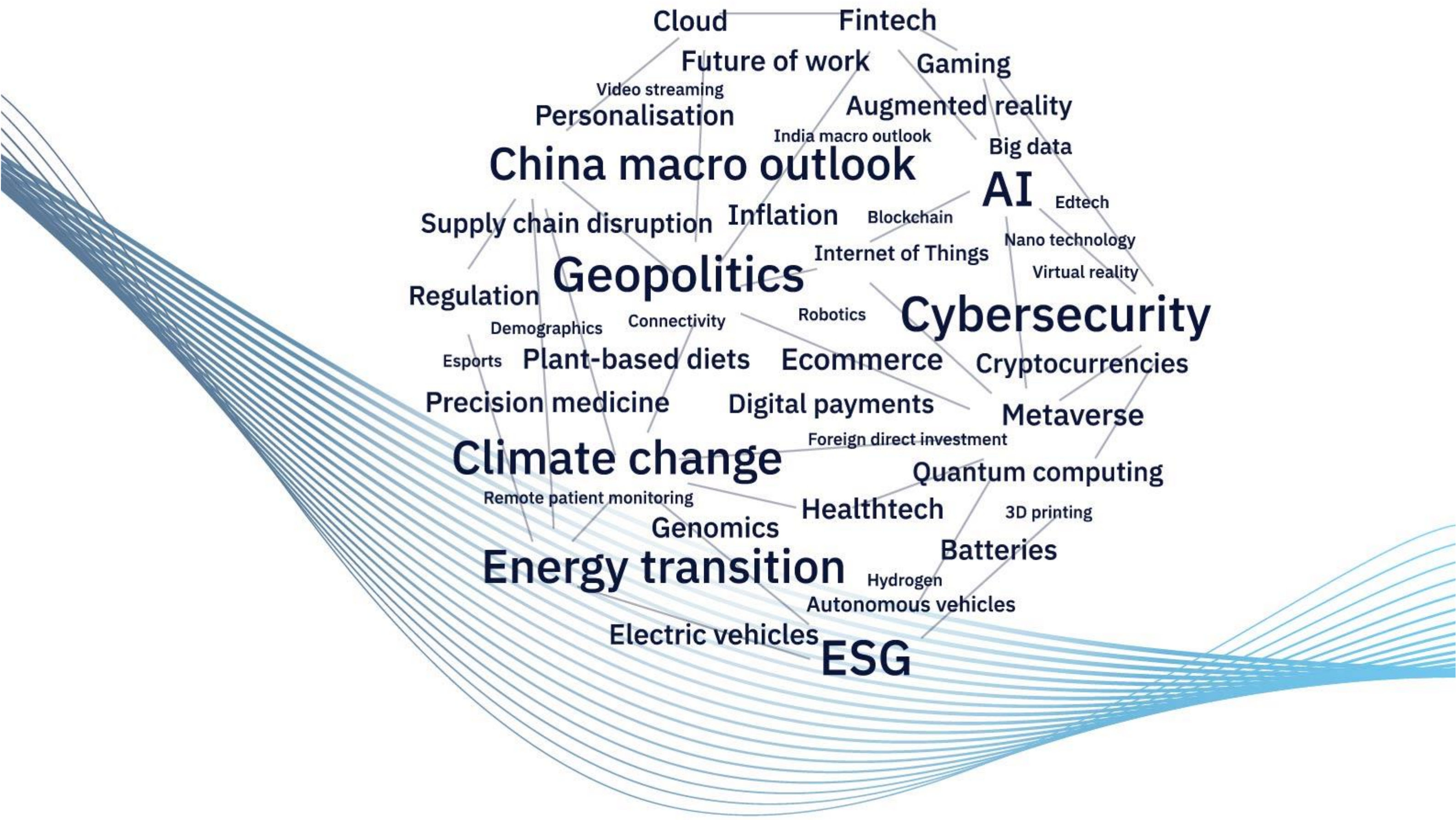


Thematic Intelligence
Technology

GDTMT-TR-S501
April 24, 2024

Cybersecurity

Contents

Executive Summary

Cybersecurity faces an AI challenge

The cybersecurity industry faces a challenge that is anything but business as usual. The prospect of offensive attacks using artificial intelligence (AI) is prompting increases in cybersecurity budgets as organizations try to understand the impact of generative AI on their security.

Cybersecurity grabs a bigger share of corporate IT budgets

Cybersecurity budgets will grow in step with IT budgets in 2024 as organizations come to terms with AI's impact on their operations.

Cybersecurity M&A will be a strong focus during 2024

Cisco's $XX billion acquisition of Splunk will be a catalyst for AI-led cybersecurity M&A deals in 2024 and beyond as the cybersecurity industry comes to terms with generative AI-led cyberattacks.

Leaders and challengers

Three of our cybersecurity value chain's pivotal areas are identity management, network security, and cloud security. Below are the leaders and challengers in these areas.

Click here to purchase the full report

Identity management

- **Leaders:** Okta among others
- **Challengers:** Duo Security among others

Network security

- **Leaders:** Fortinet among others
- **Challengers:** Appgate among others

Cloud security

- **Leaders:** Microsoft among others
- **Challengers:** IBM among others

Inside

Related reports

- Artificial Intelligence
- Global TMT M&A Deals 2023 - Top Themes and Predictions
- Cybersecurity (2023)

Report type

- **Single theme**
- Multi-theme
- Sector scorecard

Players

Cybersecurity players provide products and services to secure their clients' systems and applications. Their coverage ranges from chip-based security to identity management, network, cloud, and application security, and services such as managed security, post-breach response, and risk and compliance.

Who are the leading players in the cybersecurity theme, and where do they sit in the value chain?

Click here to purchase the full report

Source: GlobalData

Source: GlobalData

Technology Briefing

This section looks at the principal threat actors, the most common types of cyberattacks, and the main stages of an attack.

Threat actors

The cybersecurity landscape is complex. Today's always-connected world offers many opportunities for cyberattackers to disrupt countries, organizations, and individuals.

The table below shows the four main types of threat actors – thieves, hacktivists, terrorists, and other malicious players.

Threat actors	Motives	Assets targeted	Insurance implications
Thieves (typically in organized crime syndicates)	▪ Data theft ▪ Monetary theft ▪ Extortion	▪ Personal information ▪ Credit card data ▪ Money ▪ Corporate IT infrastructure	▪ Physical assets can be insured if identified ▪ Brand loyalty and customer loss are more difficult and expensive to protect with insurance
Click here to purchase the full report			

Source: GlobalData

Types of cyberattack

Cyberattacks can be split into two types: un-targeted or targeted.

Un-targeted cyberattacks

In un-targeted attacks, attackers will target as many devices, services, or users as possible. There is little direct interest in the victim because there will always be several machines or services with vulnerabilities. Attackers typically use techniques that take advantage of the internet's openness.

Targeted cyberattacks

In a targeted attack, an organization is identified because the attacker has a specific interest in its business or has been paid to target it. Planning the attack could take months as hackers look for the best route to deliver exploits directly to an organization’s systems (or users).

Organizations’ technical complexity breeds vulnerability

The enterprise of today is complex—and a perfect environment for hackers

Click here to purchase the full report

Source: GlobalData

Source: GlobalData

Stages of an attack

Cyberattacks typically have several stages in common. They may have repeated stages, where an attacker probes defenses, looking for weaknesses to exploit. The UK’s National Cyber Security Centre (NCSC) has defined the four stages of a cyberattack using a simplified version of the Cyber Kill Chain (produced by Lockheed Martin).

The survey stage

In the survey stage, attackers will seek any means available to find technical, procedural, or physical vulnerabilities that they can use to exploit defenses.

The delivery stage

During the delivery stage, an attacker will look to get into a position where they can exploit any vulnerability they have identified or that could potentially exist.

The breach stage

The harm an attack will create depends on the nature of the vulnerability and the exploitation method. The attack may allow the attacker to:

- Make changes that affect a system's operations.

The impact stage

In the impact stage, the attacker typically seeks to explore systems, expand their access, and establish a persistent presence, a process sometimes called consolidation.

Trends

The main trends shaping the cybersecurity theme over the next 12 to 24 months are shown below. These trends are classified into three categories: technology, macroeconomic, and regulatory.

Technology trends

The table below highlights the key technology trends impacting the cybersecurity theme.

Trend	What's happening?
AI as a threat	It is still too early to know where the balance truly lies in how AI impacts organizations' cybersecurity positioning. AI can help organizations improve their efficiency in threat detection, hunting, and incident response, but at the same time, adversaries will use AI in cyberattacks. A simple example is cybercriminals using generative AI to strengthen phishing attacks by eliminating the telltale signs of fake messages, such as poor grammar and spelling mistakes. ***Click here to purchase the full report***
How AI can help threat detection	***Click here to purchase the full report***
Ransomware	
Multi-factor authentication	
Mobile cybersecurity	
Cloud security	
DevSecOps	
Supply chain attacks	
Endpoint protection	

Trend	What's happening?
Open-source intelligence (OSINT)	*Click here to purchase the full report*
Convergence of security technology solutions	
Ransomware as a service	
Zero trust adoption	
Automotive hacking	
Password-less security	
Chip-based security	
Extended detection and response (XDR)	
5G rollout	

Source: GlobalData

Macroeconomic trends

The table below highlights the key macroeconomic trends impacting the cybersecurity theme.

Trend	What's happening?
The Ukraine conflict	Russia has used cyberattack tactics against Ukraine since the annexation of Crimea began in 2014. While many of these attacks are not confirmed to be state-sponsored, a November 2015 attack on the Ukrainian power grid that left over XX people without power was reportedly linked to Russia. Similarly, in 2017, the UK National Cyber Security Centre concluded that the NotPetya ransomware attack was "almost certainly" linked to the Russian military. The attack was one of the costliest in history, costing companies an estimated $XX billion globally. ***Click here to purchase the full report***
State-sponsored attacks	***Click here to purchase the full report***
The cybersecurity skills shortage	
IT budgets	
Cybersecurity culture	
Critical national infrastructure threats	

Source: GlobalData

Regulatory trends

The table below highlights the key regulatory trends impacting the cybersecurity theme.

Trend	What's happening?
Ransomware regulations	Ransomware attacks can be devastating to businesses. Ransomware is malware that blocks access to systems until a ransom is paid. Involving law enforcement reduces the total cost to organizations of a data breach. ***Click here to purchase the full report***
EU cybersecurity legislation	***Click here to purchase the full report***
Mandatory disclosure of cyberattacks	
Cooperation on supply chain security	

Source: GlobalData

Industry Analysis

Market size and growth forecasts

GlobalData forecasts show that the global cybersecurity market will be worth $XX billion by 2027, having grown at a compound annual growth rate (CAGR) of XX% between 2022 and 2027.

Click here to purchase the full report

Global cybersecurity revenues will hit $XX billion in 2027

Software will make up XX% of the market in 2027

Global cybersecurity revenue by segment, 2019 - 2027

Click here to purchase the full report

Source: GlobalData

Note: Our security revenues forecast covers hardware, software, and services. Hardware includes content-filtering and anti-spam appliances, firewalls and VPN appliances, intrusion prevention systems, multi-factor authentication, network access control, and unified threat management appliances. The software includes application security, data protection, endpoint security platforms, fraud prevention, transactional security, identity and access management, messaging security, multi-factor authentication, network monitoring, access control, network security, security intelligence and management, server security, and web security. Services cover all managed security services, including business continuity, DDoS mitigation, emergency incidence response, governance, risk and compliance, identity management, patch management, managed authentication, and managed detection and response services.

Managed security services is the largest single sub-segment of the cybersecurity market

Revenues will reach $XX billion by 2027

Revenues of cybersecurity products and services, 2022 and 2027

Click here to purchase the full report

Source: GlobalData

Buy the report now and get full access.

You are currently viewing sample pages of the Cybersecurity – Thematic Intelligence report.

Buy the Full Report Here

Reasons to Buy the Cybersecurity – Thematic Intelligence Report:

- Get a comprehensive overview of the cybersecurity theme.
- Gain insights into the cybersecurity theme and the **impact it will have on the tech, media, and telecom (TMT) industry globally.**
- Examine the competitive landscape within the cybersecurity theme.
- Identify the **technology, macroeconomic, and regulatory trends** that will shape the cybersecurity theme.

If you have any questions or need additional information:

reportstore@globaldata.com
+44 (0) 20 7947 2960

Buy the Full Report Here

Timeline

Cybersecurity is one of the most fertile and fast-moving areas of technology. New exploits are developed daily, and organizations worldwide repel hundreds of attacks each week.

Click here to purchase the full report

The major milestones in the journey of the cybersecurity theme are set out in the timeline below.

The cybersecurity story

How did this theme get here, and where is it going?

1971	The first computer worm was created, displaying the words, “I am the Creeper: catch me if you can.”
1982	
1986	
1988	
1990	
1999	
2000	
2002	
2008	
2013	
2015	
2016	
2017	
2017	
2018	
2018	
2019	
2019	
2020	
2020	
2020	
2020	
2020	
2021	
2023	
2027	

Click here to purchase the full report

Source: GlobalData

Signals

In this section, we use the 180 million signals generated by our thematic engine to predict how the cybersecurity theme will develop and the likely leaders. These signals are a useful source of competitor intelligence in the cybersecurity market. Our signals include M&As, venture financing deals, patents, company filings, and hiring intentions.

M&A trends

The cybersecurity theme is typically a hotbed of M&A activity.

The key M&A transactions associated with the cybersecurity theme since January 2023 are listed in the table below.

Date announced	Acquirer	Target	Value ($M)	Target company description
Mar 2024	CrowdStrike	Flow Security	Not disclosed	Provider of a cloud data runtime security solution

Click here to purchase the full report

Date announced	Acquirer	Target	Value ($M)	Target company description

Click here to purchase the full report

Source: GlobalData

The dominant role of private equity in cybersecurity

In August 2023, private equity firm Thoma Bravo closed its $XX billion acquisition of cybersecurity firm ForgeRock. The deal came close to being challenged by the US Justice Department over concerns that it would harm competition in identity access management, an increasingly important area of the overall cybersecurity market.

Click here to purchase the full report

Private equity is making an investment business out of cybersecurity

The cybersecurity portfolio of PE companies is starting to attract regulators' interest

Private equity's portfolio of cybersecurity companies

Click here to purchase the full report

Source: GlobalData

Venture financing trends

Venture financing is the lifeblood of new cybersecurity companies. Splunk, bought by Cisco in 2023 for $XX billion, was founded back in October 2003, and its backers were venture firms August Capital, Sevin Rosen, Ignition Partners, and JK&B Capital.

The key venture financing deals associated with the cybersecurity theme since January 2023 are listed in the table below.

Date announced	Company	Amount raised ($M)	Company description
Jan 2024	NinjaOne	XX	Platform for endpoint management

Date announced	Company	Amount raised ($M)	Company description

Click here to purchase the full report

Source: GlobalData

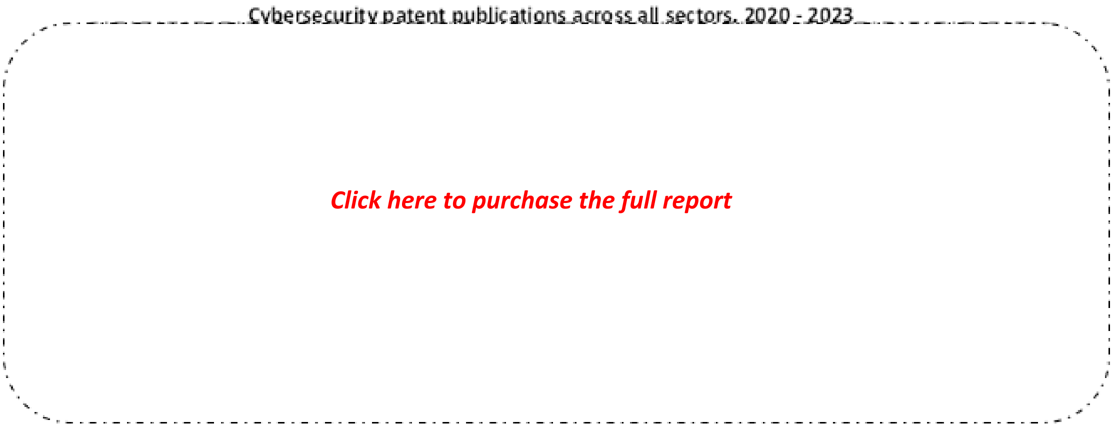
Patent trends

A high number of cybersecurity patents are published across all sectors every year. However, the annual total has declined in each of the last two years.

With AI used by both bad actors to launch attacks and defenders to tackle threats, cybersecurity patent activity will likely increase again in 2024 and 2025.

Patent publications in cybersecurity have declined but will rise again thanks to the impact of AI

The number of cybersecurity patents began to fall in 2022 but will rise in 2024

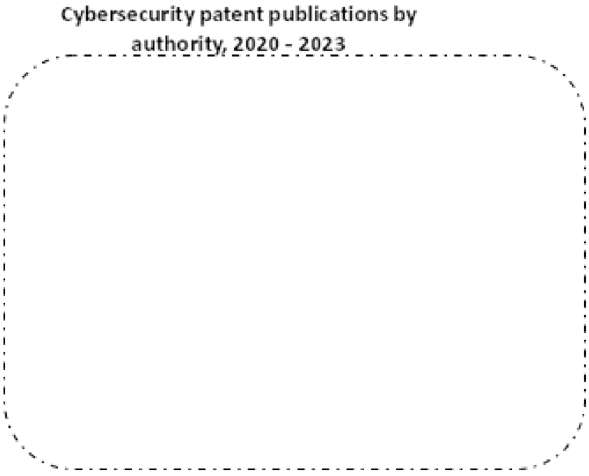


Click here to purchase the full report

Source: GlobalData

China is the top authority registering cybersecurity patents

China has registered the most cybersecurity patents in the last four years



Five of the top 10 companies registering cybersecurity patents are headquartered in the US

Top 10 companies publishing cybersecurity patents, 2020 - 2023

Click here to purchase the full report

Source: GlobalData. Note: EPO = European Patent Office, WIPO = World Intellectual Property Organization.

Company filing trends

The number of mentions of cybersecurity in company filings has more than doubled since 2020.

Click here to purchase the full report

Trends in company filings are on a steeply upward path as threats grow

Filings more than doubled between 2020 and 2023 and are likely to reach XX in 2024

Number of mentions of cybersecurity in company filings across all sectors, 2017 - 2023

Click here to purchase the full report

Source: GlobalData

Hiring trends

There are never enough people working in cybersecurity. There is a continual demand for new blood to help counter a historic cybersecurity skills gap.

With a need for expertise to cope with the likely impact of AI-led cyberattacks, there is every likelihood that the cybersecurity skills gap will continue to grow.

Cybersecurity skills vacancies continue to rise

The demand for cybersecurity skills continues to outpace supply, even after a rise in 2023

Cybersecurity-related active jobs in all sectors, July 2019 - December 2023

Click here to purchase the full report

Source: GlobalData

Buy the report now and get full access.

You are currently viewing sample pages of the Cybersecurity – Thematic Intelligence report.

Buy the Full Report Here

Reasons to Buy the Cybersecurity – Thematic Intelligence Report:

- Get a comprehensive overview of the cybersecurity theme.
- Gain insights into the cybersecurity theme and the **impact it will have on the tech, media, and telecom (TMT) industry globally.**
- Examine the competitive landscape within the cybersecurity theme.
- Identify the **technology, macroeconomic, and regulatory trends** that will shape the cybersecurity theme.

If you have any questions or need additional information:	reportstore@globaldata.com +44 (0) 20 7947 2960

Buy the Full Report Here

Value Chain

The cybersecurity value chain consists of three main areas: hardware, software, and services. The graphic below describes these three elements and identifies the leading vendors across the technology stack.

The cybersecurity value chain

Our cybersecurity value chain consists of three layers: hardware, software, and services

Source: GlobalData

In the following sections, we will look more closely at each segment of the value chain.

Cybersecurity hardware

Chips are used in mission-critical servers and safety-critical applications, so protecting them from cyberattacks is increasingly important.

Chip-based security

In an age where cyberattacks are prevalent, the implications for chip security are significant. Dealing with those cyber threats is becoming an integral part of chip and system design, with a focus on chips being secure by design. With devices and threats becoming more complex, security has evolved from a software problem, in which companies had to deal with continual software patches, to a software and hardware problem that requires a mutual focus on secure design.

The cybersecurity value chain - hardware

Chip-based security: leaders and challengers

Click here to purchase the full report

Source: GlobalData

Click here to purchase the full report to the following valuechain:

- Cybersecurity software
- Cybersecurity services

Companies

In this section, GlobalData highlights companies making their mark within the cybersecurity theme.

Public companies

The table below lists some leading listed players associated with this theme and summarizes their competitive position.

Company	Country	Competitive position in the cybersecurity theme
Accenture	US	Accenture provides cybersecurity consulting services to clients across various topics, including cyber strategy, cyber protection, and cyber resilience. It made several acquisitions in 2020 and 2021 to add to its cybersecurity portfolio, including French cybersecurity services company Openminded and cyber defense company Sentor. Its M&A activity has continued. *Click here to purchase the full report*

Company	Country	Competitive position in the cybersecurity theme
Alphabet (parent company of Google)	US	***Click here to purchase the full report***
Check Point Software	Israel	
Cisco	US	
Cloudflare	US	
CrowdStrike	US	
Darktrace	UK	
Dell Technologies	US	
Fortinet	US	
IBM	US	
Microsoft	US	
Palantir Technologies	US	
Palo Alto Networks	US	
Rapid7	US	
Tenable	US	
Trellix	US	
Zscaler	US	

Source: GlobalData

Private companies

The table below lists some interesting private companies associated with this theme and summarizes their competitive position.

Company	Country	Competitive position in the cybersecurity theme
Cybereason	US	Cybereason provides endpoint security protection software. Its Cybereason XDR platform provides different protection modules, including ransomware protection, next-generation antivirus (NGAV), endpoint controls, and digital forensic and incident response (DFIR). ***Click here to purchase the full report***
Code42	US	***Click here to purchase the full report***
ForgeRock	US	
Illumio	US	
LogRhythm	US	
Lookout	US	
Netskope	US	
OneTrust	US	
Socure	US	
Snyk	UK	
Tanium	US	
Veracode	US	

Source: GlobalData

Sector Scorecard

At GlobalData, we use a scorecard approach to predict tomorrow's leading companies within each sector. Our sector scorecards have three screens: a thematic screen, a valuation screen, and a risk screen.

Cybersecurity is a theme that impacts many of the sectors we cover. In this section, we focus specifically on the enterprise security software sector.

For a full explanation of thematic scoring, please refer to the methodology section at the back of this report.

Enterprise security software scorecard

Who's who

Who does what in the enterprise security software space?

Enterprise security software
(46 companies)

Company	Ticker	Sector	MKT CAP (US$M)	Country	Description
Akam					
Zscale					

Source: GlobalData

Thematic screen

Our thematic screen ranks companies based on overall leadership in the 10 themes that matter most to their industry, generating a leading indicator of future performance

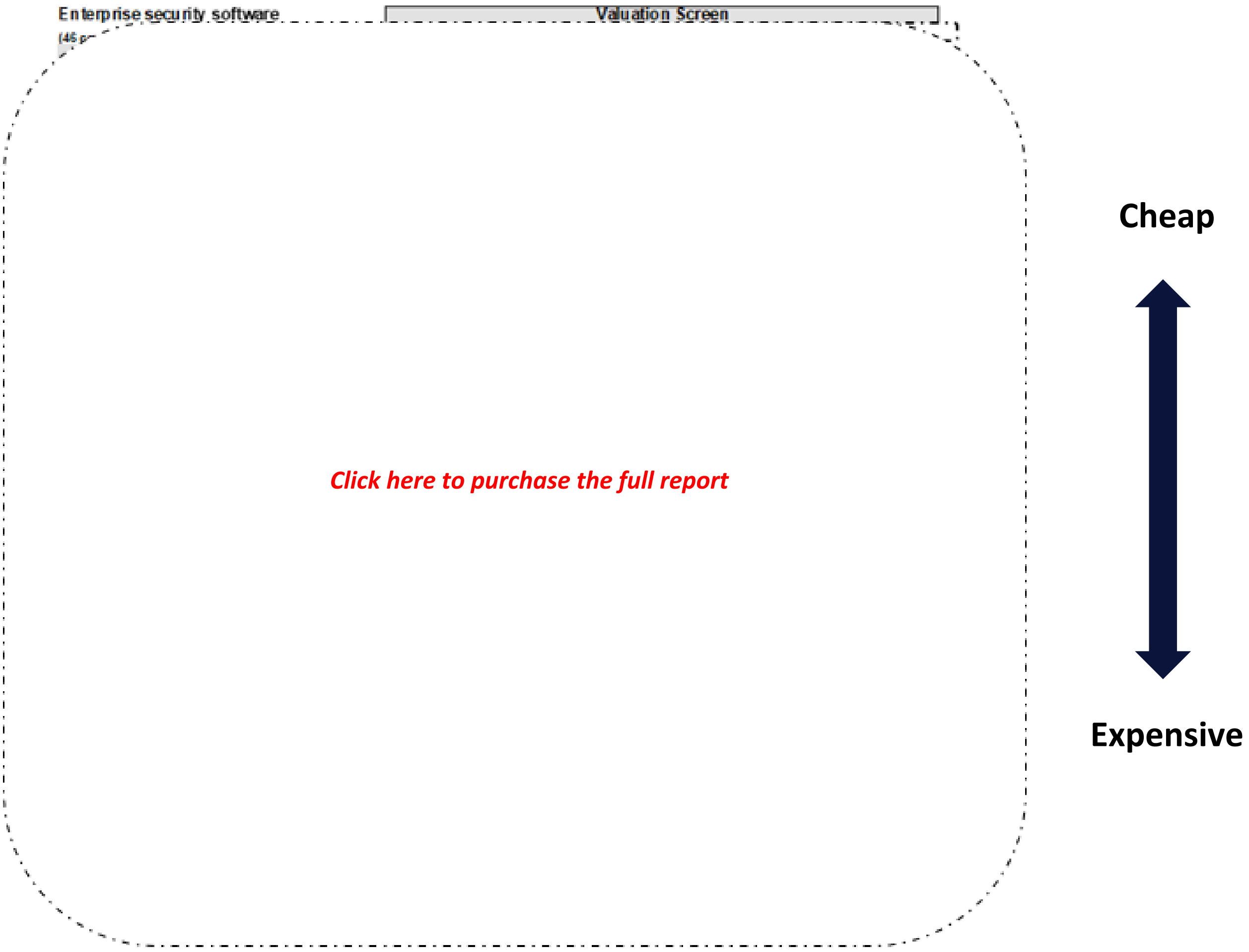
Enterprise security software
Thematic Screen
Click here to purchase the full report
Thematic leader
Thematic laggard

Key: 1 (red) implies this theme will have a negative impact on earnings over the next 12 months; 3 (amber) implies a neutral impact; and 5 (green) a positive impact. See the methodology section at the back of this report for an explanation of our research methodology.

Source: GlobalData

Valuation screen

Our valuation screen ranks our universe of companies within a sector based on selected valuation metrics


Enterprise security software
(46 p
Valuation Screen
Cheap
Expensive

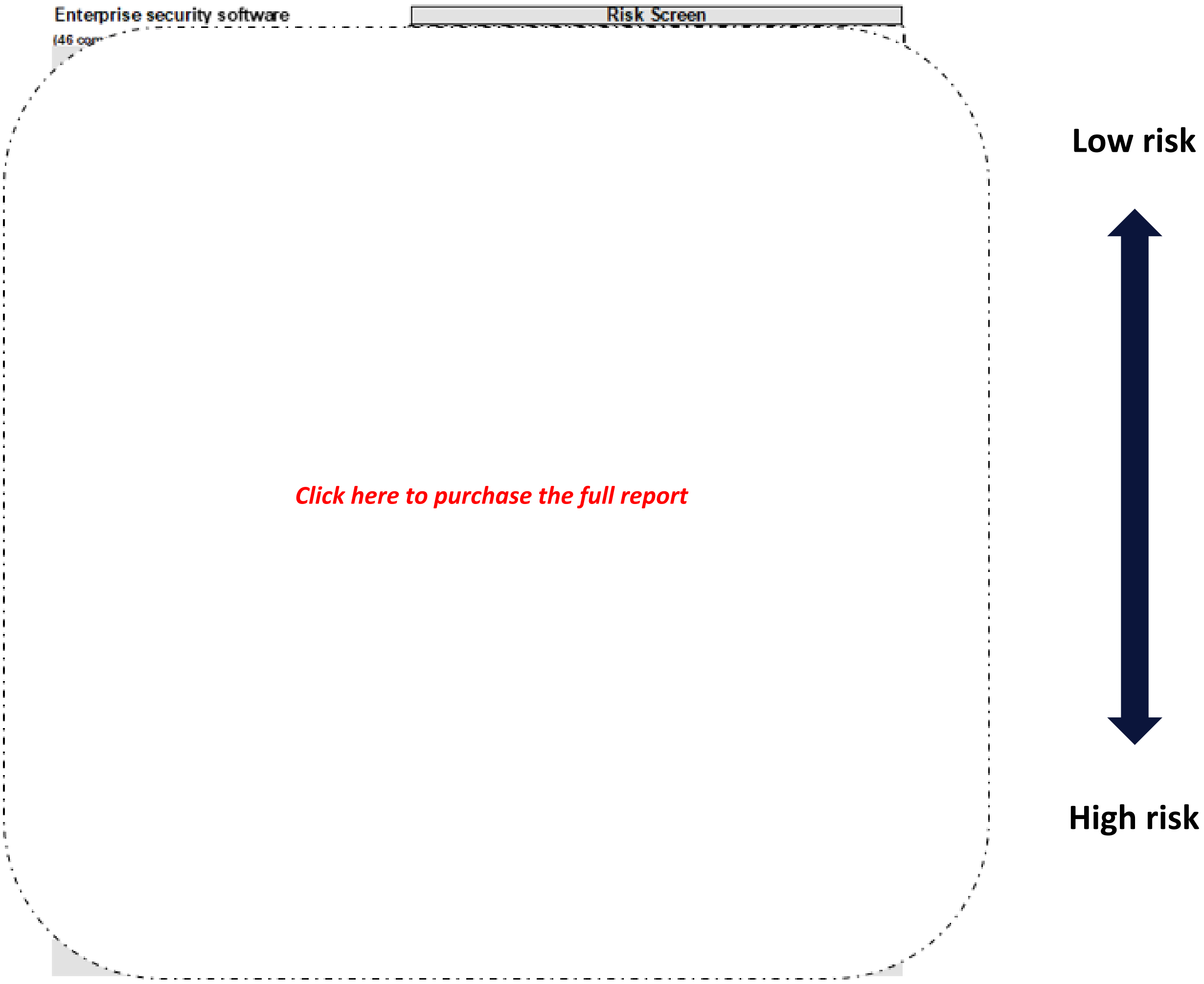
Click here to purchase the full report

Key: Green denotes that the company is cheap (15% more attractively priced than the median value for the sector) relative to its global peers; amber denotes it is within 15% of the sector median value; and red denotes that it is expensive relative to its global peers. Private companies are shown at the bottom of these rankings by default because they do not have a publicly listed market price. See the methodology section at the back of this report for an explanation of our research methodology.

Source: GlobalData

Risk screen

Our risk screen ranks companies within a particular sector based on overall investment risk



Click here to purchase the full report

Key: Green denotes low risk; amber denotes medium risk; red denotes high risk. See the methodology section at the back of this report for an explanation of our research methodology.

Source: GlobalData

Glossary

Term	Definition
5G	5G refers to the fifth generation of cellular technology standards that will be based on IMT2020 standards, under development by the 3GPP. The term ‘5G’ does not explicitly refer to any particular technology or standard and is, therefore, a loose term that can be used and interpreted in multiple different ways, typically for marketing purposes.
Adaptive authentication and authorization	An access method, also called risk-based authentication, which attempts to match the required user credentials to the perceived risk of the authorizations requested.
Advanced persistent threat	A sophisticated, systematic cyberattack program that continues for an extended period of time, often orchestrated by a group of skilled hackers
Antivirus	Software designed to identify and remove computer viruses or other malware on an organization’s devices or IT systems.
Application programming interface (API)	A set of defined methods of communication between programs so that information can be exchanged without the need to access the core of either program.
Artificial intelligence (AI)	Refers to software-based systems that use data inputs to make decisions on their own.
Attack surface	The totality of different points where hackers could enter or extract data from an environment. Applies to software, networks, and humans, and represents the sum of an organization’s security risk exposure.
Authentication	Process in which a user’s credentials are compared to what is listed in a database of authorized users’ information. Two-factor authentication involves signing in with known login information plus a second “factor,” such as a physical token.
Biometrics	The measurement and analysis of physical or behavioral characteristics as a means of verifying personal identity.
Botnet	A robot network of private computers infected with malicious software and controlled as a group without the owner’s knowledge
Chief information security officer (CISO)	The role of the CISO is to protect a company’s assets (both physical and digital) from cyberattacks.
Cloud access security broker	On-premise or cloud-based software that sits between cloud service users and cloud applications to monitor all activity and enforce security policies
Cloud computing	Computing delivered as an online service. It encompasses the provision of IT infrastructure, operating software, middleware, and applications hosted within a data center and accessed by the end-user via the internet.
Cyberattack	Cyberattacks are unwelcome attempts to steal, expose, alter, disable, or destroy information through unauthorized access to computer systems.
Cybercrime	Any crime that involves a computer and a network.

Term	Definition
Cybersecurity	The practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.
DevSecOps	DevSecOps is the philosophy of integrating security practices within the DevOps process. It involves creating a 'security as code' culture with ongoing, flexible collaboration between release engineers and security teams.
Distributed-denial-of service (DDOS)	A coordinated attack in which multiple connected machines in a botnet, usually infected with malware or otherwise compromised to co-opt them into the attack, flood a network, server, or website with so much data as to make it unusable.
Encryption	A method for scrambling a message, file, or other data and turning it into a secret code. The code can only be read using a 'key' or other piece of information (such as a long string of numbers), usually created with an algorithm
Edge computing	Refers to a network architecture concept that enables cloud computing capabilities and an IT service environment at the edge of the network. By running applications and performing processing tasks closer to the customer, edge computing delivers superior performance with reduced latency.
Endpoint	An internet-capable computer hardware device on a TCP/IP network. Typically includes desktop computers, laptops, smartphones, tablets, thin clients, printers, or other specialized hardware such as POS terminals and smart meters.
Endpoint security	A method for protecting the corporate network when accessed via remote devices such as laptops or other wireless and mobile devices. Each device with a remote connection to the network creates a potential entry point for security threats.
Extended detection and response (XDR)	A security technology that collects threat data from previously siloed security tools across an organization's technology stack for easier and faster investigation, threat hunting, and response.
Firewall	A security system that blocks unauthorized access to a network. Firewalls typically monitor and control traffic between an internal network (trusted to be secure) and an external network (not trusted).
Generative AI	Self-learning algorithms that use existing data, such as text, audio, or images, to produce realistic new content.
General Data Protection Regulation (GDPR)	A regulation that came into force across the EU in May 2018, giving consumers certain rights and protections over the data that organizations hold on them, including the right to data portability.
Hacker	A person who uses computers to gain unauthorized access to data.
Hacktivism	Computer or internet hacking activities motivated by social or political causes.
Identity management	A method to identify individuals or machines in an IT system and control their access to resources within that system by associating user rights and restrictions with each established identity.

Term	Definition
Incident response	An organization's structure for managing, mitigating, and resolving cybersecurity events, such as breaches.
Industrial control system (ICS)	Systems and associated instrumentation, including devices, systems, networks, and controls, used to operate or automate industrial processes.
Internet of Things (IoT)	An umbrella term used to describe the use of connected sensors and actuators to control and monitor the environment, the things that move within it, and the people that act within it.
Machine learning	An application of AI that gives computer systems the ability to learn and improve from data without being explicitly programmed.
Managed security services	Network security or cybersecurity monitoring services outsourced to a service provider. Services may include virus and spam blocking, intrusion detection, firewalls, and virtual private network (VPN) management.
Multi-factor authentication	Sometimes referred to as two-factor authentication or 2FA, multi-factor authentication is a security enhancement that allows someone to present two pieces of evidence (their credential) when logging in to their account.
Natural language processing (NLP)	A field of AI concerned with enabling computers to analyze, understand, and derive meaning from human language (both text and speech).
Network security	The process of using specialized hardware and software to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users, programs, and tools.
Open Web Application Security Project (OWASP)	A nonprofit foundation that works to improve the security of software, mainly through community-led open-source software projects.
Password management	The process of securing and managing passwords throughout their life cycle from creation to closure by adhering to a set of sustainable practices.
Phishing	A practice in which an attacker pretends to be a trusted entity by using fake emails and websites to steal sensitive data such as passwords or credit card details.
Privileged access management	Cybersecurity strategies and technologies used to exert control over privileged access and permissions for users, accounts, processes, and systems.
Ransomware	A type of malware that prevents access to the target's computer system or data until a ransom is paid to the attacker. Often uses encryption to lock up files or IT systems, holding them hostage until money is paid for a decryption key
Remediation	What an organization does to limit or stop an attack once it is detected, as part of incident response. Includes things like blocking IP addresses, removing infected files or devices, and restoring affected systems to a known good state.
Scanning	The process of attacking wide swathes of the internet at random.

Term	Definition
SD-WAN	An extension of the principle behind software-defined networking (SDN) to encompass the provision and management of wide area networks.
Secure access service edge (SASE)	An enterprise networking category that converges SD-WAN and network security point solutions into a unified, cloud-native service.
Secure boot	A security standard developed by members of the PC industry to help ensure that a device starts up using only software that the manufacturer trusts.
Security information and event management (SIEM)	The combined process of incident detection and incident response. Includes features such as alerts, analytics, dashboards, and forensic analysis.
Security orchestration, automation, and response (SOAR)	Refers to a collection of software solutions and tools that allow organizations to streamline security operations in three key areas: threat and vulnerability management, incident response, and security operations automation.
Smart city	A city that uses connected sensors to enhance the quality and performance of urban services such as energy, transport, and utilities to make the city function more efficiently.
Software as a service (SaaS)	SaaS is IaaS plus PaaS and the application that runs on them. The software is usually invoiced on a per-user subscription basis or on a transactional basis. SaaS allows users to access applications over the internet that are managed by a third-party vendor without having to download the software locally (e.g., Salesforce).
Software bill of materials	Effective software bill of materials (SBOM) management uses the identification of software components to mitigate cyber risk and support improved cybersecurity throughout the software's lifecycle.
Spear phishing	Sending emails to targeted individuals that could contain an attachment with malicious software or a link that downloads malicious software.
Supervisory control and data acquisition (SCADA)	A system comprised of software and hardware used to control and monitor a process or application. A typical application for SCADA would be monitoring or controlling an industrial process, or collecting, processing, and analyzing real-time data.
Supply chain attack	An attack in which threat actors compromise enterprise networks using connected applications or services owned or used by outside partners, such as suppliers.
Threat actor	A group or person behind a malicious incident.
Threat detection	Methods for identifying system vulnerabilities and hacking behaviors. Can include any number of technologies, including ML, statistical modeling, and network traffic monitoring.
Threat intelligence	Refers to data collected and analyzed by an organization to understand a cyber threat's motives and attack behaviors.
Unified threat management	A cybersecurity solution that combines multiple security functions—network firewalling, intrusion detection and prevention, anti-virus, anti-spam, content filtering, leak prevention, etc.—within a single security system.

Term	Definition
Virtual private network (VPN)	A private network (e.g., a corporate network) that extends across a public network (e.g., the internet). VPNs are used to allow secure remote access to documents across unsecured public networks.
Virus	A type of malware that, when executed, copies itself and infects other computer programs by modifying them.
Vulnerability	A weakness that allows an attacker to compromise an application, device, or network.
Water-holing	Setting up a fake website or compromising a legitimate one to exploit visiting users.
Worm	A type of malware that is standalone (unlike a virus, which is attached to another program) and spreads to other machines by replicating itself. Worms are capable of highly targeted attacks, such as the Stuxnet worm allegedly used to disrupt Iran's nuclear program in 2009–10.
Zero-day attack	A hack that exploits a vulnerability in software that is unknown to the security vendor at the time of exploit. The security vendor, therefore, has "zero days" to fix it.
Zero trust	A security model that uses strict identity verification for every person or entity attempting to access an organization's network resources, regardless of whether the person or entity is in the office, bound by the network perimeter, or accessing the network remotely.
Zero-trust network access (ZTNA)	The strategy behind achieving an effective zero trust model, ZTNA is a set of technologies and functionalities that enable secure access to internal applications for remote users.

Source: GlobalData

Further Reading

GlobalData reports

Publication date	Report title
March 2024	Thematic Intelligence: Digital Twins
March 2024	Thematic Intelligence: Global TMT M&A Deals 2023 - Top Themes and Predictions
February 2024	Thematic Intelligence: Blockchain
February 2024	Thematic Intelligence: Cloud Computing
February 2024	Thematic Intelligence: Quantum Computing
January 2024	Thematic Intelligence: Tech Sentiment Polls Q4 2023
December 2023	Thematic Intelligence: Tech, Media, & Telecom Themes 2024
December 2023	Thematic Intelligence: Tech, Media, & Telecom Predictions 2024
November 2023	Thematic Intelligence: Internet of Things
October 2023	Thematic Intelligence: Enterprise Security Software Sector Scorecard Q3 2023 Update
October 2023	Thematic Intelligence: Artificial Intelligence – Executive Briefing (Second Edition)
September 2023	Thematic Intelligence: The Space Economy
August 2023	Thematic Intelligence: Tech Regulation
August 2023	Thematic Intelligence: Data Analytics
March 2023	Thematic Intelligence: Cybersecurity (2023)
March 2023	Thematic Intelligence: 3D Printing
February 2023	Thematic Intelligence: Artificial Intelligence
December 2022	Thematic Intelligence: Digital Identity

Source: GlobalData

Our Thematic Research Methodology

Companies that invest in the right themes become success stories. Those that miss the important themes in their industry end up as failures.

Viewing the world's data by themes makes it easier to make important decisions

We define a theme as any issue that keeps a senior executive awake at night. GlobalData's thematic ecosystem is a single, integrated global research platform that provides an easy-to-use framework for tracking all themes across all companies in all sectors. It has a proven track record of identifying critical themes early, enabling companies to make the right investments ahead of the competition and secure that all-important competitive advantage.

Traditional research does a poor job of picking winners and losers

The difficulty in picking tomorrow's winners and losers in any industry arises from the sheer number of technology cycles—and other themes—that are in full swing right now. Companies are impacted by multiple themes that frequently conflict with one another. What is needed is an effective methodology that reflects, understands, and reconciles these conflicts.

That is why we developed our thematic engine

At GlobalData, we have developed a unique thematic methodology for ranking all major companies in all major sectors based on their relative strength in the big themes that are impacting their industries.

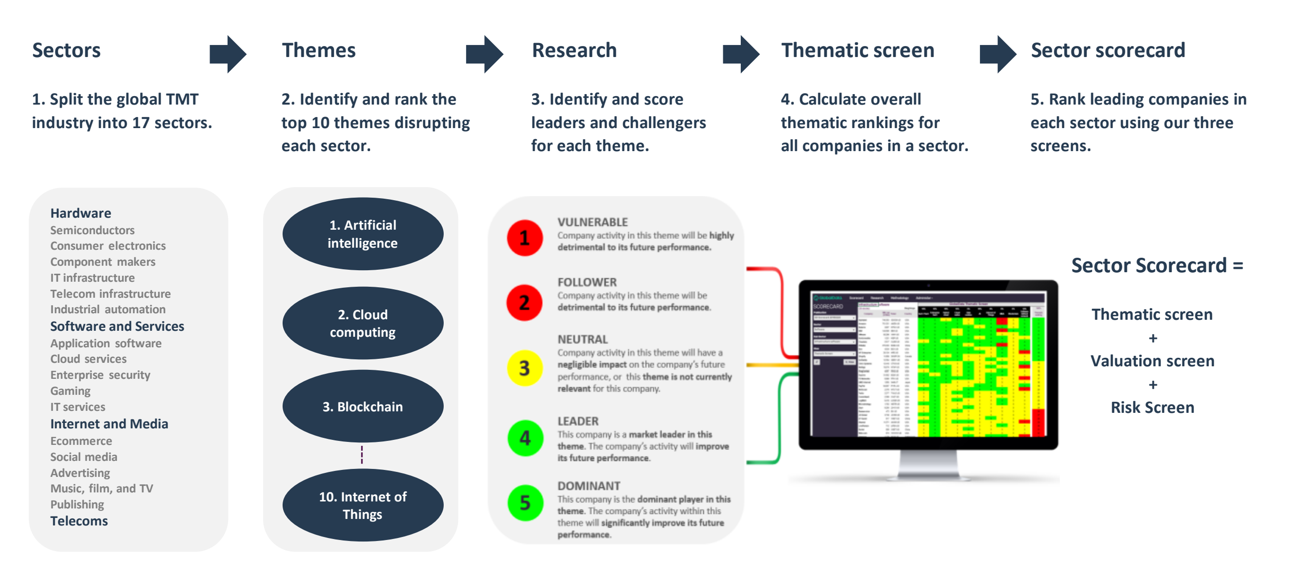
Our thematic engine tags over 180 million data items across five alternative data sets—patents, jobs, deals, filings, social media, and news—to themes. The vast datasets within our thematic engine help our analysts to produce sector scorecards that identify the companies best placed to succeed in a future filled with multiple disruptive threats.

How do we create our sector scorecards?

First, we split each industry into sectors because a different set of themes drives each sector. Taking the TMT (technology, media, and telecom) industry as an example, we split this industry into the sectors shown in the graphic below.

Our five-step approach for generating a sector scorecard

Here we use tech, media, and telecom as an example sector for illustration purposes



Sectors

1. Split the global TMT industry into 17 sectors.

Hardware
Semiconductors
Consumer electronics
Component makers
IT infrastructure
Telecom infrastructure
Industrial automation
Software and Services
Application software
Cloud services
Enterprise security
Gaming
IT services
Internet and Media
Ecommerce
Social media
Advertising
Music, film, and TV
Publishing
Telecoms

Themes

2. Identify and rank the top 10 themes disrupting each sector.

1. Artificial intelligence
2. Cloud computing
3. Blockchain
10. Internet of Things

Research

3. Identify and score leaders and challengers for each theme.

1 VULNERABLE
Company activity in this theme will be **highly detrimental to its future performance.**

2 FOLLOWER
Company activity in this theme will be **detrimental to its future performance**.

3 NEUTRAL
Company activity in this theme will have a **negligible impact** on the company's future performance, or this **theme is not currently relevant** for this company.

4 LEADER
This company is a **market leader in this theme**. The company's activity will **improve its future performance.**

5 DOMINANT
This company is the **dominant player in this theme**. The company's activity within this theme will **significantly improve its future performance**.

Thematic screen

4. Calculate overall thematic rankings for all companies in a sector.

Sector scorecard

5. Rank leading companies in each sector using our three screens.

Sector Scorecard =

Thematic screen
+
Valuation screen
+
Risk Screen

Source: GlobalData

Second, we identify and rank the top 10 themes for each sector (these can be technology themes, macroeconomic themes, or industry-specific themes). Third, we publish in-depth research on specific themes, identifying the winners and losers within each theme. The problem is that companies are exposed to multiple investment themes, and specific themes' relative importance can fluctuate. So, our fourth step is to create a thematic screen for each sector to calculate overall thematic leadership rankings after taking account of all themes impacting that sector. Finally, to give a crystal-clear picture, we combine this thematic screen with our valuation and risk screens to generate a sector scorecard used to help assess overall winners and losers.

What is in our sector scorecards?

Our sector scorecards help us determine which companies are best positioned for a future filled with disruptive threats. Each sector scorecard has three screens:

- **The thematic screen** tells us who are the overall leaders in the 10 themes that matter most, based on our thematic engine.
- **The valuation screen** tells us whether publicly listed players appear cheap or expensive relative to their peers based on consensus forecasts from investment analysts.
- **The risk screen** tells us who the riskiest players in each industry are, based on our assessment of four risk categories: operational risk, financial risk, industry risk, and country risk.

How do we score companies in our thematic screen?

Our thematic screen ranks companies within a sector based on overall leadership in the 10 themes that matter most to their industry, generating a leading indicator of future earnings growth.

Thematic scores predict the future, not the past. Our thematic scores are based on our analysts' assessment of their competitive position in relation to a theme, on a scale of 1 to 5:

1	**Vulnerable**	The company's activity in this theme will be highly detrimental to its future performance.
2	**Follower**	The company's activity in this theme will be detrimental to its future performance.
3	**Neutral**	The company's activity in this theme will have a negligible impact on the company's future performance, or this theme is not currently relevant for this company.
4	**Leader**	The company is a market leader in this theme. The company's activity in this theme will improve its future performance.
5	**Dominant**	The company is a dominant player in this theme. The company's activity in this theme will significantly improve its future performance.

How do our research reports fit into our overall thematic research ecosystem?

Our thematic research ecosystem is designed to assess the impact of all major themes on the leading companies in a sector. To do this, we produce three tiers of thematic reports:

- **Single theme**: These reports offer in-depth research into a specific theme (e.g., artificial intelligence). They identify winners and losers based on thematic leadership, market position, and other factors.
- **Multi-theme**: These reports cover all themes impacting a sector and the implications for the key players in that sector.
- **Sector scorecard**: These reports identify those companies most likely to succeed in a world filled with disruptive threats. They incorporate our thematic screen to show how conflicting themes interact with one another, as well as our valuation and risk screens.

About GlobalData

GlobalData is a leading provider of data, analytics, and insights on the world's largest industries. In an increasingly fast-moving, complex, and uncertain world, it has never been harder for organizations and decision makers to predict and navigate the future. This is why GlobalData’s mission is to help our clients to decode the future and profit from faster, more informed decisions. As a leading information services company, thousands of clients rely on GlobalData for trusted, timely, and actionable intelligence. Our solutions are designed to provide a daily edge to professionals within corporations, financial institutions, professional services, and government agencies.

Unique Data

We continuously update and enrich 50+ terabytes of unique data to provide an unbiased, authoritative view of the sectors, markets, and companies offering growth opportunities across the world's largest industries.

Expert Analysis

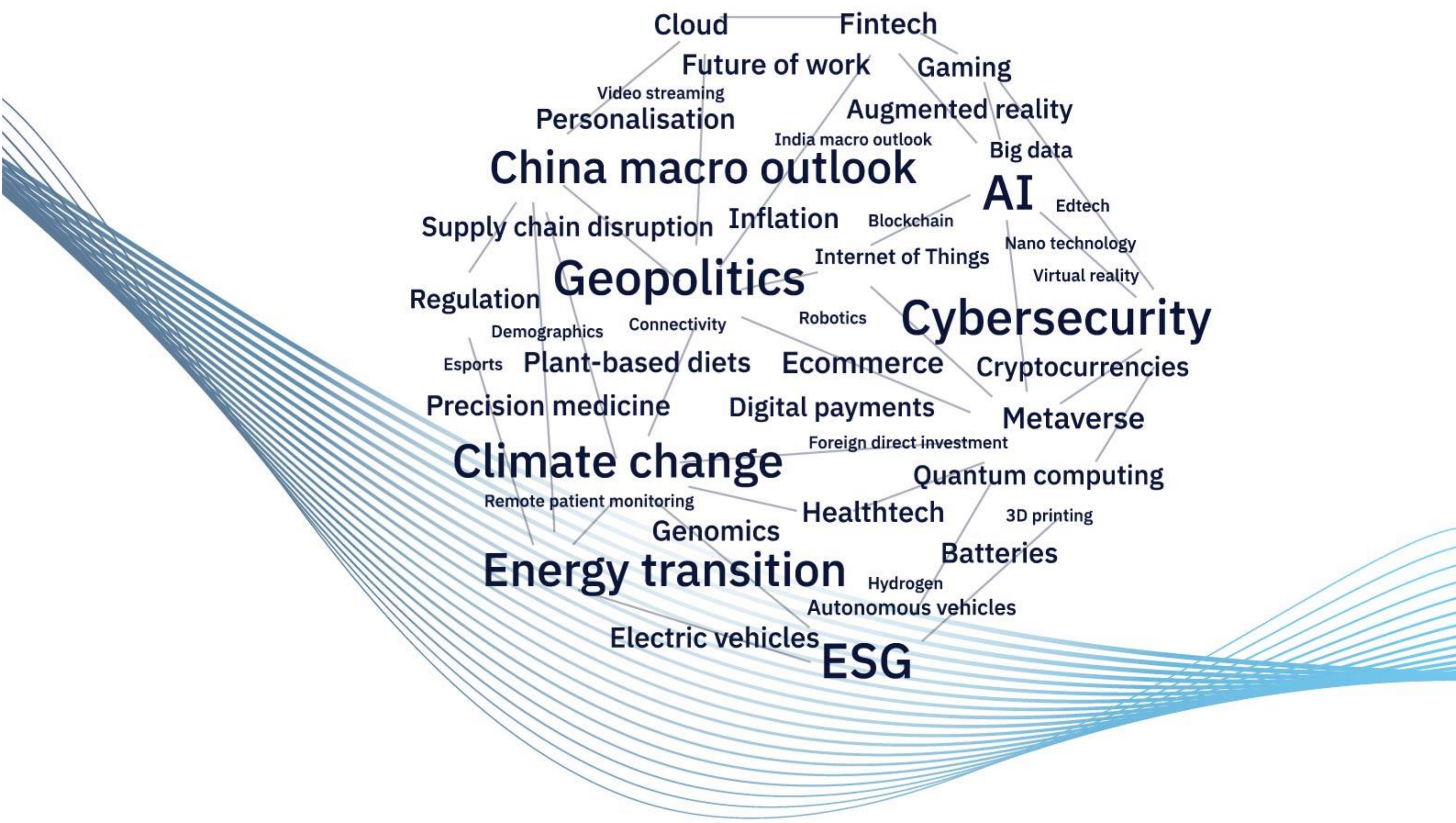
We leverage the collective expertise of over 2,000 in-house industry analysts, data scientists, and journalists, as well as a global community of industry professionals, to provide decision-makers with timely, actionable insight.

Innovative Solutions

We help you work smarter and faster by giving you access to powerful analytics and customizable workflow tools tailored to your role, alongside direct access to our expert community of analysts.

One Platform

We have a single taxonomy across all our data assets and integrate our capabilities into a single platform – giving you easy access to a complete, dynamic, and comparable view of the world’s largest industries.



Contact Us

If you have any more questions regarding our research, please contact us:

Head of Thematic Intelligence
Cyrus Mewawalla
cyrus.mewawalla@globaldata.com
+44 (0) 207 936 6522

Customer Success Team
Understand how to use our Themes product
customersuccess.thematic@globaldata.com
+44 (0) 207 406 6764

Disclaimer: © GlobalData Plc. All Rights Reserved.

This information has been extracted from GlobalData's Intelligence Center by a registered user. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the publisher, GlobalData.

The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions, and recommendations that GlobalData delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such GlobalData can accept no liability whatsoever for actions taken based on any information that may subsequently prove to be incorrect. GlobalData is not authorized or permitted to provide regulated investment advice. Any data or analysis provided by GlobalData, either verbally or in writing, should not be considered as regulated investment advice.