

UK Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 120 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License \$4750.00
- Team License (1-7 Users) \$5250.00
- Site License \$6500.00
- Corporate License \$8750.00

Report description:

The UK Cybersecurity Market size is estimated at USD 17.36 billion in 2025, and is expected to reach USD 28.49 billion by 2030, at a CAGR of 10.42% during the forecast period (2025-2030).

Key Highlights

- Increasing cyberattacks in the country have propelled it to strengthen its defensive capabilities, and the rising demand for digitalization and scalable I.T. Infrastructure, the increasing need to tackle risks from third-party vendor risks, and the adoption of a cloud-first strategy has been driving the growth of cybersecurity solutions and services in the country.
- The British government recently launched a new National Cyber Security Strategy, hailed as a 'blueprint' to protect the U.K. from cyber threats and 'solidify its position as a global cyber power.' The strategy also signals further moves to reduce the U.K.'s reliance on international suppliers or technologies that do not share 'the U.K.'s values.
- According to gov. uk, the U.K.'s cybersecurity sector is quickly increasing, with over 1400 businesses making £8.9 billion in revenue last year, supporting 46,700 skilled jobs, and attracting significant outside investment. This business is vital to cyber power, security, global influence, and economic development.
- For Vision 2030, the United Kingdom and India collaborated in April 2022 to strengthen their mutual cyber resilience by advancing a comprehensive and whole-of-society approach. To accomplish the alliance, the states emphasized their commitment to a collaborative program of cooperation concentrating on cyber governance, resilience, deterrence, and capacity building.
- With the growing 5G and total fiber broadband networks in the country, the government, in collaboration with telecommunication companies, is taking initiatives to tackle cyberattacks and improve security standards and practices across the United Kingdom's telecoms sector.
- The increased rate of cybercrimes has driven the focus on developing new solutions to tackle them, which has characterized the country's investment landscape. For instance, Bridewell Consulting, a cybersecurity services company dealing with Managed

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

Detection Response and Security Operations Centre, acknowledged a multi-million dollar investment from Growth Capital Partners, a private equity firm, to expand its operations in the U.K. and the rest of Europe.

- The U.K. is also home to the largest cybersecurity event in Europe, Infosecurity Europe. The event has over 400 exhibitors, including over 120 U.S. companies, that showcase their latest information security solutions and products to over 19,500 industry professionals.

- Further, the vulnerability and exposure to diverse cyber-attacks have increased with the increased Internet of Things (IoT) devices. Along with smart city initiatives, the trend of increasing IoT and connected devices in the country is expected to continue during the forecast period.

UK Cyber Security Market Trends

Cloud Deployment Segment is Expected to Register a Significant Growth in the Market

- The increasing realization among enterprises regarding the importance of saving money and resources by moving their data to the cloud instead of building and maintaining new data storage drives the demand for cloud-based solutions and, hence, the adoption of on-demand security services in the United Kingdom. Owing to multiple benefits, cloud platforms, and ecosystems are anticipated to serve as a launchpad for an explosion in the pace and scale of digital innovation over the next few years.
- Security has been a critical consideration at each step of the cloud adoption cycle as IT provision has moved from on-premise to outside of a company's walls. SMEs prefer cloud deployment as it allows them to focus on their core competencies rather than invest their capital in security infrastructure since they have limited cybersecurity budgets.
- Furthermore, deploying public cloud services extends the boundary of trust beyond the organization, making security a vital part of the cloud infrastructure. However, the increasing usage of cloud-based solutions has significantly simplified enterprises' adoption of cybersecurity practices.
- With the increased adoption of cloud services, such as Google Drive, Dropbox, and Microsoft Azure, and with these tools emerging as an integral part of business processes, enterprises must deal with security issues, such as losing control over sensitive data. This increases the incorporation of on-demand cybersecurity solutions in the country.
- Additionally, the increased adoption of cloud-based email security services is driving the adoption of services integrated with other security platforms, such as IPS and NGFW. This trend demotes enterprises to spend on on-premise and dedicated email or web security solutions.
- Cloud-based solutions also benefit from lower capital expenditure requirements, thus making the business much more compelling. Deploying cloud-based services can significantly reduce the Capex requirement as the companies need not invest in hardware components, driving the growth of cloud-based solutions in the country.

BFSI Segment to hold significant share in the market

- The BFSI industry is one of the critical infrastructure segments that face multiple data breaches and cyber-attacks, owing to the massive customer base that the sector serves and the financial information that is at stake.
- Being a highly lucrative operation model with phenomenal returns and the added upside of relatively low risk and detectability, cybercriminals are optimizing a plethora of diabolical cyberattacks to immobilize the financial sector. These attacks' threat landscape ranges from Trojans, malware, ATM malware, ransomware, mobile banking malware, data breaches, institutional invasion, data thefts, fiscal breaches, etc.
- Various public and private banking institutes are focusing on implementing the latest technology to prevent cyber attacks with a strategy to secure their IT processes and systems, secure customer critical data, and comply with government regulations.

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

Besides, with greater customer expectations, rising technological capabilities, and regulatory requirements, banking institutions are pushed to adopt a proactive security approach.

- With the growing technological penetration and digital channels, such as mobile banking, Internet banking, etc., online banking has become customers' preferred choice for banking services. There is a significant need for banks to leverage advanced authentication and access control processes.
- In 2022, financial firms worldwide were impacted by innovative new ransomware tactics that maximized ROI for the threat actors. While financial firms represent a small percentage of victims directly targeted by ransomware attacks, they can and have been impacted by attacks on third parties, who are prime targets. Such threats are poised to increase the usage of cybersecurity solutions in the BFSI sector in the country.

UK Cyber Security Industry Overview

UK Cybersecurity Market is semi-fragmented and has some major players who have adopted various growth strategies, such as mergers and acquisitions, new product launches, expansions, joint ventures, partnerships, and others, to strengthen their position in this market. The major players in the market are IBM Corporation, Cisco Systems Inc., Trend Micro Incorporated (UK), Broadcom Limited, and BAE Systems Inc., among others.

In October 2022 - Simplex Services, a Brighton-based digitalization services provider, partnered with NovigoSolutions, a technology solutions vendor based in Dallas. The cooperation will benefit from Simplex Services' Microsoft Cloud capabilities, which include Power Platform, SharePoint, Dynamics, Microsoft 365, Robotic Process Automation with UiPath, and Cybersecurity. Simplex will be able to support its clients by using Novigo's resource pool, boosting its market reach, increasing growth possibilities, and addressing challenges across many sectors.

In July 2022, The Cybersecurity and Infrastructure Security Agency (CISA) announced its first Attache Office in London. The Attache Office will serve for international collaboration between CISA, UK government officials, and other federal agency officials, thereby advancing CISA's missions in cybersecurity, critical infrastructure protection, and emergency communications and leveraging the agency's global network.

In April 2022, India and the United Kingdom partnered to increase their mutual cyber resilience, taking a holistic and whole-of-society approach to Vision 2030. The countries outlined their commitment to a joint cooperation program to deliver the partnership, focused on cyber governance, deterrence, resilience, and capacity building.

Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

Table of Contents:

1 INTRODUCTION

- 1.1 Study Assumptions and Market Definition
- 1.2 Scope of the Study

2 RESEARCH METHODOLOGY

3 EXECUTIVE SUMMARY

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

4 MARKET INSIGHTS

4.1 Market Overview

4.2 Industry Value Chain Analysis

4.3 Industry Attractiveness - Porter's Five Forces Analysis

4.3.1 Bargaining Power of Buyers

4.3.2 Bargaining Power of Suppliers

4.3.3 Threat of New Entrants

4.3.4 Threat of Substitutes

4.3.5 Intensity of Competitive Rivalry

4.4 Impact of COVID-19 on the Market

5 MARKET DYNAMICS

5.1 Market Drivers

5.1.1 Increasing Demand for Digitalization and Scalable IT Infrastructure

5.1.2 Need to tackle risks from various trends such as third-party vendor risks, the evolution of MSSPs, and adoption of cloud-first strategy

5.2 Market Restraints

5.2.1 Lack of Cybersecurity Professionals

5.2.2 High Reliance on Traditional Authentication Methods and Low Preparedness

5.3 Trends Analysis

5.3.1 Organizations in Thailand increasingly leveraging AI to enhance their cyber security strategy

5.3.2 Exponential growth to be witnessed in cloud security owing to shift toward cloud-based delivery model.

6 MARKET SEGMENTATION

6.1 By Offering

6.1.1 Solutions

6.1.1.1 Application Security

6.1.1.2 Cloud Security

6.1.1.3 Data Security

6.1.1.4 Identity and Access Management

6.1.1.5 Infrastructure Protection

6.1.1.6 Integrated Risk Management

6.1.1.7 Network Security Equipment

6.1.1.8 End point Security

6.1.1.9 Other Solutions

6.1.2 Services

6.1.2.1 Professional Services

6.1.2.2 Managed Services

6.2 By Deployment Mode

6.2.1 Cloud

6.2.2 On-Premise

6.3 By Organization Size

6.3.1 SMEs

6.3.2 Large Enterprises

6.4 By End User

6.4.1 BFSI

6.4.2 Healthcare

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

- 6.4.3 IT and Telecom
- 6.4.4 Industrial & Defense
- 6.4.5 Retail
- 6.4.6 Energy and Utilities
- 6.4.7 Manufacturing
- 6.4.8 Others

7 COMPETITIVE LANDSCAPE

- 7.1 Company Profiles
 - 7.1.1 IBM Corporation
 - 7.1.2 Cisco Systems Inc
 - 7.1.3 Trend Micro Incorporated (UK)
 - 7.1.4 Broadcom Limited
 - 7.1.5 BAE Systems Inc.
 - 7.1.6 Dell Technologies Inc.
 - 7.1.7 Fortinet Inc.
 - 7.1.8 Palo Alto Networks
 - 7.1.9 McAfee, LLC
 - 7.1.10 Intel Security (Intel Corporation)

8 INVESTMENT ANALYSIS

9 FUTURE OF THE MARKET

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

UK Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 120 pages | Mordor Intelligence

To place an Order with Scotts International:

- ☐ - Print this form
- ☐ - Complete the relevant blank fields and sign
- ☐ - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	\$4750.00
	Team License (1-7 Users)	\$5250.00
	Site License	\$6500.00
	Corporate License	\$8750.00
		VAT
		Total

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-03-02
		Signature	

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com



Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com
www.scotts-international.com