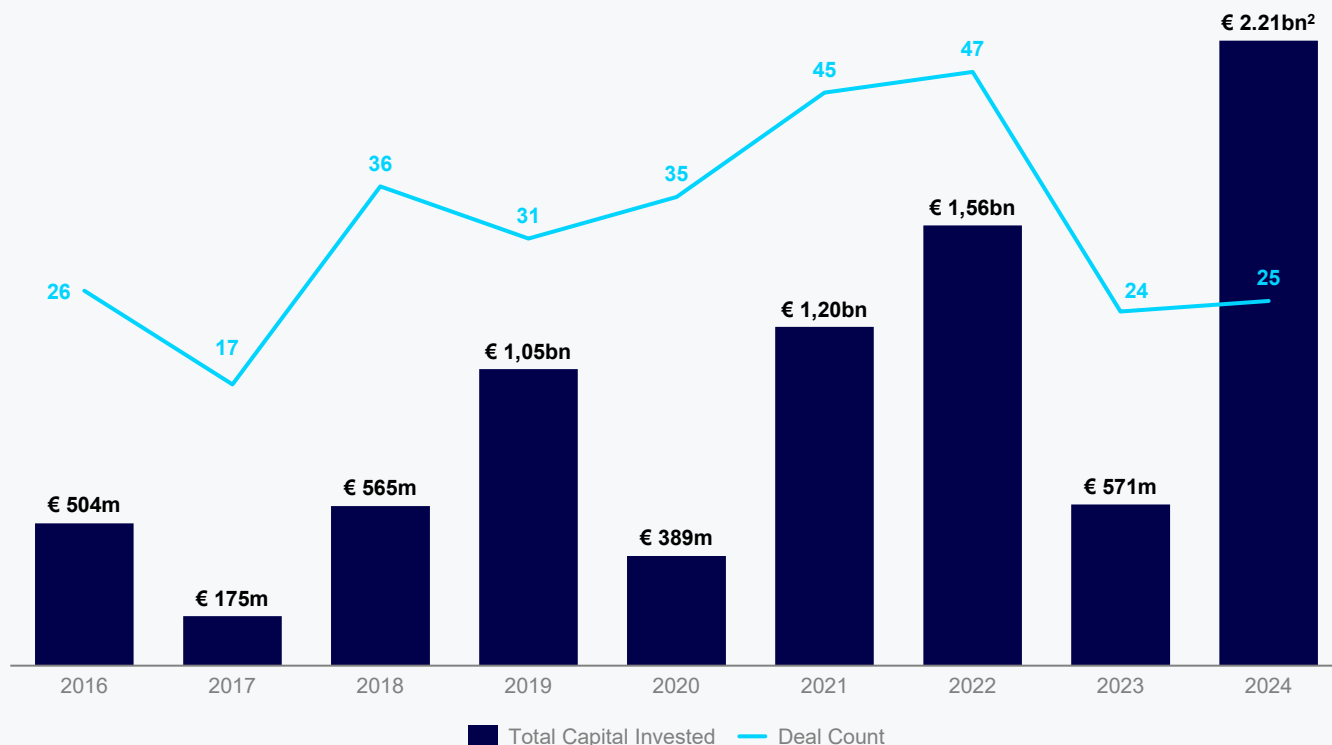
While 55% of Eastern European deals come from domestic investors, a notable 36% are backed by Western European and US investors, indicating a reliance on external capital to sustain growth.

US investors are significantly involved in Western Europe (24%), reinforcing its position as the main European gateway for international capital. Asian investors have a limited footprint overall, with their highest engagement in Western (5%) and Northern Europe (5%).

2024 sees a strong TrustTech M&As rebound after the 2023 contraction

Capital invested and deal count¹ per year

Source: PitchBook Data, Inc.



¹ Only exits with known exit size. Does not include buyouts. Does not include exits of companies which have moved their headquarters outside of Europe.

² Excluding the acquisition of Darktrace by Thoma Bravo.

Data has not been reviewed by PitchBook analysts.

Although TrustTech M&As remain cyclical, 2024 marked a massive rebound in exit amounts, largely driven by the acquisitions of the following companies:

- Featurespace (PT) – Behavioral analytics for financial crime detection. Acquired by Visa for €880m.
- Silo AI (FI) – AI lab for developing advanced AI models. Acquired by AMD for €610m.
- Vision-Box (PT) – Biometric-based systems for airports, airlines, and border control. Acquired by Amadeus IT Group for €300m.
- Next DLP (UK) – Data Loss Prevention & Insider Risk Platform. Acquired by Fortinet for €96m.

Notable mentions (2024):

- Recorded Future (US, Swedish roots) – Threat intelligence analytics software. Acquired by MasterCard for €2.5bn.
- Darktrace (UK) – AI-driven cybersecurity threat detection. Acquired by Thoma Bravo for €4.9bn through an LBO.

G+D Ventures | The European **TrustTech** Report

TrustTech Searchfield

Deepfake Detection



Alberto
Pérez Arranz

Understanding Deepfakes – Types and risks

What are Deepfakes?

Deepfakes are synthetic media created through advanced machine learning techniques. These technologies enable the alteration or creation of fake audio, video, and image content, making them appear convincingly real. While deepfakes have legitimate uses in industries like entertainment and advertising, they pose significant risks when misused.

Types of Deepfakes?

- Video Deepfakes – Face-swapping and digital puppetry create hyper-realistic videos.
- Audio Deepfakes – AI-synthesized voices enable impersonation.
- Text-based Deepfakes – AI-generated content mimicking real authors.
- Image Manipulation – AI-generated photos and identity forgery.

Why are Deepfakes dangerous?

- **Disinformation and Fake News:** Deepfakes can be used to create misleading content that erodes public trust in media and manipulates public opinion.
- **Hate Speech:** Malicious deepfakes can promote violence or hostility against individuals or groups, based on race, ethnicity, or other sensitive attributes.
- **Financial Fraud:** Deepfakes are increasingly used in scams, where malicious actors impersonate key figures to manipulate financial transactions or investments.
- **Privacy and Reputational Damage:** Personal and brand reputations are at risk as deepfakes misappropriate sensitive data for defamation or privacy breaches.
- **Cybersecurity Threats:** Deepfakes enable industrial espionage, sabotage, and disruption of operations, using deceptive practices that compromise digital security.



Example of a deepfake

Source: [News18](#)

CNN World

Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'

By Heather Chen and Kathleen Magramo, CNN

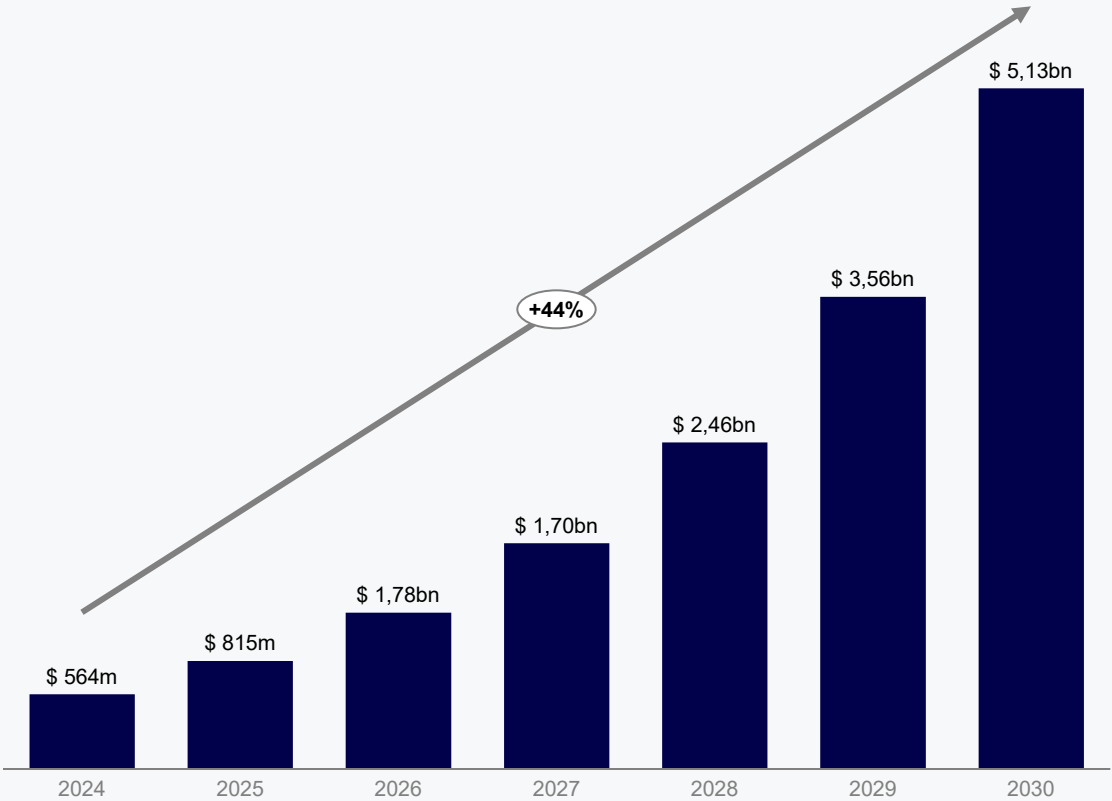
One of the dangers of deepfakes

Source: [CNN World](#)

Deepfake market expansion and regulatory drivers

Total size of overall Deepfake AI market (generation and detection)

Source: Markets and Markets



The Deepfake market

The deepfake generation and detection market is experiencing rapid growth, with the sector projected to expand from \$564 million in 2024 to \$5.1 billion by 2030, driven by developments in GenAI technologies. While deepfakes are used for legitimate applications, their misuse is pushing demand for detection tools. These solutions are essential for mitigating risks across various industries, including finance, media, and cybersecurity.

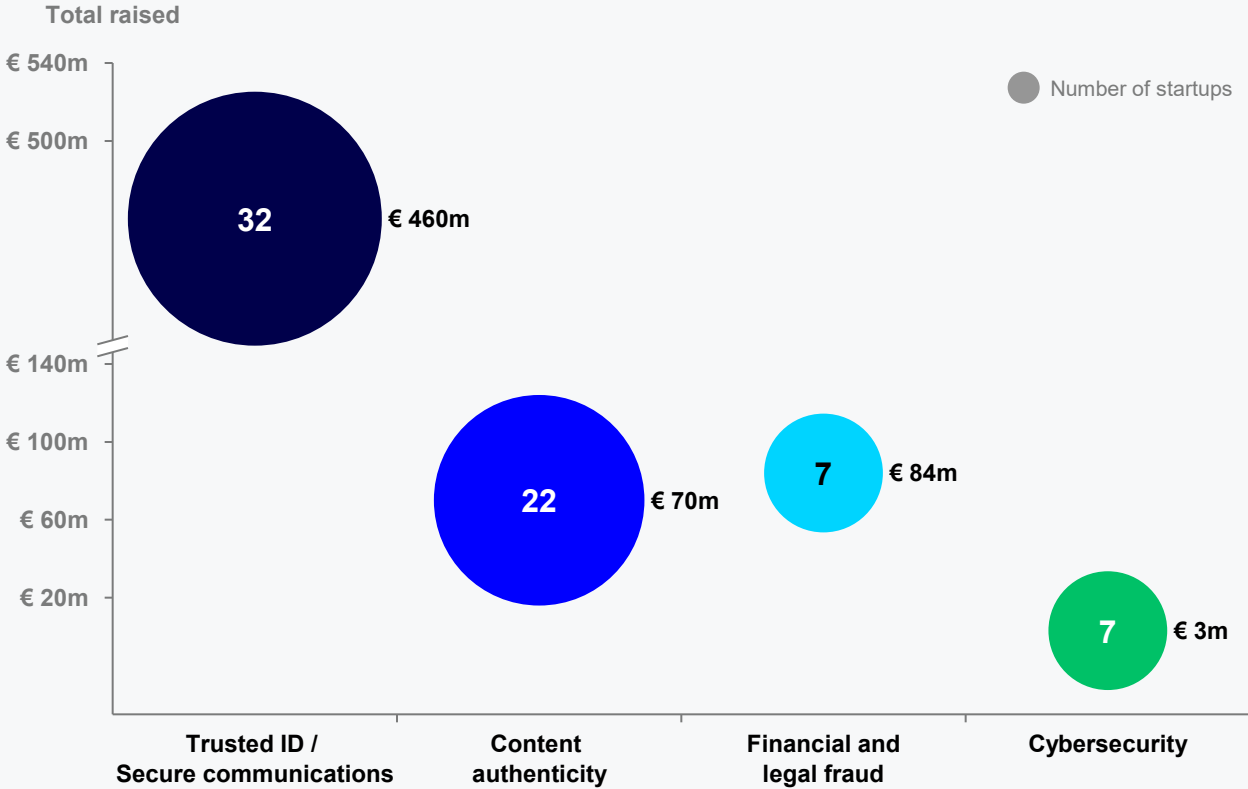
Regulatory landscape and compliance pressures

The regulatory landscape is evolving to address the dangers posed by deepfakes. The European Union's **Digital Services Act (DSA)**, effective in 2024, mandates that illegal deepfakes—those that incite violence, spread misinformation, or engage in other harmful activities—be swiftly removed by digital service providers. Furthermore, the **AI Act** requires deepfakes to be labeled as fabricated material, increasing accountability. These regulations are driving the demand for deepfake detection technologies, as businesses must comply with new standards to avoid penalties.

G+D Ventures segmentation of the deepfake detection market

Deepfake detection use cases

Source: G+D Ventures



Our analysis of more than 50 companies offering deepfake detection solutions uncovered the following emerging clusters:

Trusted ID & Secure Communications – Solutions that verify user authenticity in real-time across various digital interactions, including phone calls, video conferencing, and identity verification (KYC) processes.

Content Authenticity – Solutions that verify the integrity of digital content, helping media organizations, journalists, and law enforcement identify AI-generated or manipulated material.

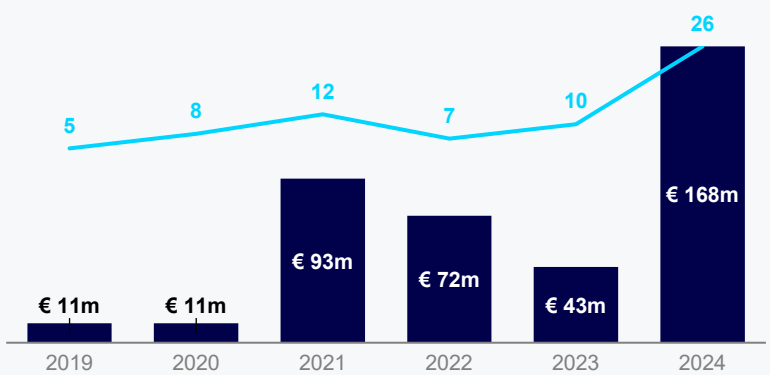
Financial & Legal Fraud Detection – Solutions that mitigate fraud by detecting deepfake-generated documents used for financial gain, such as fake insurance claims, invoices, healthcare records, and certifications.

Cybersecurity – Solutions that search online for illegal deepfake content to mitigate potential threats, as well as products that proactively train and test employees’ cybersecurity skills. While these products complement broader solutions, the market opportunity is relatively narrow when limited specifically to deepfake detection.

Deepfake detection funding and deal count

Source: G+D Ventures

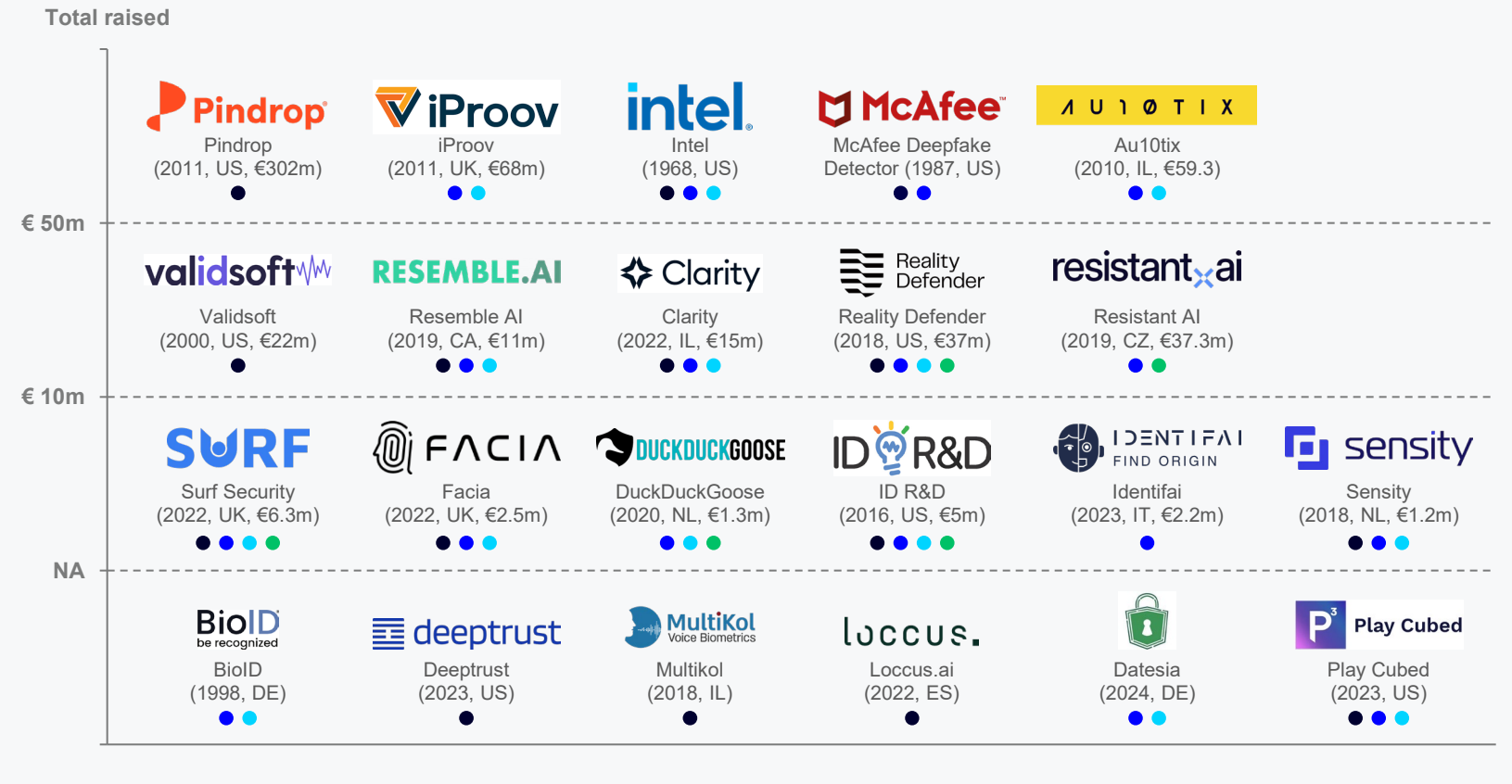
■ Total Capital Invested
— Deal Count



Trusted Identification & Secure Communications: Deepfake detection in authentication and fraud prevention

Deepfake detection: Trusted ID / Secure communications use case

Source: G+D Ventures



This category is driven by **established biometrics and authentication providers**. Pindrop leads the global market for voice security and audio verification, while major KYC providers, including IDnow, Veridas, Au10tix, and Veriff, have already integrated deepfake detection into their identity verification offerings.

Fraudulent calls and impersonation attempts remain a challenge, but mitigation strategies are evolving. Telecommunication providers continue to use traditional verification methods, while **AI-powered scam detection** is emerging at the device level. For instance, Google's Gemini AI model is being tested to detect scam calls on Android devices, and OEMs such as Lenovo, Dell, HP, and Samsung have integrated McAfee's deepfake detection solutions.

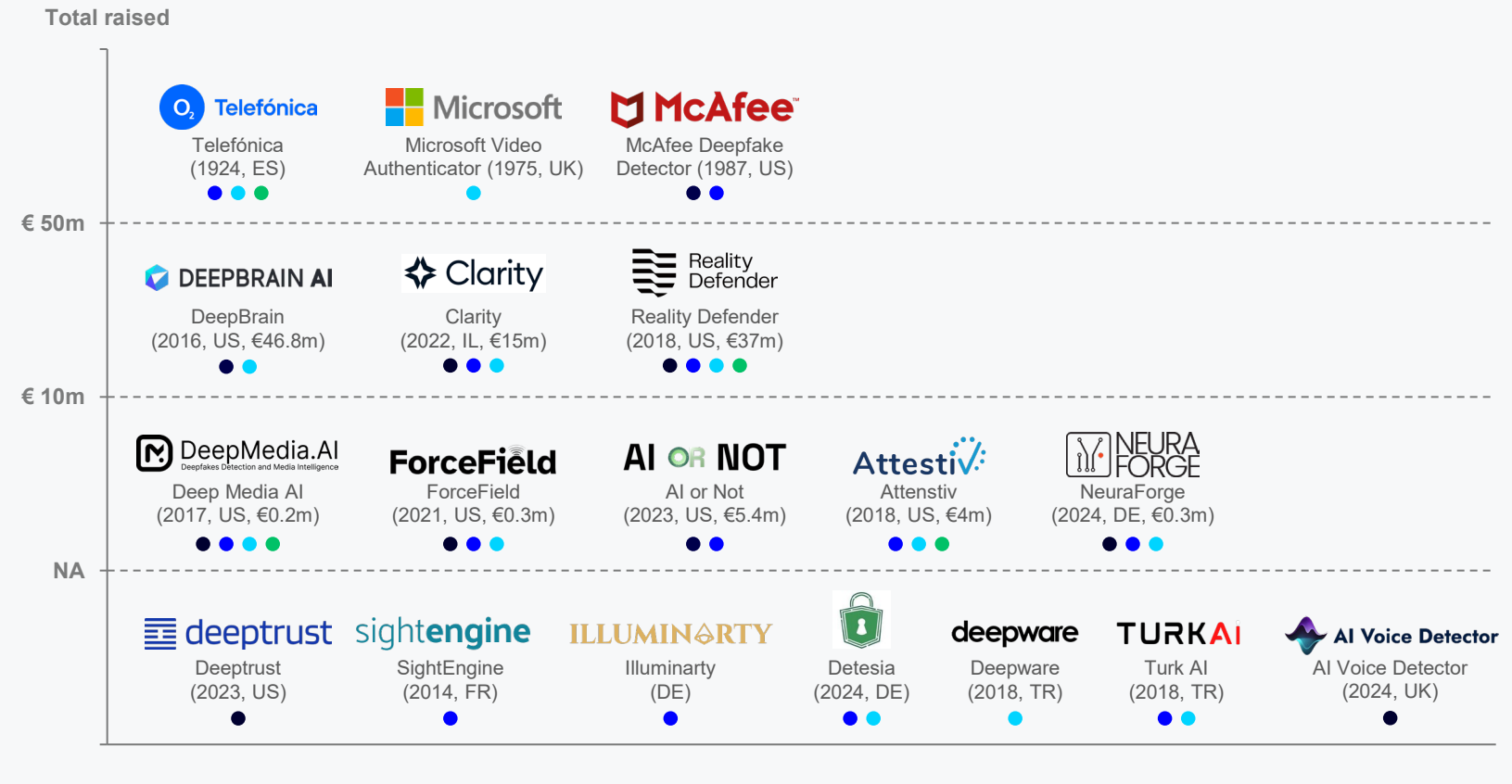
The rise of deepfake-driven fraud is prompting organizations to secure video and audio communications. While dedicated deepfake detection solutions exist, major platforms (e.g., Microsoft Teams, Zoom, Google Meet) are expected to **develop in-house capabilities to safeguard users**.

As the authentication landscape evolves, deepfake detection is increasingly positioned as a **value-added feature within broader identity verification and communication security solutions**, supporting organizations in mitigating AI-driven impersonation threats.

Content Authenticity: Deepfake detection in media

Deepfake detection: Content authenticity use case

Source: G+D Ventures



In this use case, deepfake detection **competes with alternative technologies** such as content certification and watermarking, which provide proactive verification rather than reactive detection.

These proactive methods authenticate **content at the point of creation**. These approaches are gaining traction, particularly in entertainment and media, as they offer clear attribution and persistent validation.

By contrast, deepfake detection operates at the point of content consumption, assessing whether content has been manipulated. While this is valuable for identifying deceptive content, adoption challenges persist due to **accuracy limitations and computational costs**. Media organizations are cautious about relying solely on detection tools, as false positives and negatives could undermine credibility and workflow efficiency.

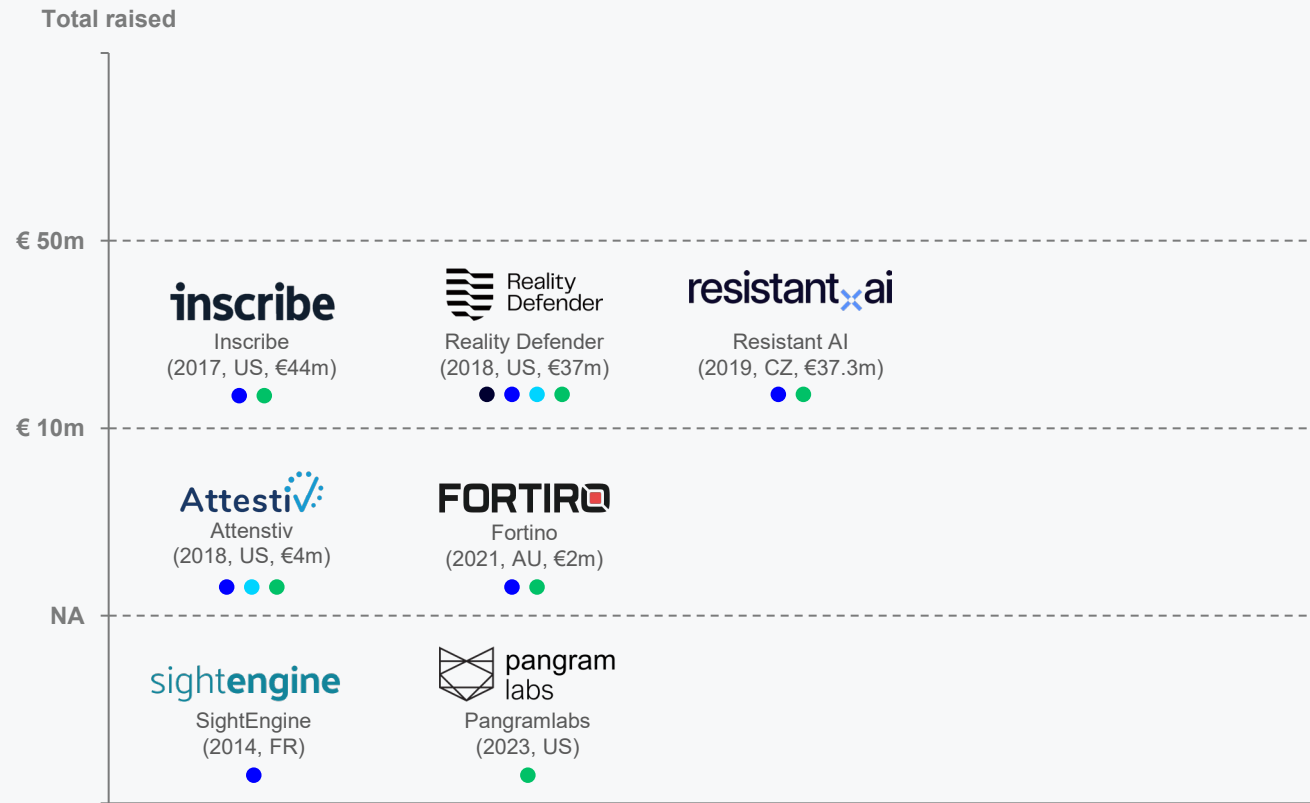
While investment in deepfake detection continues, business traction in this space remains questionable.

Future adoption will likely be driven by regulatory requirements, integration with media verification platforms, and advances in detection accuracy.

Financial & Legal Fraud Mitigation: Addressing the rise of AI-driven document fraud

Deepfake detection: Financial and legal fraud use case

Source: G+D Ventures



The Financial & Legal Fraud Mitigation segment represents a **high-growth opportunity**, as financial institutions, insurers, and legal entities seek to counter the rising threat of AI-generated fraud. The **increasing automation of document processing** has inadvertently created new vulnerabilities, making fraud attempts more scalable and sophisticated.

First-party fraud, where individuals manipulate their real identities by falsifying financial information, continues to challenge lenders and financial institutions. Fraudulent personal loan applications and altered financial details in supporting documents are becoming more prevalent, raising concerns about the reliability of traditional verification methods. At the same time, the **accessibility of AI-generated fraudulent documentation** is expanding, with an increasing number of falsified bank statements, income records, and other financial documents appearing in application processes across multiple industries. Social media and online fraud networks further amplify these risks by providing readily available tools for document manipulation.

To address these challenges, organizations are integrating **AI-driven fraud detection into document verification workflows**. While traditional KYC processes focus on identity verification, the broader opportunity lies in **enhancing the security of processes** such as loan underwriting, insurance claims validation, merchant onboarding, tenant screening, and employee background checks. As fraud techniques become more advanced, financial institutions and legal service providers are prioritizing **multi-layered verification** strategies that incorporate deepfake detection alongside other risk management technologies. The adoption of these solutions will be driven by regulatory pressures, the need for higher accuracy in fraud detection, and the growing financial impact of synthetic identity fraud on businesses worldwide.

Reach out to us for more insights on TrustTech topics!

 gd.ventures



Michael Hochholzer
Managing Director



Assaf Shamia
Investment Partner

 Click to go to LinkedIn profile!



Andreas Barthelmes
Investment Manager



Alberto Pérez Arranz
Investment Manager



Ena Uffelmann
Investment Analyst

Methodology

Our analysis of TrustTech startups in Europe, including their deal specifics (deal size, data, valuation...), investors (type, origin...) and exits (exit amount, type, buyer...) was conducted using data sourced from PitchBook, Inc., and further supplemented by G+D Venture's own research. The selection and analysis of startups, their deals, and investors were based on the following criteria:

- Location: Startups were included if their official headquarters were located in the EU, UK, or Switzerland as defined by PitchBook, Inc. US startups with offices in Europe were not considered.
- Founding Date: The analysis focused on startups founded between January 1, 2014, and December 31, 2024.
- Deal Types: Only venture capital (VC) deals—including accelerator/incubator, seed, early-stage VC, and later-stage VC—and private equity growth/expansion deals were considered.
- Sector: TrustTech was defined according to G+D Ventures, combining PitchBook, Inc. industries and specific keywords found in startup descriptions.
- Investors: No restrictions were placed on the type or origin of investors.
- Exits: Founding date restrictions on startups were lifted. Only exits that occurred between January 1, 2014, and December 31, 2024, were included.

All figures on the graphs are in EUR.

Data has not been reviewed by PitchBook analysts.