



# DSIT AI and Software Cyber Security Market Analysis

# Table of Contents

Executive Summary.....	2
Introduction and Methodology.....	6
Introduction .....	6
Research Objectives .....	6
Market Definitions and Scope.....	7
Research Methodology.....	9
Research Interpretation and Limitations .....	16
Identification of Providers .....	17
Introduction .....	17
Number of Providers .....	18
Products and Services.....	20
Market Analysis .....	24
Introduction .....	24
Size and Scale .....	24
Revenue and Employment .....	27
Investment .....	34
Customers, Partnerships and Demand .....	37
Technical Analysis .....	42

## Executive Summary

In November 2024, DSIT commissioned Perspective Economics to undertake an analysis of the market for software and AI cyber security services. This is aligned with the annual DSIT Cyber Security Sectoral Analysis. This work supports DSIT's ongoing efforts to secure digital technologies, specifically software and AI, through identifying companies that offer crucial and relevant services. This includes the AI Cyber Code of Practice, and the draft Code of Practice for Software Vendors. The study employs an experimental methodology combining extensive data collection, machine learning-enabled web analysis, and detailed classification frameworks. This enables identification and mapping of these market segments, providing baseline data on market scale, capability, products, services and standards.

The research explores three market segments in detail, namely:

- 1. Cyber Security for AI: Providers specialising in securing AI systems and applications.** This typically includes firms focused on the security of AI systems (e.g. LLM security, model protection), and providers of advisory or implementation support for AI system security.
- 2. Specialist Software Security Providers: Firms with clear specialisation in software security provision, including** Application Security (AppSec) testing and tooling, Secure Development lifecycle solutions, software vulnerability assessments, DevSecOps implementation, code and API security, and container and supply chain security solutions.
- 3. Wider Software Security Provision, where firms offer support for software security as part of a broader offering.** This typically includes firms with the ability to provide AppSec capabilities as part of wider security services, code review, vulnerability assessment, and broader software security testing for clients.

## Key Findings

- **We estimate there are 66 firms active in the UK providing cyber security for AI systems, of which:**
  - 14 are specialist providers focused exclusively on AI cyber security
  - 52 are wider cyber security firms providing AI security capabilities
- **We estimate there are 960 firms active in the UK providing software security<sup>1</sup> services, of which:**
  - 93 are specialist software security providers (i.e. they appear to exclusively focus on the provision of software security) and
  - 867 firms offer some form of software security solutions to their clients as part of a wider cyber security offering.

## Size and Scale

- The Cyber Security for AI (66 firms) analysis highlights the majority of specialist providers are typically small or micro (given relatively new entry to market), with a median headcount of 16 staff in the UK. However, this category also includes over 50 larger multinational firms with wider teams that will also be important for enabling adoption of Cyber Security for AI solutions to enterprise clients and for the wider economy.
- For Software Security, among the specialist providers (n=93), there is a relatively balanced size distribution. An estimated 38% of providers have a large or medium presence in the UK, suggesting a maturing specialist market that has developed over time, supporting both niche providers and companies that have successfully scaled their operations.
- In contrast, partial providers (n= 867) show a skew towards micro enterprises, with 52% (450) in this category. This distribution may reflect the large number of IT consultancies, managed service providers, and wider cyber security firms that offer software security as part of their broader portfolio e.g. security services such as application security and penetration testing.
- We estimate that specialist software security providers (n=93) employ an estimated 7,960 FTEs specifically in cyber security roles, with the wider software security ecosystem (n=867) employing approximately 19,940 FTEs working in cyber security

---

<sup>1</sup> Please note that the software security classification includes the 66 firms engaged in AI security.

roles. This suggests that almost one in three<sup>2</sup> (30%) UK cyber security employees work in a company with some form of software security capability.

### Location and Market Presence

- For Cyber Security for AI providers, we find a mix of domestic and international firms operating in the UK, with 48% of firms being UK headquartered, and 38% of providers being headquartered in the United States, with the remainder (14%) across the European Union and rest of world.
- Review of UK locations highlights some concentration in London (59%) and the South East (17%). While some presence exists in regional clusters such as the North West (9%, 6 firms) and East of England (6%, 4 firms), the data suggests more limited distribution of Cyber Security for AI capability across other regions.
- For Software Security, we estimate that 79% (757 firms) are UK-headquartered, and 21% (203 firms) represent international firms with a UK presence.
- Review of UK locations suggests a similar concentration of specialist security firms as with cyber security for AI; however, the wider set of software security providers suggests more regional activity across the UK, with each region highlighting some form of software security provision.

### Investment

The research explores external investment raised by each category over the last five years (2019-2024). It suggests that:

- For cyber security for AI providers:
  - Among specialists (n=14), 50% have raised external investment, with a total of investment of £82m raised, of which £68m has been raised since Q1 2022
  - Notable investments include Lancaster University spin-out Mindgard (raising over £9m), and Harmonic Security (£20m) targeting enterprise AI protection
- For software security providers:
  - We have identified £828m of investment across 42 deals among 15 specialist software security firms from 2019 to 2024.
  - Deal volume has remained relatively stable (6-7 deals annually) through 2019-2021, before moderating in recent years, with greater focus on established firms.

---

<sup>2</sup> 19,940 FTEs in cyber security roles in these companies (divided by the estimated total cyber security sectoral employment of 67,299 FTEs) = 30%.

- Some notable software security investments in 2023 and 2024 include PortSwigger securing £88m growth investment in June 2024 to accelerate their web security testing platform development and expand international market presence; Panaseer has raised over £36m to enhance their Continuous Controls Monitoring platform and expand global market presence; and OnSecurity raised over £5.5m seed funding in 2024 to expand their penetration testing platform and grow their testing team capabilities.

**Technical Capabilities, Products and Services, and Key Sectors Served:**

The research also uses web data to explore technical capabilities, products and services, and customers and sectors supported by cyber security for AI and software security providers.

It explores where providers mention provision of solutions such as LLM and Generative AI (GenAI) security, as well as security integration, cloud security, code and API security, secure development and more.

These are explored in further detail in the relevant sub-chapters; however, provide an insight into the breadth of products and solutions available, and the levels of specialisms and technical capabilities among providers.

# 1. Introduction and Methodology

## Introduction

The Department for Science, Innovation and Technology (DSIT) has recently undertaken two public calls for views to gather feedback on proposed interventions to address software and AI cyber security risks. These include a Code of Practice for Software Vendors and an AI Cyber Security Code of Practice which is being used to develop a global standard in the European Telecommunications Standards Institute (ETSI).

To improve the underlying evidence base, DSIT commissioned Perspective Economics to undertake an analysis of the market for software and AI cyber security services. This is undertaken in line with the ongoing DSIT Cyber Security Sectoral Analysis. This document sets out the initial findings from this research.

## Research Objectives

The purpose of this research is to:

- Define and segment product and service provision within software and AI cyber security, developing a comprehensive tiered taxonomy.
- Identify and analyse market participants operating in software and AI cyber security, with particular focus on UK provision and their relative market positioning.
- Assess current market approaches to software and AI security.
- Map and evaluate emerging innovative tools and methodologies being developed by market participants to address evolving cyber security challenges.
- Develop an analytical framework to support ongoing market assessment, including:
  - Creation of a representative sample frame for quantitative and qualitative research
  - Development of functional datasets capturing market dynamics
  - Production of detailed analysis highlighting key trends and market developments
- Synthesise findings to provide evidence-based insights supporting policy development in software and AI security areas.

This requires an experimental approach, including the development of a working scope and definition, product and service mapping, taxonomy development, and the use of automated and manual review of company product and service provision. This approach is required as

there is no pre-existing approach for defining or measuring companies working in AI security or software security.

As such, this report provides an initial estimate of the number and type of firms active in each market, aligned to the definitions set out in the full project methodology. Please note that this data is subject to interpretation as it requires a review of trading data and subjective interpretation for classification. As such, it should be used as informative only.

## Market Definitions and Scope

This research examines the UK AI and software cyber security markets through three (in-scope) segments, developed via comprehensive analysis of firm-level activities, market positioning and service provision. The box below sets out the scope of these segments.

Definition and Scope:

### **In scope:**

#### **Cyber Security for AI:**

##### **Providers specialising in securing AI systems and applications, including:**

- Firms focused on security of AI systems (e.g. LLM security, model protection)
- Providers of dedicated advisory or implementation support for AI system security
- Highly specialist start-ups developing innovative Cyber Security for AI solutions
- Larger consultancies and firms with dedicated Cyber Security for AI product offerings

#### **Specialist Software Security Providers:**

##### **Firms with clear specialisation in software security provision, including:**

- Application security (AppSec) testing and tooling
- Secure development lifecycle solutions
- Software vulnerability assessment
- DevSecOps implementation
- Code and API security
- Container and Supply Chain security

##### **Firms offering software security within broader portfolio offerings, including:**

- AppSec capabilities as part of wider security services
- Code review services
- Vulnerability assessment provision
- Broader software security testing for clients

### **Outside Scope:**

#### **AI for Cyber Security:**

**Providers that are using AI to enrich, update, or advance existing cyber security tools**, including:

- SOC automation
- AI for threat intelligence
- Other AI-enhanced cybersecurity capabilities

Note: While firms using AI for Cyber Security have been tagged in the review, they are not within scope of this market report. These are considered in the wider DSIT Cyber Security Sectoral Analysis.

While some firms within the wider studies utilise AI to enhance cyber security capabilities (e.g. SOC automation, threat intelligence), 'AI for Cyber Security' services are not considered within scope of this market analysis. The prevalence and impact of AI adoption within general cyber security services is examined separately within the broader DSIT Cyber Security Sectoral Analysis.

In addition, DSIT has previously undertaken research into the UK's [AI Assurance market](#), that suggests there are “84 firms that are UK-based specialised AI assurance companies providing assurance services and products as part of their core offering.” However, this focuses on the use of broad terms such as 'AI assurance, AI governance, responsible AI etc.'

This document is focused upon identifying providers that provide security solutions for AI deployment (e.g. LLM security, securing systems, preventing data exfiltration etc) and software security tools and support.

## Research Methodology

The research methodology uses a data-driven approach leveraging company datasets, and large language models (LLMs) for efficient processing and analysis of extensive web data. This approach has been designed to comprehensively identify and classify firms within both the Cyber Security for AI and software security domains, building on the baseline firms identified within the Cyber Security Sectoral Analysis.

### Stage 1: Data Collection and Desk Review

#### Initial Datasets:

The research team reviewed firms present in both DSIT Cyber Security (c. 2,200 active firms) and AI (c. 3,700 firms) sectoral datasets. This yielded the initial identification of 144 firms with presence in both datasets. All firms were subject to analyst review to identify common language, products, and services that could be included within an initial wider search strategy for additional relevant firms.

The research team also undertook an additional global market review using business data platforms such as Crunchbase. In addition, it undertook the batch identification of companies with relevant terms (e.g. LLM security) using search APIs at a firm and cohort level, using semantic and similarity search. This also helped to identify relevant market maps and existing cohort mapping (e.g. [Geodesic Capital's GenAI Cyber Security Market Map](#)) which were reviewed and considered by the research team.

From this data, we created a long list of 2,537 companies for further consideration.

#### Desk Review:

As this study focuses upon identifying cyber security for AI firms, and software security firms within two distinct datasets, the research team determined to use two different but aligned approaches to best identify relevant firms from this long-listing exercise.

#### *Cyber Security for AI:*

For cyber security for AI, the underlying assumption was that this would be a much more niche area, given the nascence and specialist nature, with a small subset of specialist providers. However, the research team also found evidence of large businesses with AI and cyber security capability (e.g. appeared in both the DSIT AI Sectoral Analysis and DSIT Cyber Security Sectoral Analysis exercises) which could potentially be in scope (e.g. offer penetration testing for LLM applications). Further, many of these providers across both

studies may also use AI to enhance cyber security provision (e.g. AI for threat intelligence) but not appear to be involved in securing AI applications for customers.

As such, the cyber security for AI identification approach sought to:

- Identify new, emerging, specialist providers of cyber security for AI;
- Identify existing providers of cyber security products or solutions that are involved in securing AI applications for customers in the UK; and
- Identify the delineation between firms that provide ‘cyber security for AI’ versus ‘AI for cyber security’ and consider how these may impact policy and market development.

**The research team developed a ‘cyber security for AI’ shortlist of 303 firms for subsequent enrichment and review. This list was shared with DSIT and additional review was undertaken to ensure any known firms were captured and in scope.**

*Software Security:*

As set out in the [DSIT Call for Views on the Code of Practice for Software Vendors](#), “software has become so widespread in day-to-day organisational operations and processes that we barely notice its presence, yet compromised or faulty software can bring organisations to a halt.” This research strand therefore aims to identify any cyber security provider operating in the UK that has the capacity, capability, or ability to support any business developing software with areas set out in the Code, such as secure design and development, build environment security, deployment and maintenance, and ongoing security updates.

For software security provision, the research considers the role of specialist providers (i.e. firms that only or mainly appear to support customers with areas such as application and code security), and wider provision (i.e. firms that offer software security among wider provision, such as managed security service providers that can support with secure development or container security). This is important as it helps to inform estimates of how many organisations and staff can support UK firms with software security requirements.

**Given the breadth of potential provision, all firms (c. 2,200) within the DSIT Cyber Security Sectoral Analysis, and the cyber security for AI (303) sample were determined to be in scope for enhanced review to identify the extent of software security provision.**

## Stage 2: Enrichment and Definitional Review

In order to consider the relevance of each company's product and service offering, the research team proceeded to:

- **Identify active websites and company registration details:** All firms were reviewed to ensure they had a current active domain and, where possible, could be mapped against registered entities within UK Companies House.
- **Review web data:** The research team reviewed web data (where available) to help identify and weight relevancy of firms for the study e.g. website content (respecting 'robots.txt') and wider search results and articles.
- **Review for relevant content:** The research team reviewed a small sample of providers to review the web data in scope to ensure accurate matching and relevancy of content found. Where any errors were flagged (e.g. insufficient content), the team undertook additional checks to ensure best possible coverage. The team also reviewed known 'exemplar' providers to consider web data identified, and its ability to help inform subsequent identification of similar providers (see Figure 2.1 in the Identification of Providers).

## Stage 3: Identification and Classification

Following web data collation, the research team developed two bespoke scripts to review web data and identify relevancy for each sub-sector.

For the 'cyber security for AI' providers, the team analysed web data to determine:

- 'Cyber for AI' activity (i.e. clear evidence of products/services specifically designed to protect AI systems, such as AI model security, LLM security, training data protection, or adversarial AI defence).
- 'AI for Cyber' applications (Uses AI/ML to enhance traditional security products or services but doesn't focus on protecting AI systems themselves. These are typically excluded from scope unless providing 'cyber for AI')
- No clear evidence of security for AI

For 'software security' providers, the team sought to analyse the web data to determine where providers were offering solutions aligned to the [draft implementation guidance](#) for the Code of Practice for Software Vendors. Based on this review, and analysis of existing providers, the team identified seven areas for market consideration. consideration.

	Rationale
Secure Development	Secure Development is a key aspect of the first principle of the Code of Practice. It is a foundational component of software security as implementing secure development practices, such as by following an established secure development framework (e.g. Secure Development Life Cycle, SDLC), can help to limit the number of vulnerabilities written into code at the development stage and to ensure that security is considered from the very beginning of software development. Organisations within this segment provide tools to make it easier for software developers to implement secure development practices. This could include security management, threat modelling, guidelines and standards enforcement, and wider security workflow tools (in addition to some of the areas set out below).
Application Security	Application Security (often referred to as AppSec) includes all processes involved in protecting software applications from threats and vulnerabilities throughout their lifecycle. Initiatives such as the OWASP Top 10 can help to enable more secure code by highlighting the top application security risks e.g. broken access controls, injection, insecure design, misconfiguration etc., and help improve software security. Organisations within this segment may provide services or tools to help detect and prevent runtime security threats, analyse application behaviour for vulnerabilities, manage application access controls, and protect against common attack patterns. This includes web application firewalls (WAF), runtime application self-protection (RASP) solutions, application-level encryption tools, and security testing services focused on identifying vulnerabilities in applications.
Code Security	Code Security focuses on identifying and fixing vulnerabilities within software code itself, whether developed in-house or via third-party components. Organisations in this segment may provide tools and processes such as Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and Software Composition Analysis (SCA) which can be used by those developing and maintaining software to identify potential security issues before they reach production.
DevSecOps	DevSecOps represents the integration of security practices within DevOps processes and culture, ensuring security is built into every

	stage of the software development and operations lifecycle. Tools or services provided by organisations in this segment can help organisations deliver secure code faster by incorporating automated security testing, verification, and monitoring throughout the continuous integration and deployment (CI/CD) pipeline. Examples include security orchestration platforms that automate and coordinate multiple security tools within CI/CD pipelines, compliance monitoring and reporting tools, and security policy automation frameworks that help to enforce security controls across development and deployment processes.
API Security	API Security includes organisations that provide products or services to address the protection of Application Programming Interfaces (APIs), between different software components and services. This includes authentication, authorisation, encryption, and monitoring of API endpoints to prevent unauthorised access, data exposure, and other security risks that could compromise connected systems.
Cloud/Container Security	Cloud/Container Security focuses on protecting applications and data deployed in cloud environments and containerised infrastructure. This includes products and services that can help to secure container images, runtime environments, orchestration platforms (e.g., Kubernetes), and cloud services while ensuring appropriate access controls, network security, and compliance with security standards.
Supply Chain Security	Supply Chain Security addresses the risks associated with third-party components and dependencies within software. Given the 742% increase in software supply chain attacks between 2019 and 2022 (as noted in the Call for Views), this includes products and services that enable software developers to maintain accurate inventories of components (e.g., Software Bill of Materials), monitor for vulnerabilities, and enable secure build and distribution processes.

These definitions were subsequently included within company review, using human and automated (LLM) review processes. In summary, for identifying 'cyber security for AI' providers:

- 303 firms were reviewed, of which 268 firms were found to have relevant readable web data.

- The review process was maximised to ensure that the LLM model considered relevant content, included the ability for user feedback, and provided relevant markers of where firms met the definitional criteria or not. Additional validation based on sources and quality of data was also used. A small sample was also manually reviewed, with sources checked against web data to confirm accuracy and relevancy.
- Overall, 108 providers were considered to clearly offer 'cyber security for AI'. A further 147 mainly appeared to focus on using 'AI for cyber', and 13 were considered of low relevance and not in scope.
- The providers that offered cyber security for AI may also provide other services (e.g. consultancy) but had a clear reference to providing 'cyber security for AI' applications.
- Subsequent checks were undertaken from the web data and Companies House matching to ensure UK activity could be captured. **This resulted in 66 firms active in the UK offering some form of cyber security for AI.**

In summary, for identifying 'software security' providers:

- All firms within the cyber security sectoral analysis (c. 2,200) and wider set (303) were considered in scope for review. A Python script was used to review and extract content for analysis.
- The seven core software security capability areas were assessed. For each capability area, firms were rated as having 'Strong', 'Partial', or 'No' relevance based on evidence of relevant products or services, use of recognised software security tools and methodologies, alignment or mention of relevant standards and methodologies, and evidence of implementation and expertise via client case studies.
- A weighted scoring system was applied across all seven areas to determine overall categorisation. Each provider was segmented into one of the following:
  - **Software Security Specialist:** Strong evidence across multiple capabilities, clearly appears to be a specialist in software security (company focus)
  - **Partial Software Security:** Some dedicated capabilities but not the sole focus of the company (e.g. offers some AppSec or pen testing)
  - **Minimal or General:** The firm has very limited or no clear references to software security provision
- **Additional validation and enrichment was undertaken aligned to the previous steps mentioned (e.g. web and Companies House checks).**
- This resulted in 960 firms active in the UK offering software security services, with 93 identified as specialists and 867 providing partial software security capabilities.

**Stage 4: Data Extraction and Analysis**

The web data analysis generated comprehensive datasets for both cyber security for AI and software security providers. These datasets captured detailed information about each organisation's capabilities, evidence of provision, and technical depth.

To enrich this initial dataset, matching was undertaken with Companies House data to capture registration details, trading status, and latest accounts information. This enabled validation of organisation status and more accurate size classification based on employee counts and financial data in the UK.

Investment data was identified using Beauhurst, enabling analysis of total investment raised, deal volumes and values over time. This helps to inform understanding of market maturity and growth potential, particularly for emerging specialist providers.

**Stage 5: Review and Quality Assurance**

A robust quality assurance process was implemented to ensure confidence in the final datasets. This included validation of the extraction and matching processes, with regular testing sessions held with DSIT analysts to verify outputs. A random sample of records (c. 50 for each dataset) was manually reviewed against source data to confirm accuracy of the extraction and classification.

The classification approach was regularly validated through human review of categorisation decisions. This was particularly important for edge cases where the distinction between categories (e.g., between 'cyber for AI' and 'AI for cyber') required careful consideration.

Data quality was assessed through completeness and consistency checks. A comprehensive QA log was maintained throughout the process to track decisions and document any limitations or constraints identified.

Regular engagement with DSIT analysts provided additional validation of the methodology and approach. These sessions enabled discussion of complex cases and the refinement of classification criteria based on policy requirements. This iterative feedback process helped ensure the final datasets were fit for purpose and aligned with policy objectives.

## Research Interpretation and Limitations

As noted within the Cyber Security Sectoral Analysis and AI Sectoral Analysis, there is no unique agreed definition or classification for mapping technology industries. As such, definitional scoping and the use of web data is required to help identify relevant companies.

We set out research interpretation considerations and limitations below.

- The three distinct categories selected for analysis (Security for AI, Specialist Software Security, Wider Software Security) align with DSIT cyber security policy priorities and particular areas identified for improved security practices in the tech market. These target policy areas are currently being addressed through the development of guidance and standards such as the Code of Practice for Software Vendors and the AI Cyber Security Code of Practice.
- We acknowledge boundaries between segments can be challenging to establish but have used a combination of automated and manual review to help best segment into relevant categories.
- Classification decisions have been made based on known business focus and products and services mentioned by providers whilst recognising some firms may operate across multiple segments. These areas are emergent, and definitions may be liable to change in the future. However, we apply both 'best-fit' and 'multiple' fit to ensure that if a provider appears to provide a particular product or service in a taxonomy category, this is reflected in the analysis and reporting.
- Analysis requires multiple complementary data sources including company accounts, web presence, investment data, and existing sectoral tracking. The research identified firms using existing cyber security and AI sectoral datasets, then expanded this search to find additional emerging providers.

### Key Limitations

- Financial and operational metrics for early-stage firms may be limited or unavailable through standard reporting channels.
- Capability assessment relies significantly on reported information through web data.
- Some firms may understate or overstate their security capabilities for competitive or strategic reasons.
- Some firms may not be in scope of web data review (where web review is explicitly prevented or outside of T&Cs).
- Firms may pivot between segments or expand service offerings over time.

- The distinction between specialist and partial software security provision requires an element of qualitative assessment, with evidence scoring applied based on volume, quality, and relevance of content.
- Some firms may have relevant capabilities that are not publicly documented.
- Firm counts should be interpreted as indicative of market scale rather than exact measurements.

This analysis represents a point-in-time assessment of a dynamic market. Users should consider these limitations when interpreting findings and making strategic or policy decisions based on this research.

## 2. Identification of Providers

### Introduction

The DSIT Cyber Security Sectoral Analysis tracks approximately 2,300 cyber security firms active in the UK. The DSIT AI Cyber Security Sectoral Analysis also tracks c. 3,700 active 'AI' firms. Reviewing this data highlights 144 firms that are contained in both sectoral sets. This includes a wide range of firms, such as those using AI for cyber security and threat intelligence e.g. Darktrace, Tessian; diversified firms developing cyber and AI capabilities and bringing these to market e.g. Deloitte, BT, Accenture; and a smaller number of firms focused on the cyber security of AI e.g. Mindgard, RevEng.ai, and CloudGuard.

This suggests that the existing sectoral datasets contain a mix of providers that either:

- Develop cyber security solutions explicitly for securing AI systems and processes;
- Use AI to enhance existing cyber security products and services;
- Provide wider software security approaches, methodologies and advice to customers;
- Mention AI and software security but have varying levels of technical and market specificity;
- or a combination of all or any of the above.

This research therefore intends to capture an initial baseline for the extent of providers that offer Security for AI and Software Security in the UK. We recognise that many firms within the security for AI sub-sectors may be nascent, recently founded, or within 'stealth mode'<sup>3</sup>. As

---

<sup>3</sup> 'Stealth mode' refers to a company operating within an initial temporary form of secrecy or pre-trading status e.g. an AI security firm developing a new product prior to customer launch.



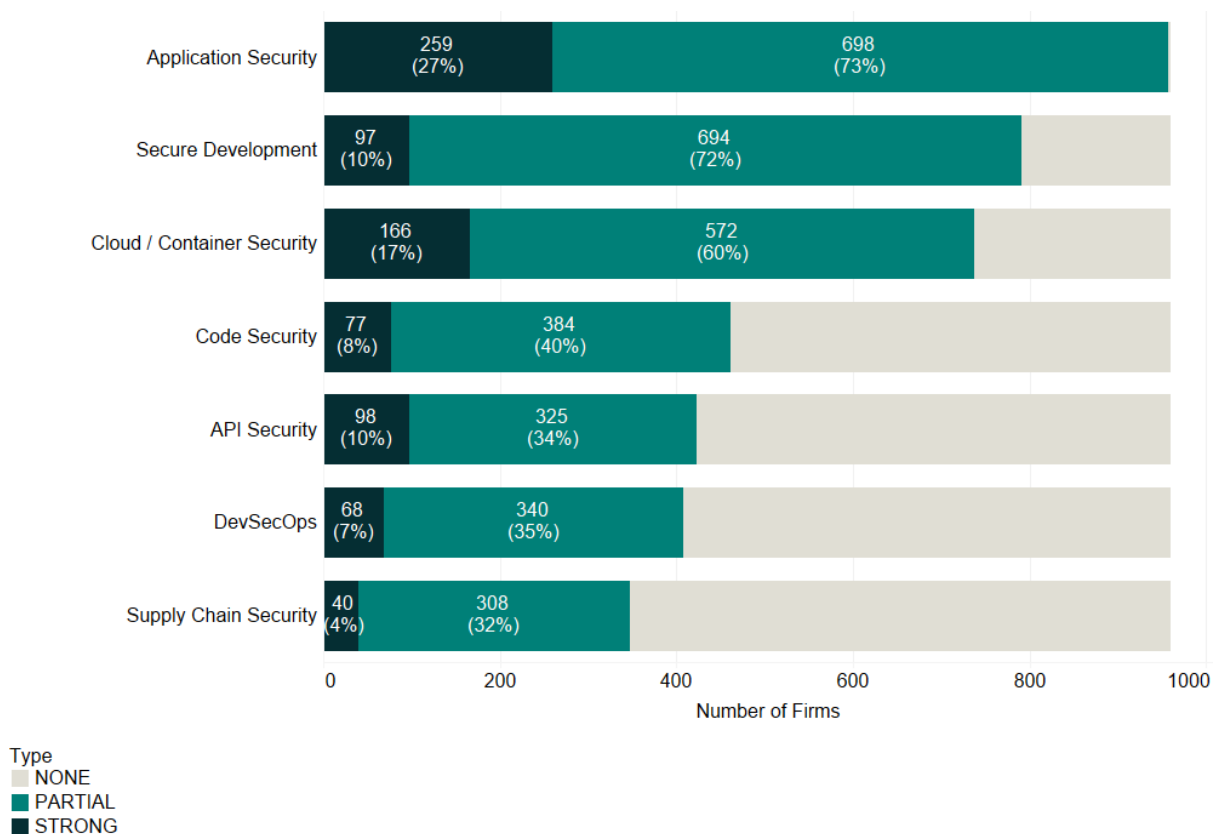
identified 93 providers as ‘specialist’ i.e. they mainly focus on software security, and a further 867 providers that offer some solutions as part of a wider offering (e.g. MSSPs that offer support with application security and vulnerability analysis etc).

Each provider has been reviewed and applied a ‘strong’, ‘partial’ or ‘null’ tag against the following areas of software security (Secure Development, Application Security, Code Security, DevSecOps, API Security, Cloud/Container Security, and Supply Chain Security).

As highlighted in Figure 2.2, **all providers are considered to offer some form of application security**, followed by secure development (82%), cloud / container security (77%), code security (48%), API security (44%), DevSecOps (42%) and supply chain security (36%).

Figure 2.2 highlights the count of providers that have been identified and reviewed using web data to consider the strength and relevancy of their service offering against each category.

Figure 2.2. Extent of Software Security Provision (by provider count):



Source: PE analysis of 960 providers (web data)

## Products and Services

This section explores the products and services mentioned by Cyber Security for AI and Software Security providers in more detail.

### **Cyber Security for AI:**

The products and services mentioned within provider web data suggests there are three distinct market segments for consideration:

#### **1. Specialist Cyber Security for AI Firms:**

This is a small group (c. 14) of firms active in the UK with a sole focus on Cyber Security for AI. The majority are small or micro, with an average of 21 FTE employees. Beauhurst investment data suggests that eight of these firms have raised external investment, with over £80m raised to date (the majority since Q1 2022).

Notable examples include Mindgard (automated red teaming specifically for LLMs and GenAI), Advai (AI testing methodologies), and SECQAI (specialists in use and security of quantum algorithms). We also find some firms with dual UK-US positioning e.g. Harmonic Security, founded in 2023.

#### **2. Larger Cyber Security for AI Integrators:**

We find evidence of (c. 31) dedicated cyber security firms operating in the UK that have offer some form of cyber security for AI product or service to their customers. This includes several dedicated UK headquartered security specialists such as Tessian, Darktrace, and Mimecast. It also includes FDI into the UK from firms such as Checkmarx, Rapid7, Anomali, CrowdStrike and Palo Alto Networks.

#### **3. Advisory, Consultancy, and Managed Services with Cyber Security for AI:**

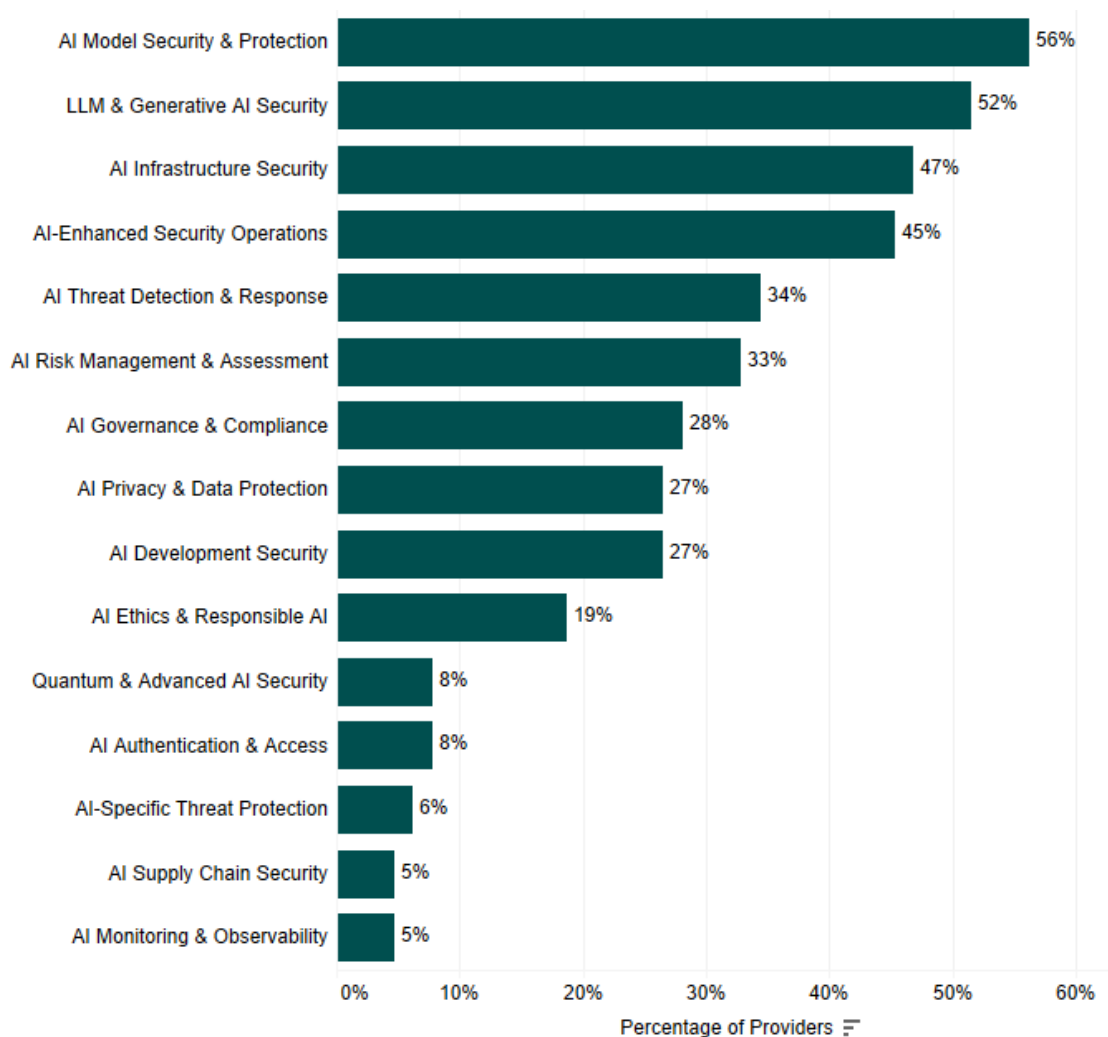
We find evidence of (c. 21) advisory and implementation support with Cyber Security for AI. This can vary from established tech platforms such as IBM, AWS, Microsoft, Oracle, and NVIDIA all offering Cyber Security for AI tools and solutions; to more direct advisory support from consultancy firms (e.g. Deloitte, KPMG, Accenture, Capgemini) and specialists such as Trilateral Research, Fuzzy Labs, Roke, and Kroll.

Figure 2.3 highlights the percentage of cyber security for AI providers (n = 64 with web data) that mention a product or service offering that falls under at least one of the following

categories. The research team found that these providers mentioned 341 unique products or services, which have been assigned to relevant categories e.g. AI model security.

This highlights the breadth of provision in relation to cyber security for AI; several providers will offer multiple distinct solutions depending on the customer requirements and AI use cases. Further, it highlights that, given the nascence of this market and response by vendors to the rising adoption of Large Language Models (LLMs), it is unsurprising that the majority of vendors (56%) directly mention securing AI models, and LLM and GenAI security (52%). Whilst not the focus of this study, AI Governance and Compliance (28%) and AI Ethics (19%) remain closely aligned to this market. Further, quantum AI security (8%) and AI supply chain security (5%) have much smaller market scale in the UK, and remain highly specialised, albeit should be tracked to monitor market adoption in the coming years.

Figure 2.3. Analysis of Product and Service ‘Focus Areas’ for Cyber Security for AI Providers



Source: PE analysis of 64 security for AI specialist providers with web data (341 terms, 15 classification areas)

**Software Security:**

For software security provision, we segment 93 providers as 'specialist' i.e. they mainly focus on software security, and a further 867 providers that offer some wider solutions as part of a wider offering (e.g. MSSPs that offer support with application security and vulnerability analysis etc).

Figure 2.4 explores the products and services mentioned by specialist software security providers across the UK market. In total, the research team identified 440 distinct tools and technologies being offered or integrated by 90 providers. These have been classified into 25 categories to enable analysis of market focus and capability.

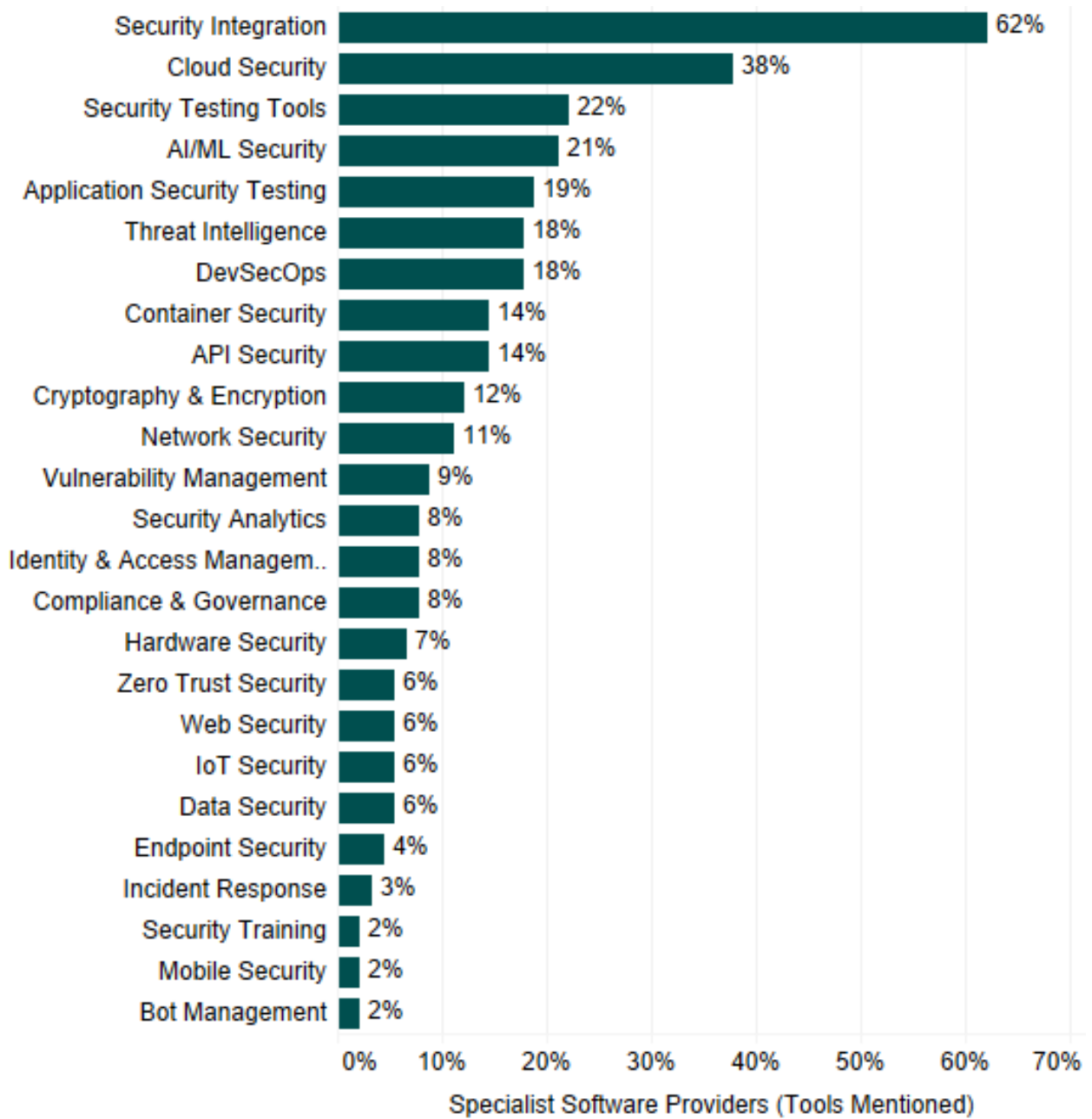
The data highlights that Security Integration (62%) appears to be the dominant focus area offered or mentioned among specialist providers, with many firms producing tools and services that help development teams combine and implement various security tools and platforms effectively. This includes capabilities to support secure integration throughout the software development lifecycle and into wider systems.

Cloud Security (38%) emerges as the second most prevalent category, reflecting the growing importance of securing cloud environments and infrastructure, as software shifts away from on-premises and towards cloud-based SaaS models.

A subsequent tier of capabilities includes Security Testing Tools (22%), AI/ML Security (21%), Application Security Testing (19%), Threat Intelligence (18%) and DevSecOps (18%). This distribution suggests a mature market for core software security functions, with providers actively supporting the security testing and verification requirements outlined in the Code of Practice for Software Vendors.

Some capabilities show fewer explicit mentions in provider materials, though interpretation requires careful consideration, as many of these approaches may be integrated within wider provision or not be explicitly mentioned by providers. This data highlights the complexity of modern software security requirements and the varied ways providers position their capabilities in the market; often showcasing the breadth of provision to meet varying client requirements. For example, vendors may position their offering in line with software development processes (e.g. they offer a Prevent – Detect – Respond approach for software security which covers areas such as training, SAST, SCA, container security, and application risk).

Figure 2.4. Products and Services (Software Security Provision)



Source: PE analysis of 90 specialist providers (with web data) (440 top terms classified into 25 areas)

## 3. Market Analysis

### Introduction

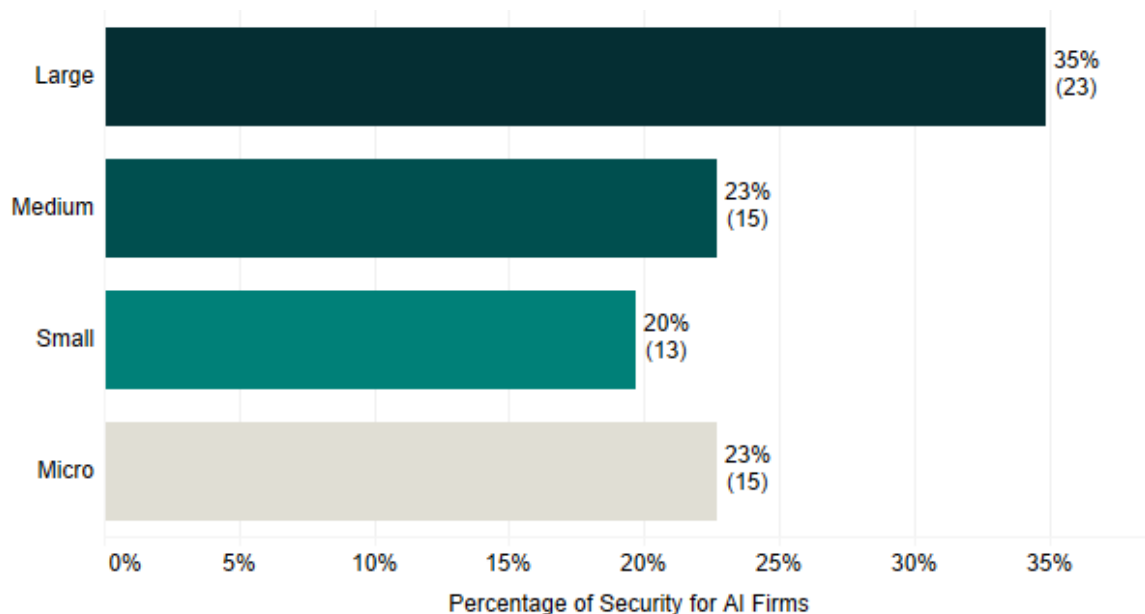
This section explores the firm-level characteristics of providers identified in the Cyber Security for AI and Software Security sets. It considers size and scale, estimated revenue and employment, location, external investment, and wider partnerships and demand.

### Size and Scale

#### Cyber Security for AI:

For the Cyber Security for AI firms registered in the UK, review of company accounts and wider trading data suggests that there is a relatively even distribution between large, medium, small and micro<sup>4</sup> firms. This reflects the previous discussion of how these firms can consist of both specialist start-ups, as well as large IT firms offering Cyber Security for AI as a new product or service offering to existing commercial customers.

Figure 3.1. Cyber Security for AI: Estimated Size



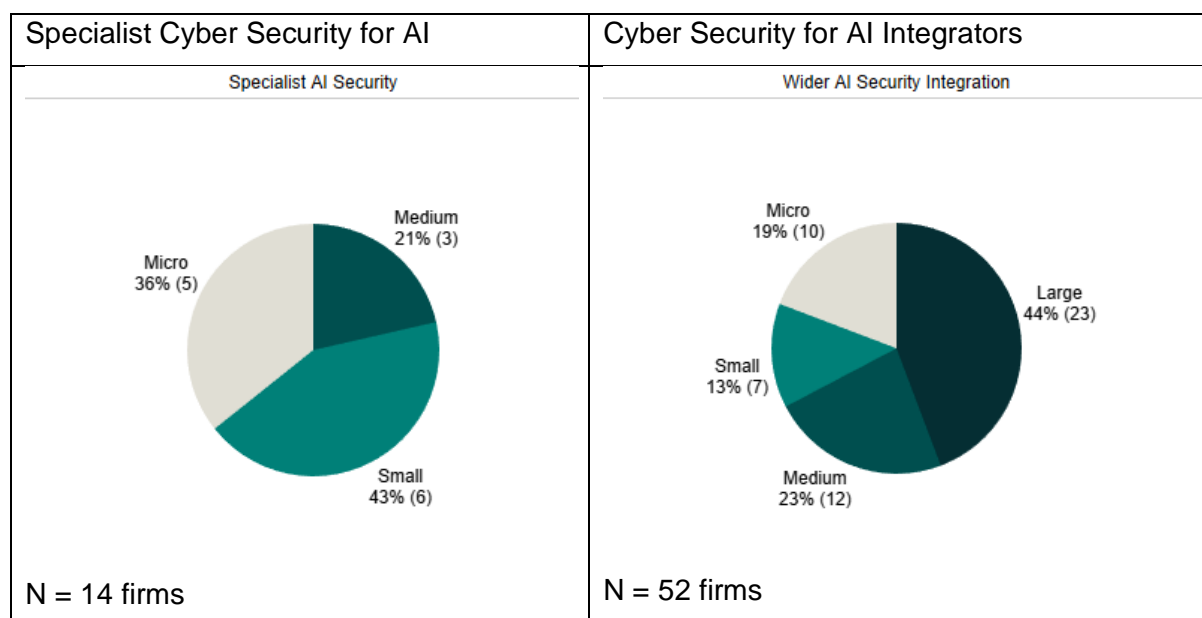
Source: Perspective Economics analysis, n = 66 registered Cyber Security for AI firms

<sup>4</sup> Full size definitions: Large: Employees  $\geq 250$  and Turnover  $> \text{€}50$  million or Balance sheet total  $> \text{€}43$  million // Medium: Employees  $> 50$  and  $< 250$  And Turnover  $\leq \text{€}50$  million or Balance sheet total  $\leq \text{€}43$  million // Small: Employees  $> 10$  and  $< 50$  And Turnover  $\leq \text{€}10$  million or Balance sheet total  $\leq \text{€}43$  million // Micro: Employees  $< 10$  And Turnover  $\leq \text{€}2$  million or Balance sheet total  $\leq \text{€}2$  million

However, segmenting Cyber Security for AI providers between ‘Specialist Cyber Security for AI Firms’ (n = 14) and larger multinational integrators (n = 52) highlights the nascence of the initial category. While this is a small sample size, it highlights that the majority of specialist providers are micro or small, with a median headcount of 16 staff in the UK. The wider size estimates also highlight the importance of larger firms adopting and rolling out Cyber Security for AI solutions to enterprise clients, as these will enable the development of relevant skills, security, and implementation of Cyber Security for AI across the wider UK economy.

These size estimates indicate two immediate considerations for policy-makers. Firstly, to grow and scale an emerging specialist Cyber Security for AI market, growing from a small base, requiring investment and support to scale. Secondly, to enable the adoption and rollout of Cyber Security for AI approaches among wider providers to their end clients in the UK.

Figure 3.2. Cyber Security for AI: Size by Specialist and Integrators



Source: Perspective Economics analysis, n = 66 registered Cyber Security for AI firms

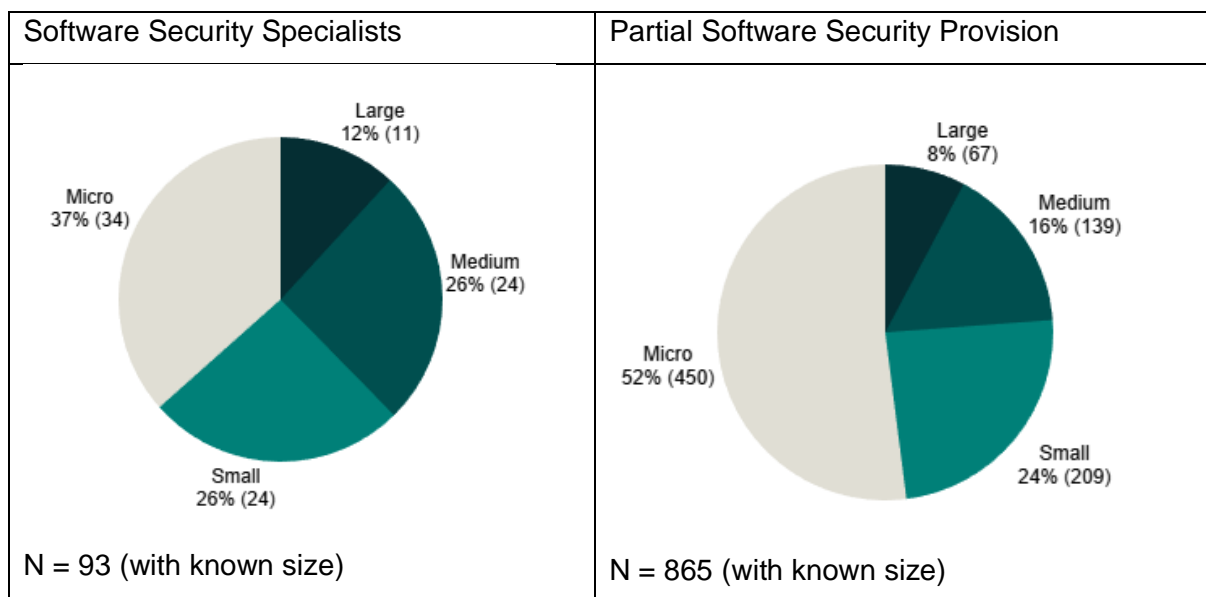
### Software Security

The Software Security landscape demonstrates a notably different size composition compared to Cyber Security for AI firms. For specialist providers of software security, there is a relatively balanced size distribution. An estimated 38% of providers have a large or medium presence in the UK, suggesting a maturing specialist market that has developed over time, supporting both niche providers and companies that have successfully scaled their operations.

In contrast, partial providers show a skew towards micro enterprises, with 52% (450) in this category. This distribution may reflect the large number of IT consultancies, managed service providers, and wider cyber security firms that offer software security as part of their broader portfolio e.g. security services such as application security and penetration testing.

Overall, this data is encouraging from a market perspective, as it highlights a range of providers across the UK, with varying levels of capacity to support organisations with software security solutions.

Figure 3.3. Software Security: Estimated Size



Source: Perspective Economics analysis, n = 958 registered Software Security firms with identifiable size

## Revenue and Employment

The DSIT [Cyber Security Sectoral Analysis \(2025\)](#) estimates the annual revenue and employment of the UK's cyber security sector each year. The most recent published report estimates the annual revenue of the sector at £13.2bn with c. 67,300 Full Time Equivalent employees. This reflects a 'best estimate' by the research team, based upon agreed estimation techniques drawing on accounts data, survey findings, and web data.

Estimating revenue and employment specifically for Cyber Security for AI and Software Security sub-sectors presents additional methodological challenges. These segments represent emerging categories within the broader cyber security sector, comprising both large providers (requiring careful segmentation of relevant workforce) and smaller firms that fall below statutory reporting thresholds.

Drawing on available data and cross-referencing with ongoing DSIT Cyber Security Sectoral Analysis (2025) internal estimates, we can provide indicative employment figures:

For Cyber Security for AI:

- Specialist Cyber Security for AI providers (n=14) account for an estimated £68.6m in revenue and 277 FTEs
- The broader Cyber Security for AI provider base (n=66) employs over 163,000 people in total, with approximately 9,740 working in cyber security roles. The specific proportion focused on Cyber Security for AI activities cannot be determined from available data

For Software Security:

- Specialist providers (n=93) employ an estimated 14,581 FTEs, with 7,960 specifically in cyber security roles
- The wider software security ecosystem (n=867) employs over 532,000 people in the UK, with approximately 19,940 FTEs working in cyber security roles. This suggests that almost one in three<sup>5</sup> (30%) UK cyber security employees work in a company with some form of software security capability.

---

<sup>5</sup> 19,940 FTEs in cyber security roles in these companies (divided by the estimated total cyber security sectoral employment of 67,299 FTEs) = 30%.

These estimates should be treated as indicative rather than definitive, given the complex nature of segmenting revenue and employment in overlapping domains. This is particularly challenging when attempting to isolate Cyber Security for AI activities within larger organisations' cyber security operations. Additional modelling and data collection would be required for more precise estimates, particularly regarding revenue attribution across service lines.

## Location

This section explores the registered location (i.e., where each business has located its registered address with Companies House), and the active international locations (i.e., where each business has a trading presence or office outside of the UK) of relevant firms.

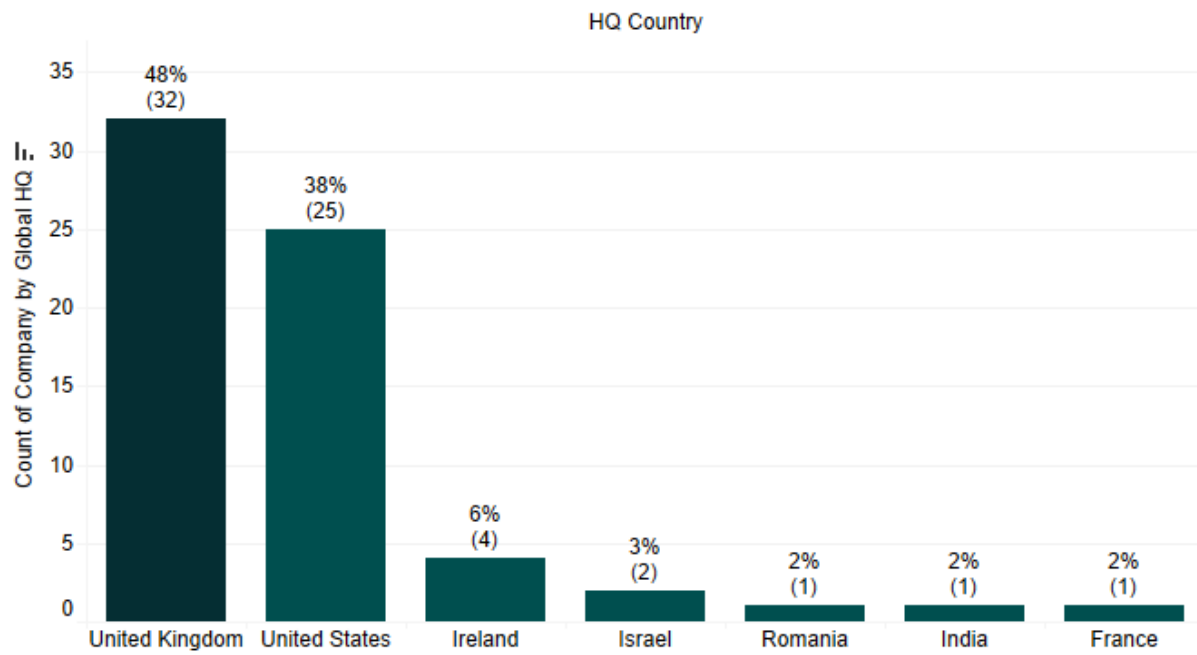
Understanding the addresses of security firms in the UK enables regional analysis and supports the evidence-based identification of notable clusters or hotspots of activity. Identification of international offices also enables an assessment of where firms are founded in the UK, or reflect Foreign Direct Investment into the UK, or where UK firms are exporting and interacting with international markets.

This section provides a high-level overview of location by headquartered country, and UK registered locations.

### **Cyber Security for AI**

Of the 66 Cyber Security for AI firms identified, there is a relatively balanced split between UK-headquartered companies (48%, 32 firms) and those with headquarters in other countries but registered UK presence (38%, 25 firms from the United States). The remaining firms are predominantly headquartered in Ireland (4 firms), Israel (2 firms), and single representations from Romania, India, and France. This suggests a mix of domestic capability alongside active foreign direct investment, particularly from the United States.

Figure 3.4. Cyber Security for AI: Company Location by Headquartered Country



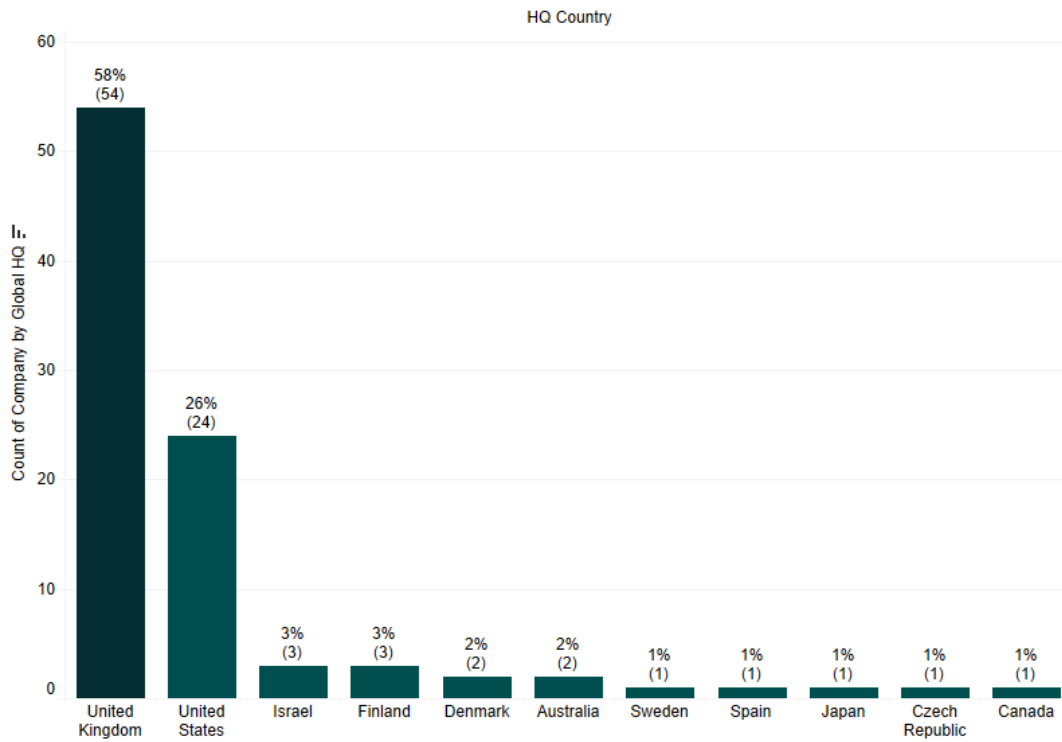
UK Marker Final  
 ■ UK Headquartered  
 ■ UK Registered (FDI)

Source: Perspective Economics analysis, n = 66 registered Cyber Security for AI firms

### Software Security (Specialist)

The software security landscape shows a stronger domestic presence, with 58% (54 firms) of specialist providers headquartered in the UK. The United States remains a significant source of foreign investment with 26% (24 firms) of providers headquartered there. This is followed by European Union / European Economic Area countries with 8 firms (9%).

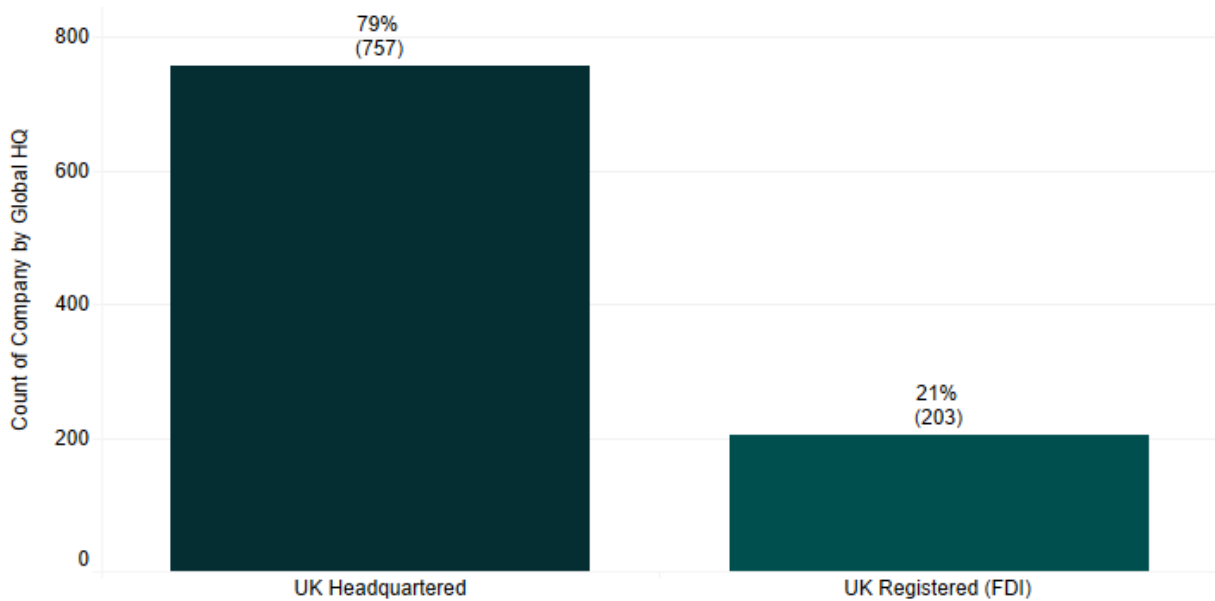
Figure 3.5. Software Security (Specialists): Company Location by Headquartered Country



Source: Perspective Economics analysis, n = 93 providers

Across the broader software security landscape, we estimate that most of these are UK-headquartered firms, with 79% (757 firms) having their primary base in the UK. This suggests some capacity among smaller UK focused entities to support the wider economy with software security requirements.

Figure 3.6. Software Security (All): Company Location by Headquartered Type

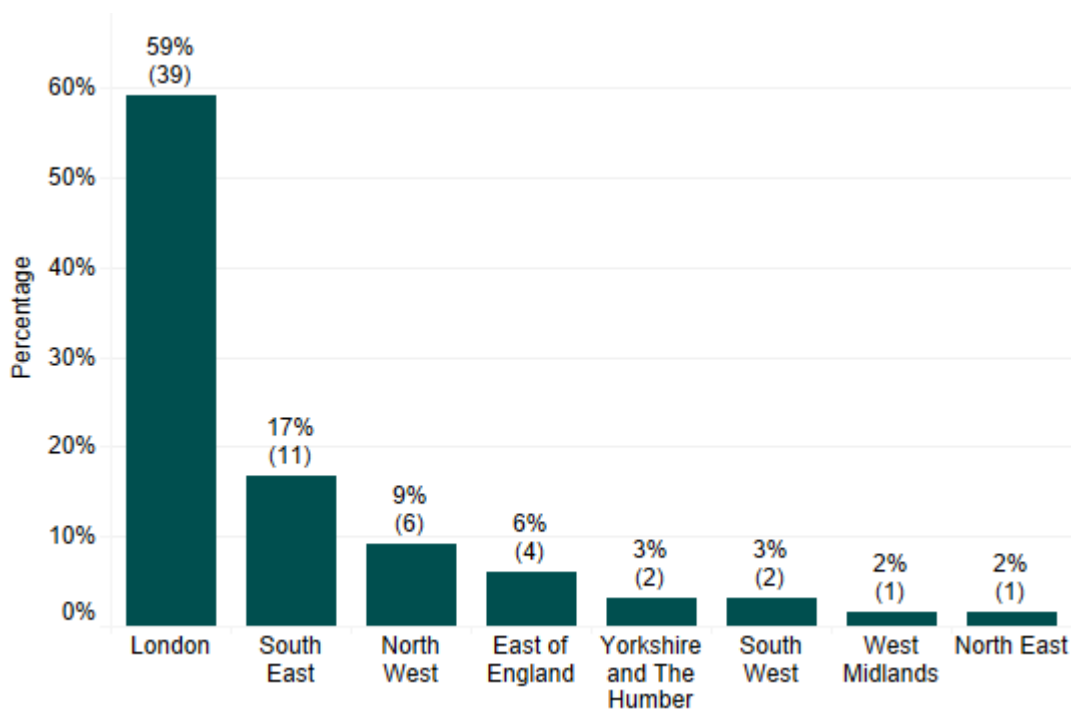


Source: *Perspective Economics analysis, n = 960 providers*

**UK Locations:****Cyber Security for AI:**

Analysis of Cyber Security for AI firm registration data indicates significant geographic concentration, with London (59%, 39 firms) and the South East (17%, 11 firms) accounting for the majority of registrations. While some presence exists in regional clusters such as the North West (9%, 6 firms) and East of England (6%, 4 firms), the data suggests more limited distribution of Cyber Security for AI capability across other regions. However, we note caution with the low sample size (66 firms) and registered focus.

Figure 3.7. UK Registered Location (Cyber Security for AI)



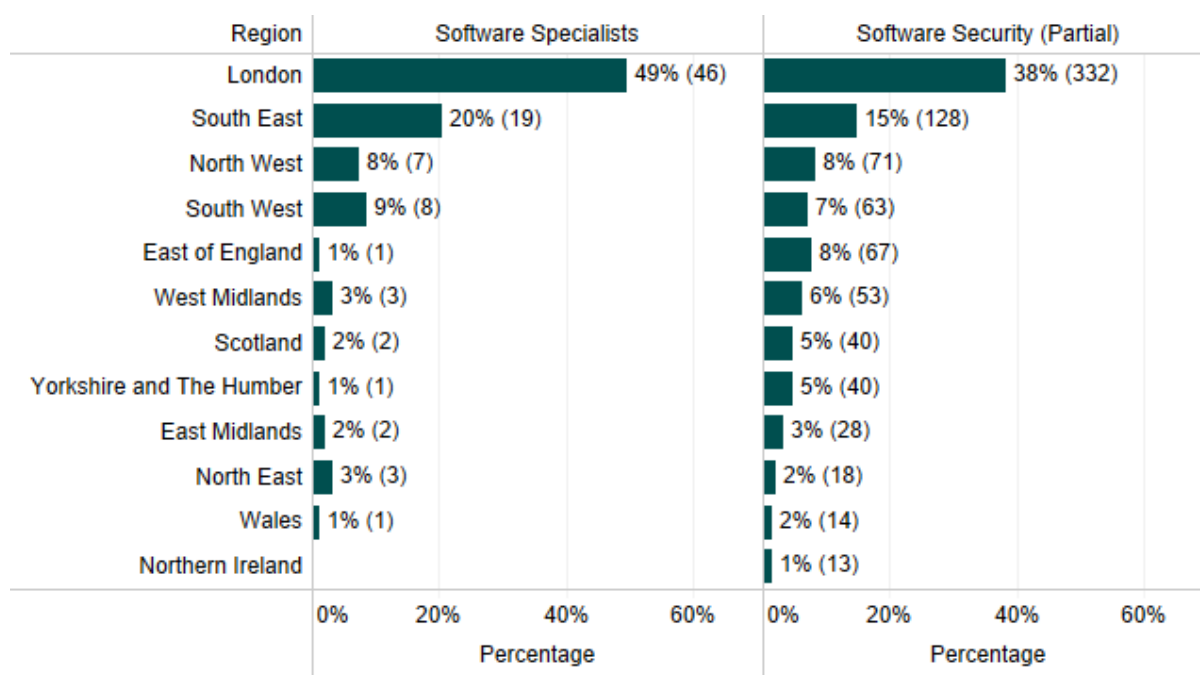
Source: Perspective Economics analysis, n = 66 providers

### Specialist Software Security Providers:

For specialist software security providers (n=93), registration data shows similar concentration in London (49%, 46 firms) and the South East (20%, 19 firms). Regional distribution remains limited, with the South West (9%, 8 firms) and North West (8%, 7 firms) representing other clusters outside of London and South East.

However, wider (partial) provision of software security suggests (n=772) a more distributed pattern. While London maintains the highest concentration (38%, 332 firms), there are more substantial regional counts from the North West, East of England, and South West (each 7-8%). Scotland and Wales demonstrate modest but established presence (40 and 14 firms respectively). Every UK region appears to contain firms offering some form of software security provision, which is beneficial from a market access perspective.

Figure 3.8. UK Registered Location (Software Security)



Source: Perspective Economics analysis, n = 960 providers

## Investment

This section explores external investment in Cyber Security for AI and Software Security firms. Given the nascence of many of these firms, the extent of external investment can reflect both expectations and future demand for these solutions, as well as provide an indication of how companies are able to secure external finance for product development and growth.

Given the relatively small sample frame for Cyber Security for AI firms, we provide an overview of investment and case studies. The data for specialist software security firms is considered to be more extensive and can be tracked over a longer period of time.

### Cyber Security for AI:

Using the Beauhurst platform, we estimate that 20 of the 66 (30%) Cyber Security for AI firms have raised some form of external investment. However, this includes a wide set of firms as discussed in previous sections. For the 14 Cyber Security for AI specialist firms identified, seven of these (50%) have raised external investment. We estimate these firms have raised over £82m<sup>6</sup> since incorporation, with the majority (£68m) of this investment occurring since Q1 2022. Some key investments include:

- **Mindgard** help clients automate and scale security testing, detection, response and remediation of their AI models. In 2023, they raised £3m<sup>7</sup> in seed funding to scale the business, followed by a further \$8m in late 2024.
- **Harmonic Security**, a specialist in data protection for GenAI, have raised over \$26m (£20m)<sup>8</sup> to support expansion of their AI model security testing capabilities and international growth, particularly focusing on financial services and healthcare sectors.
- **418Sec (Huntr)**: In 2023, Protect AI announced the launch of huntr<sup>9</sup>, an AI/ML based bug bounty platform, that enables website owners to identify vulnerabilities within their infrastructure. Originally established by 418Sec, huntr.dev rose to become the world's

---

<sup>6</sup> £62m identified via Beauhurst, plus Harmonic

<sup>7</sup> Lancaster University (2023), 'Lancaster University spinout Mindgard Ltd raises £3M in seed funding', Available at: <https://www.lancaster.ac.uk/news/lancaster-university-spinout-mindgard-ltd-raises-3m-in-seed-funding>

<sup>8</sup> Harmonic Security (2024), 'Harmonic Security raises \$17.5 million Series A to accelerate zero-touch data protection to market', Available at: <https://www.harmonic.security/blog-posts/harmonic-security-raises-17-5-million-series-a-to-accelerate-zero-touch-data-protection-to-market>

<sup>9</sup> Protect AI (2023), 'Protect AI acquires Huntr; Launches world's first artificial intelligence and machine learning bug bounty platform', Available at: <https://protectai.com/newsroom/protect-ai-acquires-huntr>

fifth largest Certified Naming Authority for common vulnerabilities and exposures in 2022.

We also note investments raised by firms developing adjacent Cyber Security for AI capabilities, such as Optalysys<sup>10</sup> (have raised over £31m) to develop optical processors with applications in big data and supercomputing; Pimloc<sup>11</sup> (have raised over £8m) to develop AI-driven, automated and selective anonymisation of video for data privacy use cases; and Hazy<sup>12</sup> (who develop security software to anonymise data and protect customer information) have raised over £13m.

### **Software Security (Specialists)**

We have identified £828m of investment across 42 deals among 15 specialist software security firms over the last five years (2019 – 2024). However, analysis of this external investment data requires careful interpretation due to outliers. While the data shows total investment reaching £432m in 2021, approximately £400m of this reflects Snyk's individual fundraising activity. Adjusting for this outlier provides a more representative view of broader market dynamics.

Deal volume has remained relatively stable (6-7 deals annually) through 2019-2021, before moderating in recent years. This suggests a maturing market, with capital increasingly focused on established firms rather than early-stage investments. The 2024 data (£125m across fewer deals) supports this interpretation with firms such as PortSwigger and OnSecurity raising investment in 2024.

This investment pattern reflects broader market development, where initial investment is followed by targeted growth capital for established providers. Recent investment suggests continued market confidence in specialist software security solutions, particularly those with demonstrated product-market fit and scalable business models.

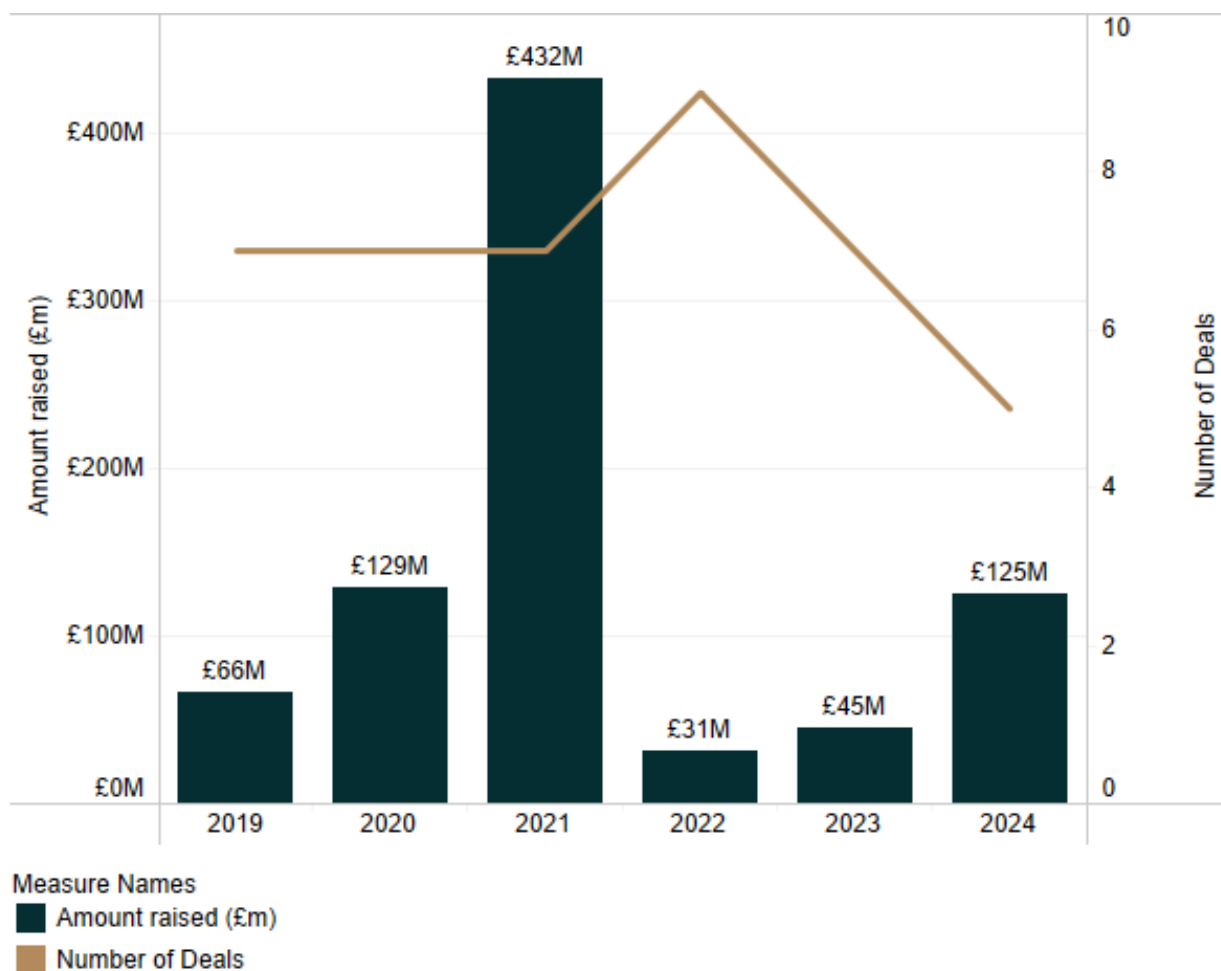
---

<sup>10</sup> UK Tech News (2023), 'Optalysys secures £21 million Series A investment led by Lingotto', Available at: <https://www.uktechnews.info/2023/07/17/optalysys-secures-21-million-series-a-investment-led-by-lingotto/>

<sup>11</sup> Pimloc (2023), 'Pimloc raises \$7.5M for visual AI that protects privacy instead of imperils it', Available at: <https://www.pimloc.com/blog-1/pimloc-raises-7m-for-visual-ai-that-protects-privacy-instead-of-imperils-it>

<sup>12</sup> Hazy (2023), 'Announcing our Series A funding', Available at: <https://hazy.com/resources/2023/03/28/announcing-our-series-a-funding>

Figure 3.9. External VC Investment in UK Software Security



Source: Perspective Economics, Beauhurst

Some notable software security investments in 2023 and 2024 include:

- **PortSwigger** secured £88m<sup>13</sup> growth investment in June 2024 from Five Arrows to accelerate their web security testing platform development and expand international market presence. The investment reflects strong market validation of their Burp Suite product line and growing enterprise demand.
- **Panaseer** has raised over £36m<sup>14</sup> to enhance their Continuous Controls Monitoring platform and expand global market presence.

<sup>13</sup> UK Tech News (2024), 'Bootstrapped PortSwigger secures £88m in first external investment', Available at: <https://www.uktech.news/cybersecurity/portswigger-brighton-park-capital-funding-20240701>

<sup>14</sup> Panaseer (2023), 'Cybersecurity startup Panaseer raises \$26.5M Series B led by AllegisCyber Capital', Available at: <https://panaseer.com/about/press-awards/cybersecurity-startup-panaseer-raises-26-5m-series-b-led-by-allegiscyber-capital>

- **Crypto Quantique** secured £6m in Q4 2023 to develop their quantum-driven semiconductor security solutions, specifically targeting IoT device protection use cases. They have raised over £19m to date.
- **OnSecurity** raised over £5.5m seed funding<sup>15</sup> in 2024 to expand their penetration testing platform and grow their testing team capabilities.

## Customers, Partnerships and Demand

Analysis of customer and partnership data provides insight into market demand and sector maturity across both AI and software security provision. **We have used web data to identify thousands of customers and partnerships mentioned by providers. Each customer or partnership has been analysed and categorised by sector or use case.**

The following provides a high-level overview; however, these typically reflect case studies and notable customers mentioned by providers, and as such, provide an initial indication of customer types and demand. This may be liable to some skew where providers are more likely to mention particular customer archetypes; however, this does provide some useful insight into adoption and use cases.

### Cyber Security for AI Demand

For specialist Cyber Security for AI providers, web analysis identified 45 strategic partnerships mentioned by 12 providers, indicating early stages of market development. However, notable examples include:

- **Advai:** Demonstrates strong public sector engagement through the Defence and Security Accelerator (DASA), with established partnerships across UK Ministry of Defence and leading AI research institutions such as the AI Security Institute.
- **Harmonic Security:** Recognition as a Gartner 'Cool Vendor' in Data Security, with strategic integration partnerships including KnowBe4, focusing on secure GenAI implementation.
- **Mindgard** have leveraged institutional support through schemes such as the NVIDIA Inception Programme, Microsoft Founders Hub, and academic partnerships via Lancaster University.
- **Holistic AI** have worked with customers such as MindBridge, Starling Bank and Unilever.

---

<sup>15</sup> FinSMEs (2024), 'OnSecurity Technology raises £5.5M in Seed funding', Available at: <https://www.finsmes.com/2024/06/onsecurity-technology-raises-5-5m-in-seed-funding.html>

## Software Security Demand

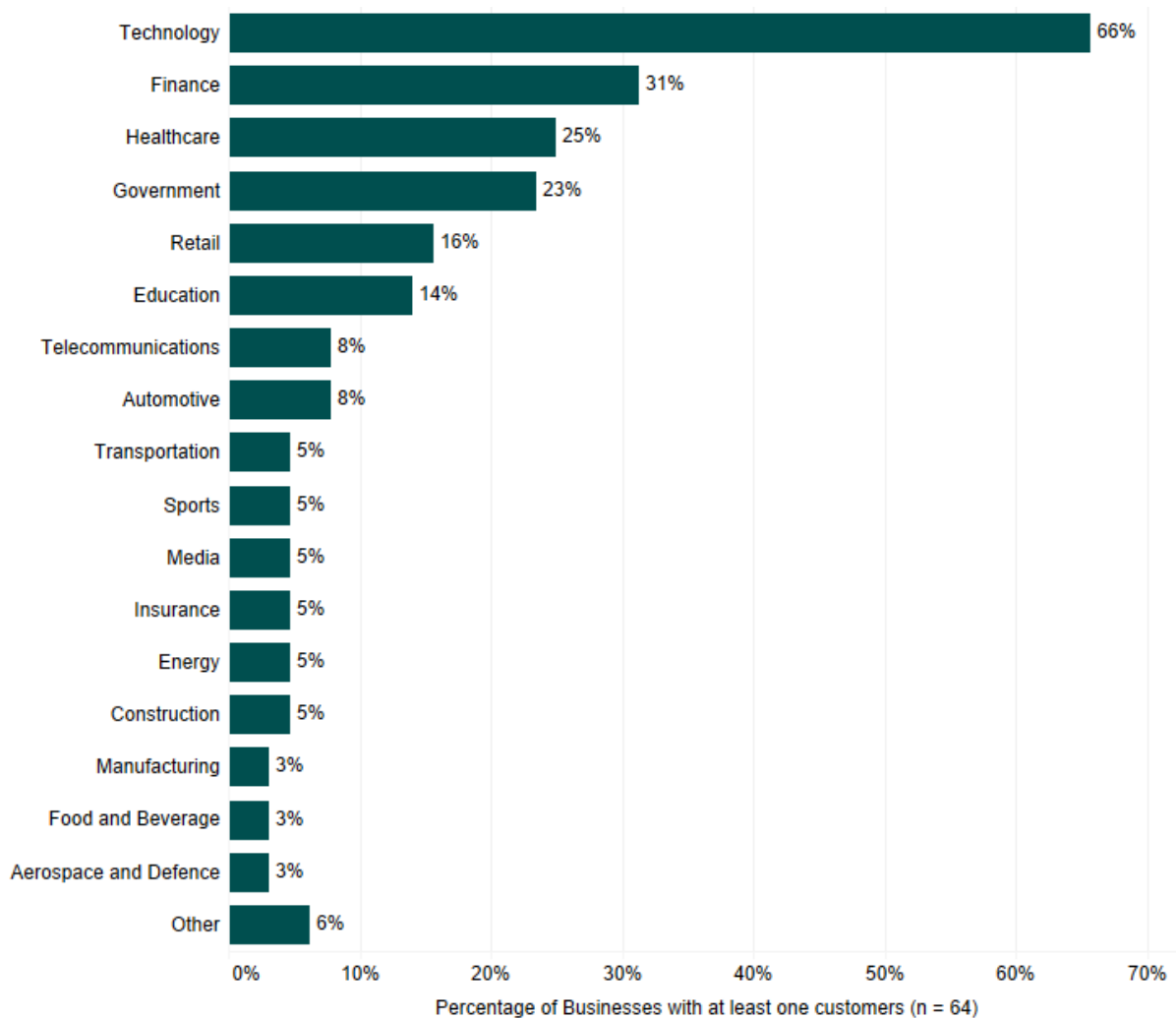
For specialist software security providers, we found that 64 providers mentioned at least one customer or partnership within web data. Providers typically work across a range of sectors; however, the data suggests that 66% of providers mentioned at least one customer within the broader tech sector, followed by 31% that mentioned a financial services customer. Healthcare (25%) represent the next largest customer segment, followed by government (23%).

We also identified approximately 1,400 customer and partner mentions across web data for 428 software security providers. We also note that some caution should be taken with this data, where partnerships and case studies may be more prone to include 'high profile' organisations. However, this highlights a strong public sector presence (e.g. organisations such as the Ministry of Defence (23 mentions) UK Government (12) and NHS (15) are commonly mentioned. Further, there are also signs of strategic technology partnerships e.g. Microsoft, Cisco, and Oracle; financial services adoption e.g. Lloyds Banking Group, HSBC, BNP Paribas; and international reach e.g. NATO, US Department of Defense.

This customer distribution suggests broad market penetration across some critical infrastructure sectors and the public sector, with particular focus in public sector and regulated industries. However, the count of unique customers is typically singular, suggesting potential scope for further market growth and adoption of specific software security solutions across the UK.

### Software Security Specialists:

Figure 3.10. Percentage of Software Security (Specialists): Sector Focus

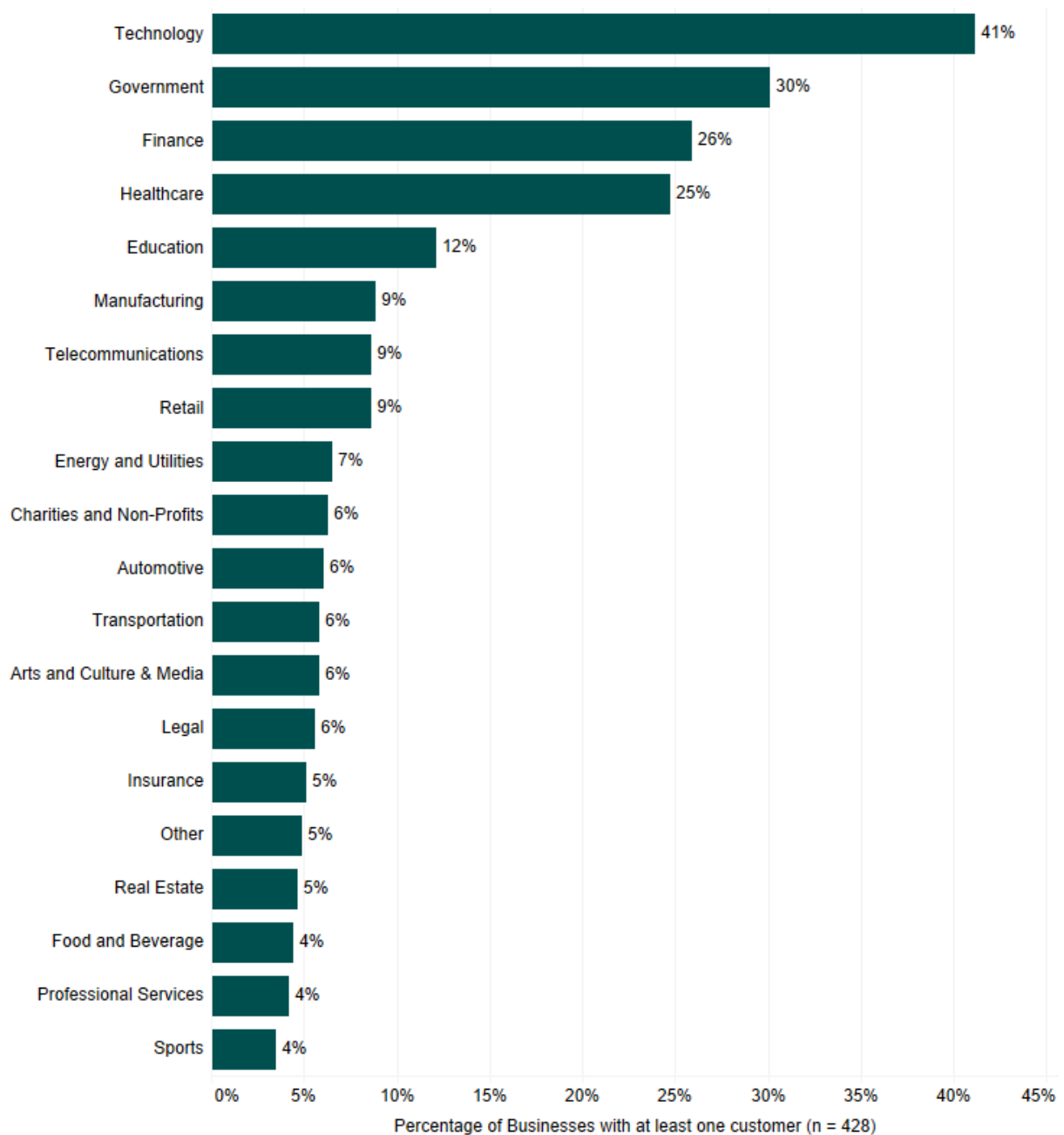


Source: Perspective Economics analysis of web data

Analysis of the wider software security provider base (n=428 with known data) as shown in Figure 3.11 indicates broader sectoral engagement compared to specialist providers. While technology customers remain the primary customer sector (41% of all providers mention at least one consumer in this sector), there is notable engagement across government (30%), finance (26%), and healthcare (25%). The data also suggests more extensive engagement with manufacturing (9%), telecommunications (9%), and critical national infrastructure segments such as energy and utilities (7%). This wider distribution likely reflects pre-established relationships between these sectors and IT service providers, who may be encouraged to integrate software security capabilities into existing service delivery.

This broader adoption pattern presents potential policy considerations, particularly regarding software security deployment in the context of increasing AI adoption. Organisations may also prefer to use existing IT partnerships for software security. This suggests an opportunity to explore how broader software security providers could support national security objectives, potentially offering a more practical route for implementing security standards and best practice across the wider economy.

Figure 3.11. Percentage of Software Security (All): Sector Focus



Source: Perspective Economics analysis of web data



## 4. Technical Analysis

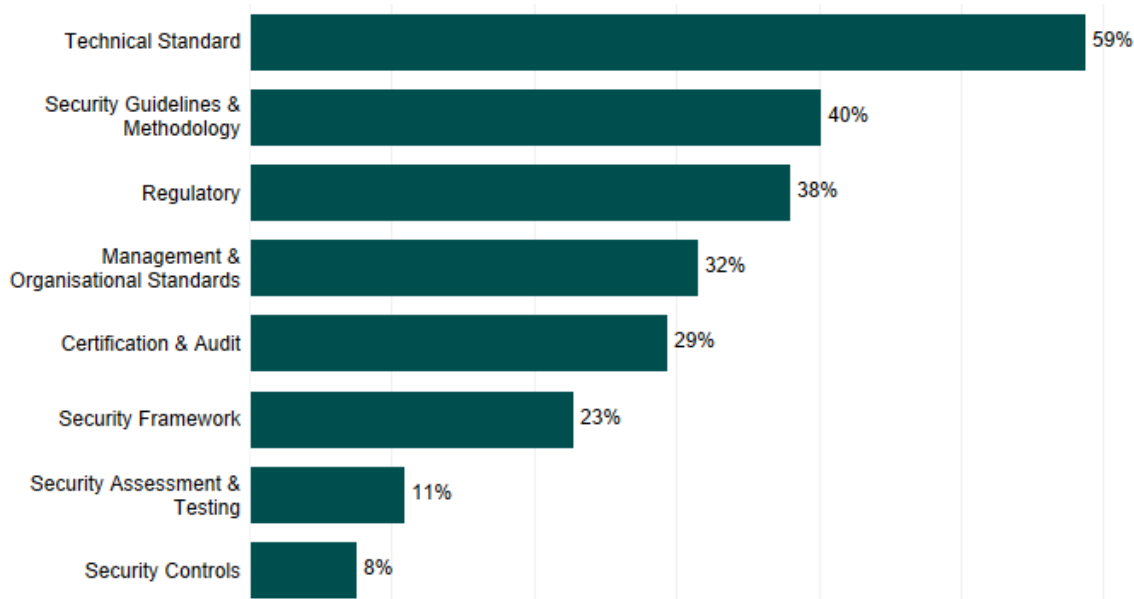
This section examines standards engagement, certifications, and technical capabilities across software security providers. This analysis is informed by web data to identify common approaches and emerging technical priorities.

A review of provider engagement with standards indicates broad adoption across multiple categories. Technical standards (59%) show highest prevalence, followed by security guidelines and methodologies (40%), and regulatory compliance (38%). This suggests mature engagement with established standards frameworks.

Key areas of standards engagement include:

- Technical Standards: ISO 27001, PCI DSS Software Security Standards, FIPS 140-2
- Security Guidelines: OWASP methodology adoption and implementation
- Regulatory Alignment: HIPAA, GDPR, CCPA compliance
- Management Standards: NIST framework implementation, ISO 9001

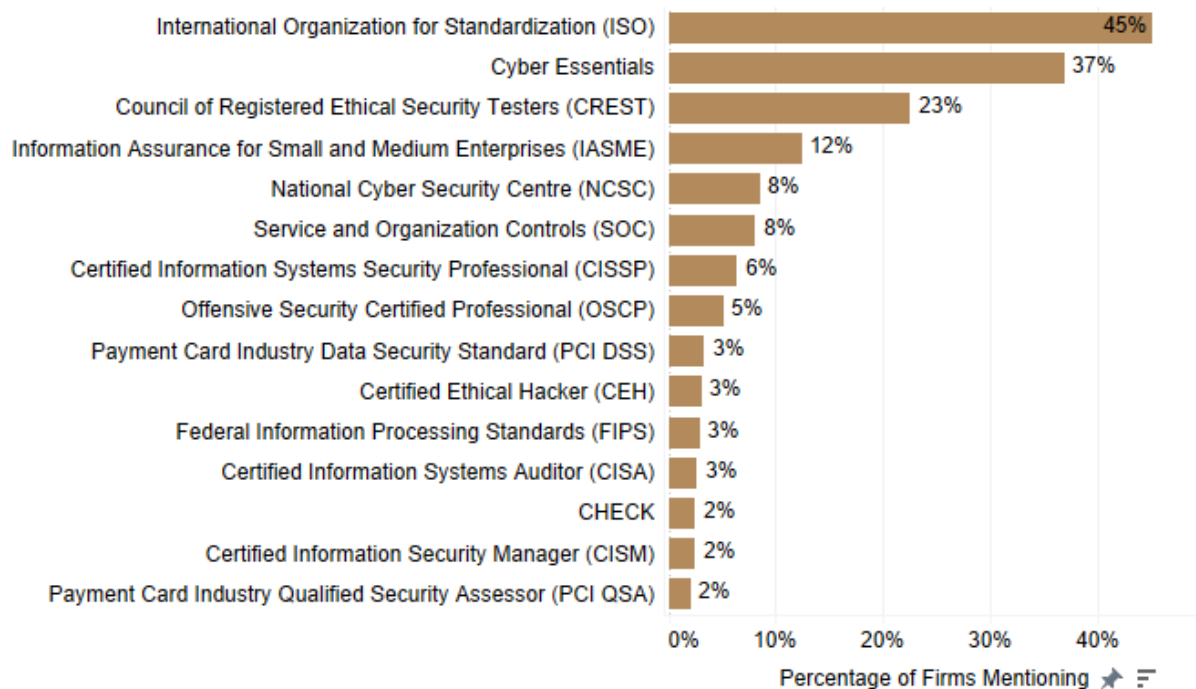
Figure 4.1. Percentage of Software Security Specialists mentioning standards



Source: Perspective Economics analysis of web data (n = 92 with standards identified)

Analysis of certification mentions across providers highlights ISO certification prevalence (45%), followed by Cyber Essentials (37%) and CREST (23%). UK providers also provide reference to established national recognition among organisations such as IASME (12%) (aligned to Cyber Essentials) and the NCSC.

Figure 4.2. Top 15 Standards and Credentials Mentioning by Software Security Firms



Source: Perspective Economics analysis of web data (n = 483 firms with identified standards or credentials)

Web review also identified several common technical themes across a range of providers, such as:

- Widespread adoption of continuous monitoring approaches
- Growing implementation of Continuous Threat Exposure Management (CTEM).
- Strong focus on end-to-end encryption capabilities.
- Provider engagement with the use of Software Bill of Materials (SBOM), with firms such as APH10 and Device Authority specialising in SBOM implementation.
- Established use of CVE Program and CVSS frameworks for vulnerability management e.g. with firms such as AppCheck being authorised by the Common Vulnerabilities and Exposures (CVE) Program as a CVE Numbering Authority (CNA),

While the Cyber Security for AI provider sample remains too limited for detailed analysis, evidence suggests concentration in LLM security with emerging capability in areas such as quantum security and training data protection. These may represent potentially important areas for future market development.