A technology landscape analysis of cybersecurity

2026 Edition

About metis analytica

metis analytica is a small consulting firm specializing in data-driven innovation management for businesses, governments, and research institutions. Our services include:

Competitive Intelligence: Our expertise lies in patent analytics, particularly through statistical patent analysis. This approach aids clients in shaping their innovation strategies, formulating innovation policies, making informed investment decisions, and evaluating M&A opportunities. Additionally, it facilitates the search for R&D partnerships and helps anticipate market shifts. By providing valuable insights, we enable clients to refine their innovation strategies and optimize their investments, ultimately leading to more effective resource allocation.

Capacity Building: We offer workshops and initiatives that integrate advanced tools like machine learning, natural language processing, and social network analysis into decision-making processes. This enhances clients' teams' capabilities, empowering them to make informed, data-driven decisions that drive innovation. Additionally, we provide IP management and strategy courses to equip clients with the knowledge and skills needed to effectively manage their intellectual property assets.

Customized Analytics: We develop interactive dashboards to track the success of innovation initiatives, allowing clients to monitor multi-parameter ecosystems. This enables clients to adjust their strategies based on comprehensive data insights, maximizing the impact of their innovation efforts.

A technology landscape analysis of cybersecurity © 2026 by Altay Özaygen is licensed under CC BY 4.0. To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

Executive Summary

This report maps the cybersecurity technology landscape using USPTO granted patent data and IPC-based analysis. Its purpose is to identify the most active actors, the dominant and emerging technology domains, and the patent-based signals that can reliably inform strategic decisions related to R&D positioning, partnerships, and M&A screening. The analysis is deliberately iterative and reproducible, combining statistical indicators, network metrics, and semantic structure.

Approach

- Data: USPTO granted patents, analyzed on a publication-year basis.
- Methods: statistical patent analysis, citation-network analysis, and semantic clustering.
- Process: iterative refinement of search scope and results to ensure robustness and repeatability.

Key findings

- Scope: 2,556 granted patents analyzed (through 2025). The technological core of the dataset is concentrated in IPC classes G06F 21 (computer and data security) and H04L 9 (secure communications and network protocols).
- Applicant landscape (G06F 21 / H04L 9): IBM is the leading corporate applicant and the remaining top applicants are largely established incumbents.
- Pure-play dynamics: specialized cybersecurity vendors (e.g. *FireEye, Wiz*) exhibit focused IPC profiles. *Wiz* shows a pronounced surge in patent publications after 2023, consistent with rapid scaling in cloud-security technologies.
- Internal R&D signal: Individual patents are both numerous and more diversified across IPC subclasses than most corporate portfolios, pointing to broad, retained R&D activity rather than narrow defensive patenting.
- Network centrality: *Bank of America* has the highest betweenness centrality in the citation network, acting as a structural bridge across technology clusters. Other highly central actors are predominantly large engineering and systems firms, with consultancies (e.g. *Accenture*) also occupying influential positions.
- Geography (EP filings): European cybersecurity patenting is highly concentrated. Île-de-France is the leading hub, followed by major German regions (Bayern, Baden-Württemberg) and selected northern European clusters.
- Thematic structure: semantic clustering identifies five coherent technology themes, ranging from core network and cloud security to more specialized domains such as quantum-secure communications and transportation system monitoring.

Interpretation notes

- Keyword scope matters: cybersecurity-specific keyword searches favor domain-focused players and may underrepresent diversified IT firms whose cybersecurity inventions form a small share of broader portfolios.
- Deterministic signals: the combined use of patent counts, citation-network metrics, and semantic clustering produces stable, reproducible indicators suitable for comparative and longitudinal analysis.
- Iterativeness: reliable landscape insights require repeated refinement of search criteria and validation by domain experts to balance recall and precision.

Recommendations and next steps

This analysis provides an initial but structured view of the cybersecurity technology landscape. Further work should be guided by explicit strategic objectives and conducted iteratively with domain experts.

1. Define the focal firm or stakeholder, then apply combined patent-based signals (technological diversity, similarity, complementarity, individual filing behavior, and citation metrics) to shortlist candidates for R&D partnerships or M&A screening.
2. For a given acquirer, benchmark competitors and potential targets to assess strategic fit, overlap, and complementarity under alternative acquisition or collaboration scenarios.
3. Deepen analysis within priority technology clusters by increasing clustering granularity, refining keywords and IPC/CPC filters, and validating cluster interpretations with subject-matter experts.
4. Extend coverage to additional patent offices (EPO, CNIPA, KIPO, JPO) where jurisdictional exposure, regulatory considerations, or market access are strategically relevant.

Contents

1 Introduction

Cybersecurity has become a strategic priority across industries as digitalization, cloud adoption, and interconnected systems continue to expand the attack surface. The economic impact of cybercrime has reached unprecedented levels, with global annual costs projected to reach $9.5 trillion in 2024 and $10.5 trillion by 2025, reflecting both the growing volume and the increasing severity of attacks (Morgan, 2023). High-profile incidents affecting critical infrastructure, financial systems, and large enterprises underscore that cybersecurity is no longer solely a technical concern, but a material business, economic, and societal risk (Ali & Santos, 2015; Dieye et al., 2020).

Empirical evidence further highlights the strategic relevance of cyber risk. Cyber incidents have been shown to generate negative abnormal returns for affected firms, particularly those that are highly visible, hold significant intangible assets, or exhibit weak board- level attention to cybersecurity governance (Kamiya et al., 2018; Kammoun et al., 2019). These dynamics reinforce the need for firms and policymakers to anticipate technological change in cybersecurity rather than respond reactively.

As in last year's edition, this report demonstrates how patent data can be used strategically to support technology intelligence. The analysis is produced using *TechLand*, the technology landscape platform developed by metis analytica.

In parallel, cybersecurity investment and innovation continue to accelerate. Industry and policy reports point to rapid growth in cybersecurity capabilities and spending, driven by regulatory pressure, technological complexity, and rising interdependencies across digital ecosystems (Aiyer et al., 2022; Bueermann & Rohrs, 2024). The World Economic Forum (2026) emphasizes that the pace of technological change, combined with persistent structural vulnerabilities, positions cyber risk as a long-term strategic challenge requiring coordinated and forward-looking responses. In this environment, patents provide a systematic and comparable signal of where firms allocate R&D resources, which technologies dominate, and how innovation trajectories evolve.

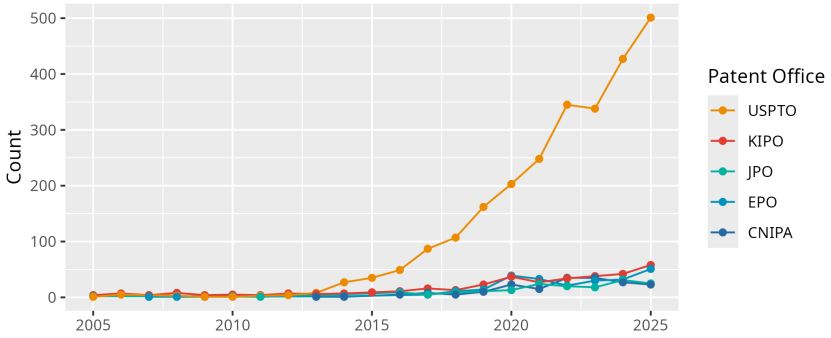


Figure 1: Yearly granted patent counts across major patent offices.

Patent activity in cybersecurity reflects this sustained innovation dynamic. Figure 1 shows the evolution of first-publication counts of granted cybersecurity patents across the five largest patent offices. The upward trend over time is consistent with increasing technological effort and formalization of intellectual property in response to growing cyber threats.

This report presents a technology landscape analysis of cybersecurity grounded primarily in USPTO-granted patents, using publication year as the temporal reference. While cybersecurity

innovation is global, the USPTO offers the most comprehensive and consistent coverage of granted patents in this domain, making it a suitable anchor for landscape-level analysis. Selected complementary views, including European filings, are introduced where they add geographic or structural insight.

Technology landscape analysis is widely used in competitive intelligence to map innovation systems and strategic positioning. By combining patent statistics, citation-network analysis, and clustering methods, such analyses reveal dominant technologies, key actors, emerging subfields, and potential competitive threats or opportunities (Jaffe & Trajtenberg, 2005; Kang & Tarasconi, 2016; Lerner & Seru, 2022; Nagaoka et al., 2010). Citation networks trace technological trajectories and knowledge flows, while clustering and portfolio comparisons support strategic decisions related to R&D collaboration, market entry, and merger and acquisition targeting (Aharonson & Schilling, 2016; Srivastava & Jain, 2024; Verspagen, 2007; Yang et al., 2010).

Patent-based analysis has well-known limitations. In cybersecurity, particularly for offensive techniques or sensitive operational capabilities, firms may avoid patenting to limit disclosure. As a result, patent data tends to reflect the activity of larger, more visible organizations and may underrepresent smaller or more secretive innovators. Similar constraints apply in other domains where secrecy or speed to market outweigh formal intellectual property protection (Lerner & Seru, 2022; Nagaoka et al., 2010).

The objective of this study is to deliver a structured, reproducible, and decision-oriented view of the cybersecurity technology landscape. Unlike prior work that emphasizes technological fields or individual inventions (Daim et al., 2024), this report uses the patent applicant—primarily enterprises—as the main unit of analysis. We combine citation-network analysis and semantic clustering with iterative refinement of keywords and applicant names. Beyond standard portfolio metrics, we flag cases where applicant names include inventor names as an additional signal of internal R&D intensity, proprietary retention, or collaborative/consulting arrangements that affect strategic interpretation.

The remainder of the report is organized as follows. The next section describes the data and methodology. This is followed by the results and discussion, which interpret the findings from statistical, network, and clustering perspectives. The report concludes with implications for strategy and recommendations for further analysis.

2 Methodology

This section describes the data sources, search strategy, and analytical methods used to construct the cybersecurity technology landscape. The methodological choices are designed to balance analytical rigor, reproducibility, and strategic relevance.

2.1 Data collection

The patent dataset was constructed through a keyword-based search of patent titles and abstracts, followed by iterative refinement and filtering within TechLand.

Search strategy

- **Search keywords:** Each record must contain the token "cyber" together with at least one of the following terms: attack, crime, defense, incident, intelligence, monitoring, protection, response, risk, security, threat, or warfare. Additional explicit keywords include "cybersecurity", "cyberattack", and "cyberdefense".
- **Filters applied:**
  - Patent office: USPTO (primary focus)
  - Patent type: First publication of granted patent applications
  - Intellectual property right type: Patents of invention
  - Time window: Publications up to and including 2025

The search strategy was refined iteratively to balance recall and precision, ensuring coverage of core cybersecurity technologies while limiting irrelevant records.

2.2 Analytical framework

The analytical framework combines descriptive statistics, citation network analysis, and semantic clustering to capture complementary dimensions of technological development.

2.2.1 Statistical patent analysis

Statistical patent analysis is used to quantify innovation activity, identify leading applicants, and characterize technological focus areas. The analysis is restricted to the first publication of granted patent applications.

This restriction serves three purposes:

- **Uniqueness of inventions:** First publications represent distinct inventive outputs and avoid multiple counts of the same invention through subsequent publications or family members.

- **Robust citation linkage:** Citations are most consistently attributed to the original publication, supporting longitudinal analysis.
- **Legal validation:** Limiting the dataset to granted applications ensures that only legally validated inventions are considered.

The analysis concentrates on applicants with large patent portfolios. This focus reflects a deliberate emphasis on actors with sustained innovation capacity and structural influence on the cybersecurity technology landscape.

2.2.2 Citation network analysis

Citation network analysis (CNA) is employed to examine knowledge flows and influence structures within the patent system. Beyond citation counts, CNA identifies actors that occupy central or bridging positions in the diffusion of technological knowledge (Sharma & Tripathi, 2017).

The citation network is constructed using:

- **Backward citations:** Patents referenced by the focal patent set.
- **Forward citations:** Patents citing the focal set within three years after patent application.

The three-year forward citation window captures early technological impact while limiting noise from routine or procedurally motivated citations. For interpretability, patents are aggregated by assignee name, approximating firm-level knowledge exchanges.

2.2.3 Clustering

Semantic clustering is applied to uncover dominant technology themes within the patent corpus. TechLand implements a three-stage pipeline.

First, patent texts are converted into semantic embeddings and projected into a two-dimensional technology space, where spatial proximity indicates technological similarity. Second, the space is partitioned into coherent clusters and representative keywords are extracted for each cluster. Third, an AI enrichment layer assigns industry labels, IPC/CPC classifications, and concise summaries to support interpretation and the iterative refinement of the analysis.

By integrating semantic, spatial, and AI-driven analyses, the clustering approach yields interpretable technology groupings that support portfolio analysis, competitive positioning, and strategic opportunity identification.

3 Results and discussion

Figure 1 presents the evolution of first publications of granted cybersecurity patent applications across the five largest patent offices. Table 1 reports aggregate counts for the period 1996–2025.

Table 1: Granted patents counts for the publication period 1996-2025.

Patent Office	Application
USPTO	2,556
KIPO	392
EPO	241
CNIPA	188
JPO	170

Cybersecurity patenting is highly concentrated at the USPTO, with the United States clearly dominating and Israel emerging as the strongest non-US contributor. The applicant structure combines a small group of sustained innovators with a long tail of niche actors, indicating an open and competitive innovation landscape.

The USPTO accounts for the clear majority of granted cybersecurity patents. Given both scale and global market relevance, the USPTO serves as the primary analytical lens of this report. While a multi-office comparison would enrich jurisdictional insight, the USPTO dataset alone captures the dominant competitive dynamics in cybersecurity innovation.

The section proceeds in three parts: (1) statistical patent analysis, (2) citation network analysis, and (3) clustering. Each perspective offers a different, complementary angle on the cybersecurity technology landscape.

3.1 Statistical patent analysis

In total, 2,556 USPTO patents are analyzed. The earliest publication in the dataset dates to 1996, marking the early institutionalization of cybersecurity as a patentable domain. Note that throughout this report patent dates refer to publication year rather than filing year.

3.1.1 Patent counts by applicant countries

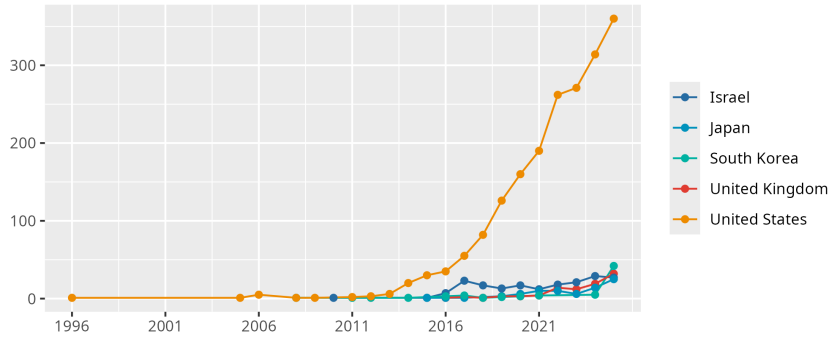


Figure 2: Yearly patent counts for top five applicant countries.

Figure 2 and Table 2 confirm the structural dominance of the United States, accounting for the overwhelming share of USPTO cybersecurity patents. Israel ranks a distant second but remains the strongest non-US contributor, reflecting its established cybersecurity ecosystem.

Table 2: Patent counts for top 10 applicant countries.

Applicants' country	count
United States	1925
Israel	186
United Kingdom	91
Japan	77
South Korea	68
Canada	64
Singapore	31
Germany	29
Saudi Arabia	29
France	27

3.1.2 The distribution of applicants by number of patents

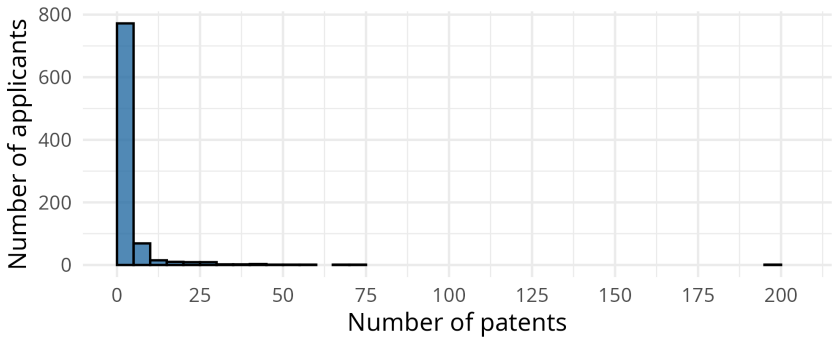


Figure 3: Distribution of published patents across applicants.

The applicant distribution in Figure 3 shows a pronounced long-tail: most applicants hold very small portfolios while a few entities account for much larger counts. In the dataset the 0–5 bin is by far the largest (772 applicants), and counts decline rapidly for larger bins (e.g., 69 in 5–10, 15 in 10–15, etc.), consistent with many small or one-off applicants and a small competitive core of sustained ones.

Note on the final bin (size = 200), this is a special aggregate, not an additional 195–200 bin. It reports the total number of patents that list individual persons in the applicant name field. Treat this value as a separate tally of individual-named applicants rather than as a bin. Its magnitude highlights that individual inventors and person+company co-applicants make a non-negligible contribution to the landscape.

Strategic interpretation:

- Core vs periphery: the pattern indicates a compact core of repeat filers (sustained R&D) and a broad periphery of niche or experimental actors.

- Individual applicant as a signal: the aggregated individual-name tally points to substantial activity occurring outside large, consolidated portfolios — a valuable source of early-stage technology, talent signals, and potential licensing or acquisition opportunities.
- Implication for analysis: to avoid double counting and to focus on unique inventive output, combine these counts with family-level deduplication and additional signals (citations, family size, assignment history) when prioritizing targets.

3.1.3 Patent grant delay

Figure 4 reports average grant delays for USPTO cybersecurity patents. Between 2014 and 2025, grant duration stabilizes between approximately 2.2 and 2.5 years.

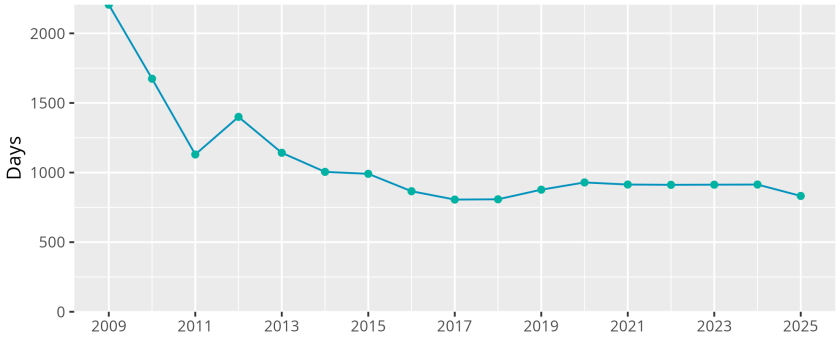


Figure 4: Average patent grant delay (days).

This plateau suggests that cybersecurity inventions are processed within a mature and predictable examination pipeline. For firms, this reduces regulatory uncertainty and supports forward planning around IP-based market entry or licensing.

3.1.4 IPC distribution

Table 3 indicates a strong concentration of cybersecurity patents in two IPC classes: G06F 21, covering security mechanisms for computing systems and data, and H04L 9, related to secure communications and network protocols. These classes capture the core technological domains of cybersecurity.

G06N 20 group indicates increasing integration of AI and machine learning into cybersecurity solutions.

The analysis follows an iterative refinement logic. Starting from a keyword-based USPTO search, we extract the IPC distribution and focus on the two dominant classes, G06F 21 and H04L 9. These classes are then used to retrieve related EPO patents so we can compare the top applicants in the USPTO corpus and map the spatial distribution of cybersecurity innovation across Europe.

Figure 5 represents the distribution of granted patents across various applicant names in the IPC groups G06F 21 and H04L 9, spanning the publication years from 2005 to 2025. The data represents a selection of major firms, each with a substantial presence in the patenting landscape. These firms, including industry giants such as IBM, Intel, and Microsoft, have been actively involved

Table 3: Top 10 IPC main class distribution of the published patents in cybersecurity.

IPC		Total
H04L 9	Arrangements for secret or secure communications; Network security protocols	1203
G06F 21	Security arrangements for protecting computers, components thereof, programs or data against unauthorised activity	1011
H04L 29	Arrangements, apparatus, circuits or systems, not covered by a single one of groups	1006
G06N 20	Machine learning	336
G06F 16	Information retrieval; Database structures therefor; File system structures therefor	321
H04L 12	Data switching networks	216
G06F 11	Error detection; Error correction; Monitoring	186
G06F 9	Arrangements for program control, e.g. control units	152
G04L 41	Arrangements for maintenance, administration or management of data switching networks, e.g. of packet switching networks	148
H04W 12	Security arrangements; Authentication; Protecting privacy or anonymity	136

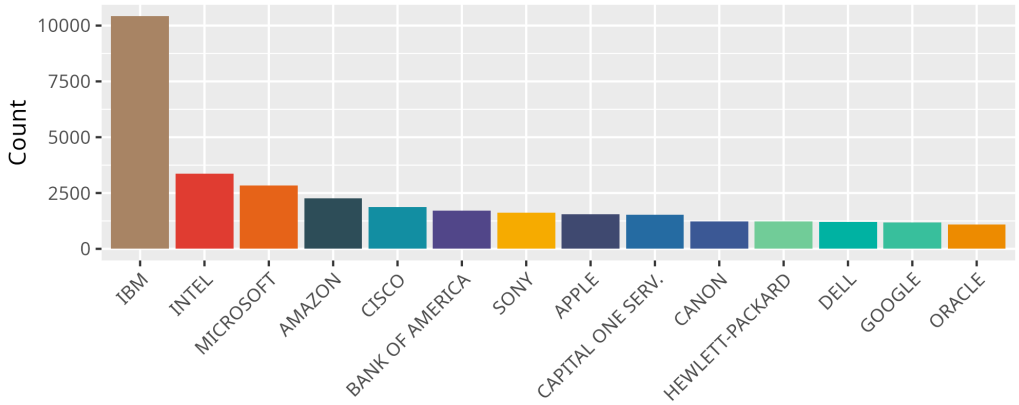


Figure 5: Distribution of granted patents in G06F 21 and H04L 9 across applicants for the period 2005-2025.

in technological advancements in areas covered by the specified IPC groups. The graph highlights the disparity in patent activity among these prominent applicants, with larger firms typically filing a higher number of patents. This reflects their significant investment in research and development, as well as their competitive position in the technology sector.

3.1.5 Applicants with high number of patents in cybersecurity

Applicants holding more than 20 granted patents form the strategic core of the landscape is given in Table 4. These actors represent sustained R&D investment rather than opportunistic filing.

Figure 6 shows a clear rise in cybersecurity patenting over time, with different strategies across applicants. WIZ INC stands out sharply in the most recent years, surging after 2023 and becoming the most prolific applicants by 2025. IBM shows steady activity through the late 2010s, peaking around 2021–2022 before declining. BANK OF AMERICA and DARKTRACE HOLDINGS exhibit

Table 4: Number of granted patents of key players (+ 20 patents) in cybersecurity.

Applicant	Total
Individual	190
WIZ INC	71
IBM	67
FIREEYE INC	59
BANK OF AMERICA	51
DARKTRACE HOLDINGS 46	
GENERAL ELECTRIC	41
HONEYWELL INT INC	41
MICROSOFT TECHNOLOGY LICENSING LLC	40
QOMPLX INC	34
RAPID7 INC	34
FIREEYE SECURITY HOLDINGS US LLC	29
BOEING CO	28
CENTRIPETAL NETWORKS LLC	28
DARKTRACE LTD	28
T MOBILE USA INC	
EXPEL INC	26
ARCHITECTURE TECHNOLOGY CORP	25
PROOFPOINT INC	25
RADWARE LTD	25
SECURITYSCORECARD INC	24
ACCENTURE GLOBAL SOLUTIONS LTD	22
BIOCATCH LTD	22
EMC IP HOLDING COMPANY LLC	21
CAPITAL ONE SERVICES LLC	20

gradual growth, with more noticeable increases after 2020. Overall, the pattern suggests accelerating innovation in cybersecurity, driven recently by newer, cloud-focused players.

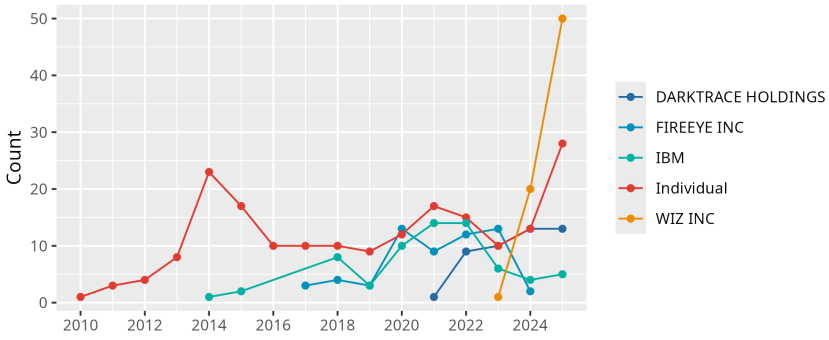


Figure 6: Number of published patents for each publication year.

Figure 7 reveals a clear strategic divide in cybersecurity innovation. Individual inventors dominate in sheer volume, particularly in G06F—the foundational class for digital data processing. However, corporate players tell a more nuanced story. IBM and DarkTrace stand out for their high density of G06N patents, which cover artificial intelligence and advanced computational models. This signals a deliberate pivot from infrastructure toward the "intelligence layer" of cybersecurity, where machine learning enables predictive threat detection and autonomous response.

H04L functions as the critical bridge within this ecosystem. As the classification for digital communication, it represents the networks through which data flows and where security models are deployed. Its presence across nearly all major assignees underscores its foundational role: the pipe connecting computing infrastructure to real-world applications.

Innovation in cybersecurity is stratifying into three distinct layers: the computing core (G06F), the communications pipeline (H04L), and the emerging intelligence layer (G06N). While individual inventors dominate infrastructure patents, corporate leaders like IBM and DarkTrace are aggressively positioning themselves in AI-driven security—a frontier that remains surprisingly underpopulated and ripe for strategic entry.

For decision-makers, the relative scarcity of G06N patents indicates that AI-driven cybersecurity remains an underpopulated frontier with room for strategic entry. A balanced innovation strategy should address three layers simultaneously: the computing core (G06F), the communications pipeline (H04L), and the emerging intelligence layer (G06N) where next-generation capabilities will be defined.

The "Individual" Signal: Hidden Innovation at Scale

Analysis reveals that "Individual" as patents applicant represent the primary entity in cybersecurity-related patents.

- **Source of novel tech and talent.** Individual (or individual+company) applicants often signal early-stage innovations and inventors worth recruiting or partnering with.
- **M&A and licensing leads.** Individual-origin patents with supportive signals (citations, family size, triadic filings) are strong candidates for licensing or acquisition.
- **Signal of external vs internal R&D.** Co-applicant patterns (company + person) can indicate consulting, collaboration, or impending assignment—use this to tailor engagement.
- **Cross-disciplinary scouting and breadth.** Individual portfolios frequently span domains and are, on average, more diversified across IPC codes than firm-level aggregated portfolios—making them a valuable source of cross-cutting techniques and unconventional approaches.

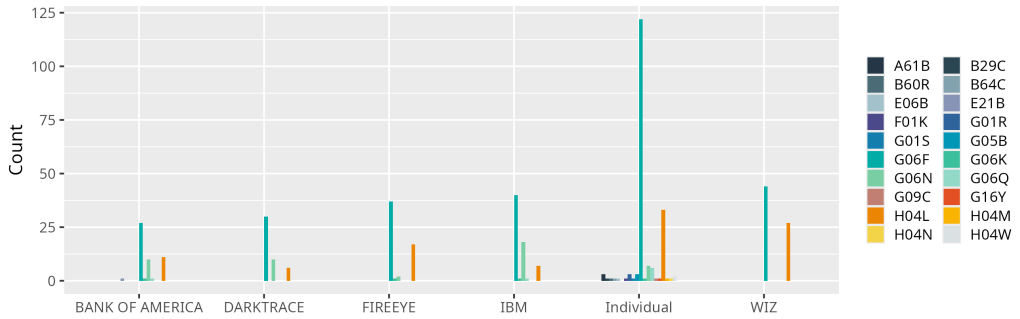


Figure 7: Top five and individual applicants and their technological capabilities shown with their IPC subclasses in cybersecurity.

3.1.6 Key players' patent portfolio

Figure 8 shows that *FireEye* and *Proofpoint* emerge as the established incumbents, with massive G06F portfolios (277 and 140 respectively) supplemented by substantial H04L holdings. This indicates mature organizations that built their foundations on traditional security technologies and have since expanded into network-layer protections. Their relatively modest G06N counts suggest they are latecomers to AI, likely relying on acquisitions or gradual integration rather than native innovation.

DarkTrace and *Rapid7* represent the AI-native challengers. DarkTrace's portfolio shows deliberate balance—30 G06F, 13 G06N, 6 H04L—with the highest G06N density among pure players. Rapid7 follows a similar pattern with 22 G06N patents alongside its infrastructure holdings. These firms are positioning themselves at the intelligence layer, betting that AI-driven detection will define the next generation of security.

The pure-play cybersecurity landscape is fragmenting into distinct niches—network specialists, AI natives, platform builders, and behavioral analysts. The winners will be those whose patent portfolios align with their go-to-market strategy and whose investments in G06N signal readiness for an AI-driven future.

Centripetal and *Radware* reveal themselves as network specialists. *Centripetal*'s 38 H04L patents against only 8 G06F signals a pure-play focus on network security and traffic filtering. Radware's perfect balance between G06F and H04L (54 each) suggests integrated appliances where computing and networking are inseparable.

Wiz and *QOMPLX* show platform ambitions. *Wiz*'s 90 G06F and 54 H04L patents point to cloud-native security infrastructure, while *QOMPLX* broad distribution across G06F, H04L, G06N, and G06Q indicates a diversified approach spanning security, analytics, and business methods.

Biocatch is a behavioral analytics specialist—its 68 G06F patents alongside smaller counts in G01C (navigation) and G01R (measurement) reveal a focus on user behavior monitoring rather than network security.

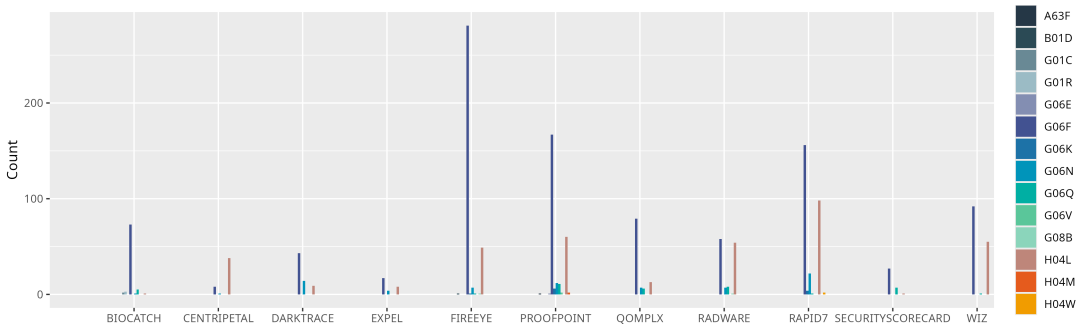


Figure 8: IPC distribution of important firms active in cybersecurity.

3.1.7 European concentration

Figure 9 and Table 5 illustrate the regional distribution of EP first-grant publications in the selected IPC classes (G06F 21, H04L 9) over the period 2005–2025, mapped at the NUTS-1 level. Results reveal a clear core–periphery structure: patenting activity is heavily concentrated in a limited number of metropolitan and industrial regions—most notably Île-de-France, Östra Sverige, Bayern, Manner-Suomi, and Zuid-Nederland—while much of Southern and Eastern Europe exhibits comparatively low levels of activity in these IPCs. Overall, the European cybersecurity innovation system appears highly spatially concentrated, with innovation capacity clustered around established economic and technological hubs.

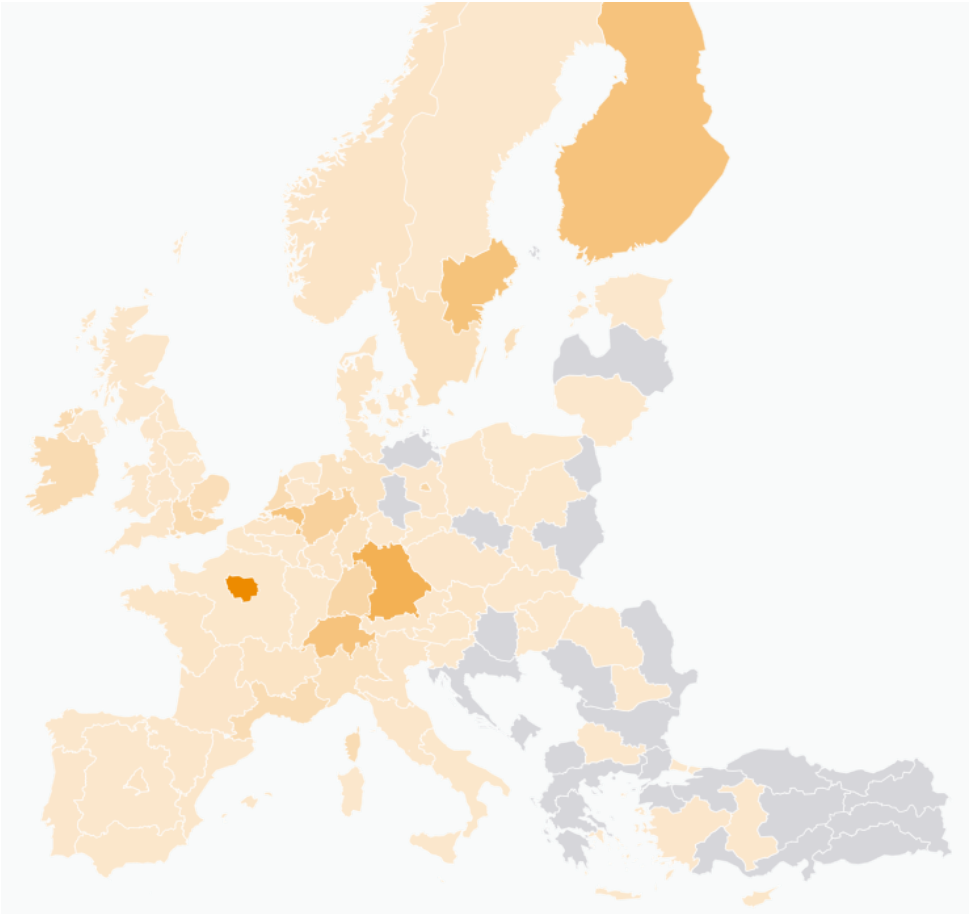


Figure 9: NUTS-1 level EP published patents between 2005–2025.

Percentages are reported instead of absolute counts to enable comparability across regions and to account for incomplete address-to-NUTS mappings. Unmapped records were excluded from the denominator. Where necessary, finer-grained NUTS-2 or NUTS-3 codes were aggregated to the NUTS-1 level.

Cybersecurity patenting in Europe is concentrated in a small number of metropolitan and industrial hubs, indicating strong agglomeration effects in innovation activity. Much of the continent remains peripheral in these core cybersecurity technologies.

Table 5: Share of mapped EP first-grant publications by NUTS-1 region (top 10), 2005–2025.

NUTS-1 region	%
ÎLE-DE-FRANCE	19.1%
ÖSTRA SVERIGE	14.1%
BAYERN	11.6%
MANNER-SUOMI	8.9%
ZUID-NEDERLAND	5.1%
SCHWEIZ/SUISSE/SVIZZERA	4.9%
NORDRHEIN-WESTFALEN	4.9%
BADEN-WÜRTTEMBERG	4.1%
LONDON	3.6%
IRELAND	2.1%

3.2 Citation network analysis

The citation network derived from the backward and forward citations of 2,556 published patents forms a directed graph with 9,353 nodes and 10,907 edges. Figure 10 visualizes this citation network. In the visualization, labels' size correspond to the betweenness centrality score (Brandes, 2001), which identifies nodes that act as critical bridges connecting different clusters. Table 6 lists the top 8 patent applicants with the highest betweenness centrality scores.

Bank of America ranks first in betweenness centrality, reflecting its role in connecting cybersecurity inventions across financial services, enterprise IT, and security vendors, and highlighting the strategic importance of cybersecurity innovation beyond traditional ICT firms.

Out of the 2,556 patents analyzed, 31 were published under the applicant name *Bank of America* as shown in Table 4, based on a search using cybersecurity-related keywords. In the context of a patent citation network analysis, it is observed that Bank of America achieved the highest betweenness score. This indicates that it plays a critical role as intermediaries within the network, facilitating connections between various actors and influencing the flow of information and resources. This high betweenness score suggest that *Bank of America* is strategically positioned to impact innovation trajectories and collaborative efforts in the industry, serving as a pivotal node that connects disparate groups and enhance knowledge dissemination across the patent landscape. Similarly, *FireEye*, which is a pure cybersecurity player, is also one of the key nodes in the development of cybersecurity related patents.

Table 6: Betweenness ranking obtained from the patent citation network.

Rank	Applicant name
1	BANK OF AMERICA
2	AMAZON
3	AT&T
4	BOEING
5	IBM
6	ACCENTURE
7	FIREEYE
8	PALANTIR

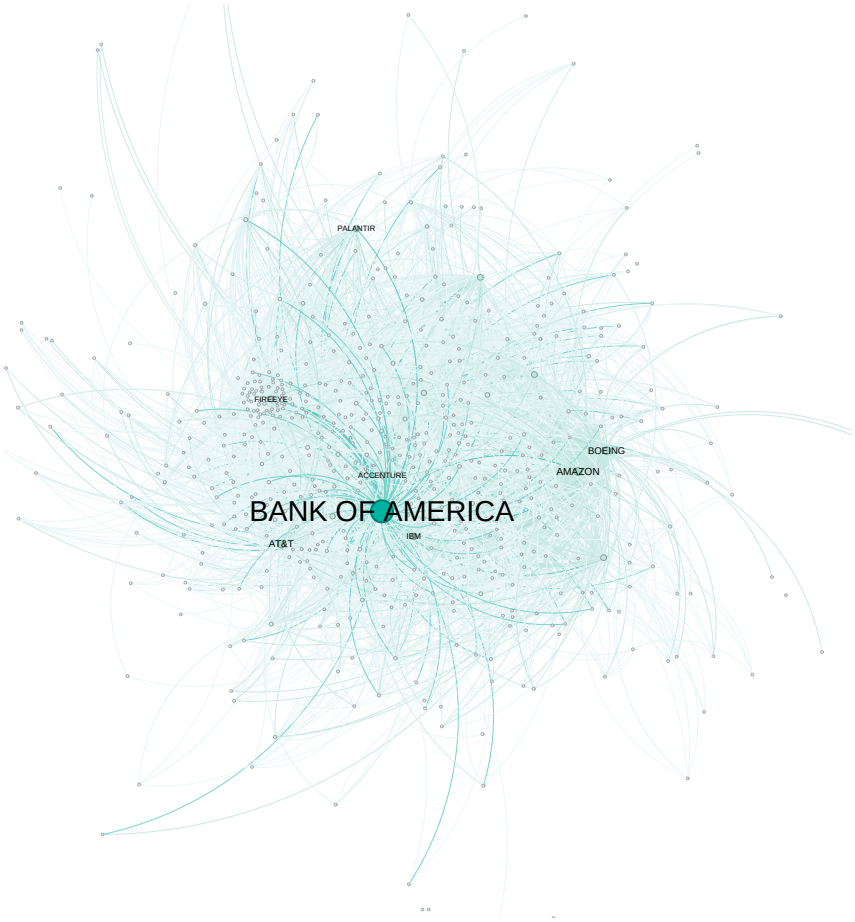


Figure 10: Citation network of patents related to cybersecurity, node and label sizes are proportional to the betweenness score.

3.3 Technology landscape: clustering and semantic mapping

To structure the cybersecurity patent landscape, we apply semantic clustering to group patents by underlying technological intent rather than surface keywords. Technology landscape analysis is inherently iterative: using TechLand's AI-supported mapping, patents and applicants are positioned in a shared two-dimensional technology space, where proximity reflects conceptual similarity. This 2D map enables the identification of coherent technology clusters as well as the applicant names most active within each cluster, providing a basis for successive refinement of the analysis.

Clustering serves three strategic purposes in this report. First, it summarizes the principal sub-domains of cybersecurity, from core network and cloud security to more specialized areas such as quantum communications and sector-specific monitoring. Second, it surfaces additional keywords, IPC/CPC classes, and applicant names that can be used to iteratively refine the initial search. Third, it enables deeper investigation of selected clusters, supporting focused competitive analysis, partnership screening, and M&A targeting.

> Mapping patents and applicants in a shared technology space makes it possible to identify both crowded innovation areas and underexplored clusters, guiding deeper, targeted analysis.

The number of clusters is defined by the analyst (ranging from two to ten), allowing the level of thematic granularity to be adjusted to the strategic question at hand. Once clustering is performed, TechLand's AI layer characterizes each cluster by generating descriptive labels, key terms, and indicators of affected application domains. The five clusters reported in Table 7 reflect a balanced trade-off between interpretability and analytical depth.

Table 7: Cluster labels produced by AI characterization of patent clusters.

Cluster	Description
1	Cybersecurity for networked computer systems
2	Quantum communication and energy management in cybersecure networks
3	Cybersecurity and network monitoring in transportation systems
4	Cybersecurity training, simulation, and performance assessment
5	Cloud computing security and cyberattack protection

4 Conclusion

This report demonstrates how patent-based technology landscape analysis can translate complex intellectual property data into actionable strategic insights for cybersecurity decision-making. The findings reveal a maturing yet dynamically evolving innovation ecosystem with clear implications for competitive positioning, investment prioritization, and technology scouting.

Three structural features define the current landscape. First, cybersecurity innovation remains highly concentrated in both geography and technology domain. The United States accounts for the overwhelming share of USPTO patent activity, with Israel emerging as the sole non-US contributor of comparable strategic weight. Within Europe, patenting clusters tightly around a handful of metropolitan industrial hubs—Île-de-France, Östra Sverige, and Bayern—confirming strong agglomeration effects and limited geographic diffusion. At the technology level, the dominance of G06F 21 (computing security) and H04L 9 (secure communications) underscores that foundational infrastructure protection remains the industry's core.

Second, the applicant structure reveals a productive tension between incumbents and insurgents. Established players such as IBM and FireEye maintain broad, citation-influential portfolios that reflect sustained R&D investment. However, the recent surge of cloud-native entrants—most notably Wiz—signals a shift in innovation velocity and competitive intensity. The substantial presence of individual inventors further indicates that significant inventive activity occurs outside corporate R&D laboratories, offering fertile ground for talent acquisition, licensing, and early-stage investment.

Third, the stratification of technological capability points to an emerging strategic frontier. The relative scarcity of G06N patents—covering artificial intelligence and machine learning—across most assignees suggests that AI-driven cybersecurity remains underpopulated relative to its anticipated importance. Firms such as DarkTrace and IBM, which demonstrate high G06N density, are positioning themselves at this intelligence layer, betting that autonomous, predictive capabilities will define the next generation of security products. For decision-makers, this represents both a competitive threat and an entry opportunity.

> Integrating statistical indicators, citation networks, and semantic clustering transforms patent data into strategic signals. The full value of such analysis, however, emerges through iterative, question-driven workflows that support targeted deep dives for M&A, R&D prioritization, and competitive positioning.

The citation network analysis adds a relational dimension to these findings. Bank of America's top-ranked betweenness centrality reveals that cybersecurity innovation is not confined to traditional technology vendors. Financial institutions and other sectoral players occupy structurally central positions, reflecting the strategic imperative to develop security capabilities in-house rather than rely solely on external procurement. This suggests that partnership, acquisition, and talent strategies must look beyond the usual ICT suspects.

Taken together, statistical indicators, network positions, and thematic clusters provide complementary signals for strategic action. Patent metrics can screen acquisition targets, identify complementary technologies, assess technological fit, and monitor competitive moves over time. In a domain as fragmented and fast-moving as cybersecurity, these signals are particularly valuable for reducing uncertainty around M&A, R&D allocation, and market entry.

The full value of technology landscape analysis, however, emerges through iteration. This high-

level overview establishes the contours of the cybersecurity innovation system, but targeted deep dives—by technology cluster, specific competitor, or geographic region—enable the precision required for investment decisions. Anchoring such analysis in clear strategic questions and refining it with domain expertise remains the critical success factor for translating patent data into competitive advantage.

References

Aharonson, B. S., & Schilling, M. A. (2016). Mapping the technological landscape: Measuring technology distance, technological footprints, and technology evolution. *Research Policy*, *45*(1), 81–96. https://doi.org/10.1016/j.respol.2015.08.001

Aiyer, B., Caso, J., Russell, P., & Sorel, M. (2022). *New survey reveals 2 trillion dollar market opportunity for cybersecurity technology and service providers* (tech. rep.). McKinsey&Company.

Ali, J., & Santos, J. R. (2015). Modeling the Ripple Effects of IT-Based Incidents on Interdependent Economic Systems. *Systems Engineering*, *18*(2), 146–161. https://doi.org/10.1002/sys.21293

Brandes, U. (2001). A faster algorithm for betweenness centrality. *Journal of Mathematical Sociology*, *25*(2), 163–177.

Bueermann, G., & Rohrs, M. (2024). *Global Cybersecurity Outlook 2024* (tech. rep.). World Economic Forum. Retrieved December 13, 2024, from https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

Daim, T., Yalcin, H., & Mermoud, A. (2024). Monitoring cybersecurity technology through the years: A technology mining approach through bibliometrics and patent analysis. *Journal of Cyber Security Technology*, 1–37. https://doi.org/10.1080/23742917.2024.2400729

Dieye, R., Bounfour, A., Özaygen, A., & Kammoun, N. (2020). Estimates of the macroeconomic costs of cyber-attacks. *Risk Management and Insurance Review*, *23*(2), 183–208. https://doi.org/10.1111/rmir.12151

Jaffe, A. B., & Trajtenberg, M. (2005). *Patents, Citations, and Innovations: A Window on the Knowledge Economy*. The MIT Press.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2018). What is the Impact of Successful Cyberattacks on Target Firms? *NBER Working Paper Series*, (24409), 59.

Kammoun, N., Bounfour, A., Özaygen, A., & Dieye, R. (2019). Financial market reaction to cyber-attacks (D. McMillan, Ed.). *Cogent Economics & Finance*, *7*(1). https://doi.org/10/gf6rv2

Kang, B., & Tarasconi, G. (2016). PATSTAT revisited: Suggestions for better usage. *World Patent Information*, *46*, 56–63. https://doi.org/10.1016/j.wpi.2016.06.001

Lerner, J., & Seru, A. (2022). The Use and Misuse of Patent Data: Issues for Finance and Beyond (A. Karolyi, Ed.). *The Review of Financial Studies*, *35*(6), 2667–2704. https://doi.org/10.1093/rfs/hhab084

Morgan, S. (2023). Cybercrime to cost the world $9.5 trillion usd annually in 2024 [Accessed: 2024-12-13]. https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

Nagaoka, S., Motohashi, K., & Goto, A. (2010). Patent Statistics as an Innovation Indicator. In *Handbook of the Economics of Innovation* (pp. 1083–1127, Vol. 2). Elsevier. https://doi.org/10.1016/S0169-7218(10)02009-5

Sharma, P., & Tripathi, R. (2017). Patent citation: A technique for measuring the knowledge flow of information and innovation. *World Patent Information*, *51*, 31–42. https://doi.org/10.1016/j.wpi.2017.11.002
00005.

Srivastava, M., & Jain, K. (2024). Application of Patent Analysis in Technology Management: A Scoping Review [Conference Name: IEEE Transactions on Engineering Management]. *IEEE Transactions on Engineering Management*, *71*, 14897–14914. https://doi.org/10.1109/TEM.2024.3470776

Verspagen, B. (2007). Mapping technological trajectories as patent citation networks: A study on the history of fuel cell research. *Advances in Complex Systems*, *10*(1), 93–115.

World Economic Forum. (2026). *The global cyber outlook 2026* (tech. rep.) (Accessed: 2026-02-18). World Economic Forum. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

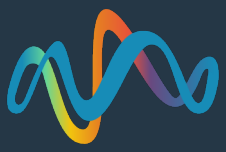
Yang, Y. Y., Akers, L., Yang, C. B., Klose, T., & Pavlek, S. (2010). Enhancing patent landscape analysis with visualization output. *World Patent Information*, *32*(3), 203–220. https://doi.org/10.1016/j.wpi.2009.12.006

Author

Altay Özaygen, PhD
Founder of **metis** analytica, France

Important Notice

Version Disclaimer: This report is **Version 2**, prepared in **February 2026**. Please note that the findings, analyses, and conclusions presented herein are subject to change as new data or insights become available. Readers are advised to consult the latest version for updated information.



+33 (0)7 45 10 61 99
info@metis-analytica.com
www.metis-analytica.com