A technology landscape analysis of cybersecurity

titlepage

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:

Management of Innovation: We focus on patent intelligence, primarily through statistical patent analysis for competitive intelligence. This supports clients in innovation strategies, innovation policies, investment decisions, M&A decision-making, searching for R&D partnerships, and anticipating market shifts. This enables clients to gain insights that guide their innovation strategies and investments, 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.

Executive Summary

This report presents the results of a technology landscape analysis of the cybersecurity sector, a critical component of modern digital infrastructure that serves as a vital defense against an increasingly intricate digital environment. Utilizing advanced patent analysis techniques and citation network analysis, the study provides a comprehensive exploration of the cybersecurity domain, identifying trends, key players, and technological opportunities. Focusing primarily on granted patent applications from the United States Patent and Trademark Office (USPTO), it examines the technology landscape of cybersecurity through the analysis of nearly 1,700 patents filed from 1995 to 2023.

The findings reveal a significant increase in patent filings post-2011, indicating the growing strategic importance of intellectual property in this sector. The United States is the predominant player in this space, with Israel emerging as a strong contender. Key players identified include FireEye, recognized as a major industrial participant, and Architecture Technology Company, noted for having the most diverse patent portfolio. Additionally, emerging entrants with recent increase in patent applications such as Proofpoint and Expel are highlighted.

Through firm-level evaluations, the report emphasizes the value of patent data for stakeholders including policymakers, investors, and industry leaders. It illustrates how patent trends can inform strategic decisions related to mergers and acquisitions (M&A). Notably, the report examines the McAfee-FireEye merger, analyzing metrics such as technological diversity, complementarity, and similarity to demonstrate the role of patents in optimizing M&A outcomes.

This analysis provides a thorough overview of the cybersecurity innovation ecosystem, highlighting its complexity, geographical concentration, and the critical role of intellectual property in understanding this technological landscape.

Contents

1 Introduction

Cybercrime continues to grow at an alarming rate, driven by the expansion of the digital environment and the increasing sophistication of cybercriminals. According to Cybersecurity Ventures, the global annual cost of cybercrime is predicted to reach $9.5 trillion USD in 2024 and $10.5 trillion USD by 2025. These numbers reflect both the rising volume and intensity of attacks (Morgan, 2023). High-profile breaches targeting critical infrastructure, financial systems, and private enterprises underscore the need for heightened security measures and robust cyber risk management practices.

Cyberattacks can render firms inoperable and have cascading effects on other firms and sectors they interact with, potentially impacting entire industries (Ali & Santos, 2015; Dieye et al., 2020). Results indicate a negative abnormal return for the NASDAQ following cyber incidents (Kammoun et al., 2019). Cyberattacks are more likely to occur at highly visible firms, firms with significant intangible assets, and firms with less board attention to risk management (Kamiya et al., 2018).

In response to this surge, a document from the World Economic Forum indicates that the cybersecurity sector is experiencing unprecedented growth (Bueermann & Rohrs, 2024). According to McKinsey, global cybersecurity spending may reach $1.5 trillion to $2 trillion (Aiyer et al., 2022). This growth is driven by increased spending by governments, corporations, and small businesses seeking to protect sensitive data and maintain operational integrity amid rising cyber threats.

This report presents the results of a technology landscape analysis of cybersecurity. Technology landscape analysis is a comprehensive examination of the patent ecosystem within a specific technological domain and serves as an important tool in competitive intelligence. It involves conducting patent statistics to identify innovation trends, key players, emerging technologies, and potential technological opportunities or threats (Jaffe & Trajtenberg, 2005; Kang & Tarasconi, 2016; Lerner & Seru, 2022; Nagaoka et al., 2010). By employing sophisticated citation network analysis, it is possible to map technological trajectories and understand the evolution of distinct technologies (Verspagen, 2007). Technology landscape analysis provides valuable insights for decision-making, innovation strategy, and competitive positioning in the industry (Aharonson & Schilling, 2016; Yang et al., 2010), and also helps identify potential opportunities for R&D partnerships and mergers and acquisitions (M&A). A recent comprehensive literature review highlights the pivotal role of patent analysis in technology management, offering valuable insights into innovation trends, competitive intelligence, and strategic decision-making (Srivastava & Jain, 2024).

> Our primary analysis focuses on the first publication of USPTO-granted patent applications. The patent dates are represented by the application year, as this is considered the closest approximation to the invention date. In this report, we focus mainly on applicants with a high number of patents active in cybersecurity.

Analyzing the cybersecurity technology landscape through patents provides valuable in-

sights into key industrial players. However, it is important to consider that in the realm of offensive strategies and attack methodologies, cybersecurity often operates in secrecy, with many advancements deliberately left unpatented to avoid public disclosure. While patent analysis offers a perspective that primarily highlights the activities of larger, established firms, it may underrepresent small, innovative companies and cutting-edge developments in covert operations. This challenge is not unique to cybersecurity; similar strategies, such as prioritizing being first to market over patenting, are common in other sectors as well.

This report provides a comprehensive analysis of the current technology landscape of cybersecurity based on patent data. Unlike the study by Daim et al., 2024, this analysis focuses on patent applicant names—primarily enterprises—as the central unit of examination. It includes citation network analysis and evaluates the McAfee and FireEye merger as a demonstration example, using diversity, similarity, and complementarity metrics derived from patent data. Furthermore, the report presents the results of a k-nearest neighbors machine learning algorithm applied to patent data, illustrating an iterative approach to technology landscape analysis for deeper insights.

The next section details the methodology employed in this report, followed by a discussion and presentation of the results, and concludes with the final section.

2 Methodology

This section describes the approach used to evaluate cybersecurity technology landscape. Below, we outline the data sources, analytical methods employed, and the rationale for each methodological choice.

The analysis utilized **metis-TechLand**, an in-house AI-supported platform for streamlining technology landscape analysis. This tool simplifies data acquisition, processing, and visualization, significantly reducing the time needed for comprehensive evaluations.

2.1 Data

The primary data source for this analysis is EPO PATSTAT, May 2024 edition. The dataset is generated by performing keyword search on patent titles and abstracts, followed by the application of filters to refine the search results.

- **Search keywords:** Besides the keywords 'cybersecurity,' 'cyberattack,' 'cyberdefense', each patent was required to include the word 'cyber' combined with one of the following terms: attack, crime, defense, incident, intelligence, monitoring, protection, response, risk, security, threat and warfare.
- **Filters applied:**
  - Patent office: USPTO
  - Patent type: Patents of invention

2.2 Analytical framework

2.2.1 Statistical patent analysis

Statistical patent analysis is the use of statistical methods to evaluate patent data, aiming to identify trends, monitor technological advancements, assess competitors, identify key innovators, evaluate patent quality, and guide policy or investment decisions.

In this report we analyze patents from two perspectives:

- First publications of granted patent applications
- Recent patent applications

By analyzing **first publications of granted patent applications**, we can uncover historical innovation trends, evaluate pioneering technologies, and assess their long-term impact through citation analysis.

On the other hand, **recent patent applications** provide valuable insights into emerging technologies, new entrants, competitive movements, and potential market opportunities. This information enables firms to strategically align their R&D efforts, identify collaboration or licensing opportunities, and target firms for M&A transactions.

In this abridged report, we focus on applicants with a high number of patents, as indicated in blue in Table 1. However, a comprehensive analysis would require data from both large and small firms. Such an in-depth exploration is beyond the scope of this report.

Table 1

	Applicants with a high number of patents	**Applicants with a low number of patents**
First publication of granted patent applications	Analyzing key players, historical trends	Identifying small applicants, niche inventions
Patent applications from the last four years	Identifying new technological trends among incumbents and new entrants	Tracking new technological trends among start-ups, new players, and predominantly pure players

2.2.2 Citation Network Analysis

Patent citation network analysis (CNA) is a research method that examines the relationships and connections between patents through their citations. By mapping how patents reference one another, this analysis reveals the flow of knowledge and innovation within a particular field or technology area. It helps identify key patents, influential inventors, and trends in technological development. By visualizing and analyzing these networks, researchers and organizations can gain insights into competitive dynamics, collaboration patterns, and the evolution of technologies over time. Generally, patents or research articles that receive a higher number of citations indicate a greater level of prominence. However, CNA goes further by identifying key nodes that play critical roles in technological development (Sharma & Tripathi, 2017).

In this study, CNA is constructed in the following manner:

- **Backward citations:** Patents cited by the analyzed patents.
- **Forward citations:** Patents that cite the analyzed patents within three years of application.

Citations within the first three years often reflect the immediate relevance and technological impact of the patent. Early citations may indicate the patent's importance in shaping subsequent innovations. Limiting the window to three years reduces the influence of later, potentially less relevant citations (e.g., routine citations or those driven by legal disputes).

In patent citation network analysis, nodes represent individual patents. In this report, the citation network analysis is conducted by aggregating data by assignee names, which often

correspond to firm names, creating a network that illustrates the flow of knowledge between institutions.

2.2.3 Innovation metrics for M&A analysis

Mergers and Acquisitions (M&A) refer to the strategic processes through which companies consolidate their operations, assets, or ownership interests. A *merger* occurs when two companies combine to form a new entity, while an *acquisition* involves one company purchasing another, resulting in the acquired company being absorbed into the buyer. M&A activities are undertaken for various reasons, including expanding market share, gaining new technologies, reducing competition, and achieving operational efficiencies.

M&A are complex processes that significantly influence both short-term and long-term success for the firms involved. Research indicates that related or focused acquisitions tend to outperform unrelated or diversifying ones, as acquirers in the former category are typically more skilled in managing operations and integrating target firms effectively. Moreover, deal performance is often enhanced when shareholders actively engage through voting, monitoring, and advising during the M&A process (Renneboog & Vansteenkiste, 2019).

In the context of technological advancements, M&As serve as essential strategic tools for firms aiming to bolster innovation and competitiveness. These transactions enable companies to deepen their existing capabilities, access new technological domains, and explore opportunities beyond their current offerings. Acquirers can benefit from combining complementary knowledge, which fosters innovation and enhances research and development (R&D) output. Studies have shown that technological complementarities between firms facilitate the creation of novel technological opportunities (Cassiman et al., 2005); furthermore, firms with either narrow or broad technological scopes tend to outperform those with moderate scopes in post-acquisition R&D output (Shafique & Hagedoorn, 2022).

To conduct successful technological M&As, firms can leverage patent evaluations to assess the technological knowledge bases of both the acquirer and the target, examining the relationships between them. By understanding these dynamics, businesses can position themselves strategically in the marketplace, making informed decisions that enhance their growth and innovation potential.

To evaluate M&A, the following metrics were calculated:

- **Technological diversity:** Measured using the Herfindahl–Hirschman Index (HHI) to assess the breadth of technological expertise within a firm.
- **Technological complementarity:** Quantifies the overlap of IPC subclasses between the acquirer and target, highlighting synergistic opportunities.
- **Technological similarity:** Examines the extent of shared IPC classes, facilitating integration and knowledge transfer.

2.2.4 Machine Learning

The k-Nearest Neighbors (k-NN) algorithm from the scikit-learn Python library (Pedregosa et al., 2011) is used to expand the search space with new keywords or applicant names. This algorithm is an example of an unsupervised machine learning technique.

k-Nearest Neighbors

The k-Nearest Neighbors (k-NN) algorithm enhances the search process by identifying:

- Applicants that are similar to those of the acquiring firm in a merger and acquisition (M&A) transaction.
- Keywords closely related to the primary search terms in the field of cybersecurity.

k-NN operates under the premise that similar data points are located close to each other in the feature space. By analyzing the "k" nearest data points which consist of all patents indexed, the algorithm can make informed suggestions regarding applicant names and related keywords, improving the accuracy and relevance of the search results.

3 Results and discussion

In this section, we present the results of the technology landscape analysis of cybersecurity, focusing on applicants with a high number of patents, as shown in Table 1. The results will be categorized according to the dataset groups: Section 3.1 First publication of granted patent applications and Section 3.2 Patent applications from the last four years.

3.1 First publication of granted patent applications

3.1.1 Descriptive results

A total of 1,698 patents were analyzed, with the first patent filed in 1995 (USPTO No: 5590197) and published in 1996, and the latest patent filed in 2023 and published in 2024. The patent dates presented in this report refer to the application date, as it is the closest date to the invention.

Patent counts by patent offices

Figure 1 illustrates the counts of first publications of granted patent applications in cybersecurity over the years across the top five patent offices, while Table 2 presents the total number of published patents in cybersecurity for these offices.

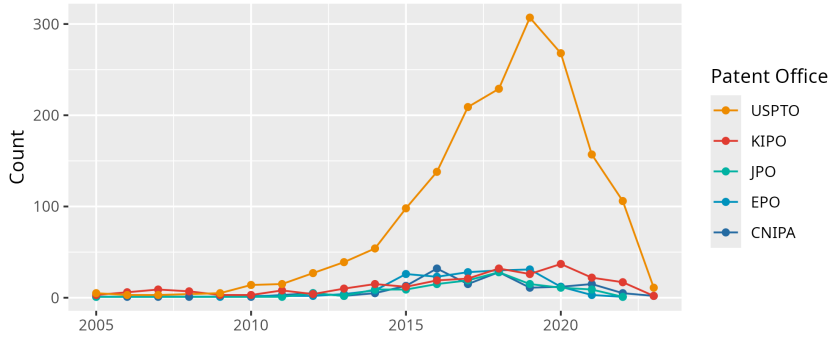


Figure 1: Yearly granted patent counts.

Table 2: Granted patents counts for the period 1995-2023.

Patent Office	Application
USPTO	1698
KIPO	301
EPO	177
CNIPA	153
JPO	129

The abrupt fall in patent publications in the last three years is due to the time gap between the patent application date and the publication date. There are patent applications currently under examination that may eventually be granted and published. This impacts the visibility of recent inventions.

In this report, we will focus on USPTO patent publications as it has the largest number of patents in cybersecurity, making it a crucial focus for analysis. The USPTO not only serves as a hub for innovation in the United States but also attracts significant international filings due to its robust intellectual property protections and established legal framework. While examining other patent offices, such as the Korean Intellectual Property Office (KIPO) and the China National Intellectual Property Administration (CNIPA), could provide valuable insights and a broader analysis, this is beyond the scope of this report.

Patent counts by applicant countries

The patent counts categorized by applicant countries highlight the leading countries contributing to cybersecurity patents. As illustrated in Figure 2 and Table 3, the United States is the dominant applicant country by a significant margin, followed by Israel, which ranks first among the other countries.

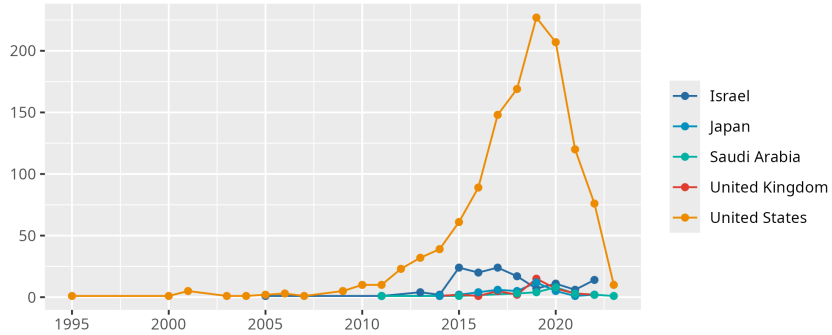


Figure 2: Yearly patent counts for top five applicant countries.

Table 3: Patent counts for top 10 applicant countries.

Applicants' country	count
United States	1241
Israel	131
Japan	39
United Kingdom	38
Saudi Arabia	23
South Korea	21
Singapore	20
Canada	19
Germany	14
Ireland	12

The distribution of applicants by number of patents

The distribution of applicants based on the number of patents they hold will reveal which entities are most active in securing patents in cybersecurity. There are 575 distinct applicant names obtained by the keyword search. Their distribution with respect to the number of patents is shown in Figure 3. The figure demonstrates a long-tail distribution, indicating that there is no concentration of cybersecurity-related patents in the hands of a few applicants.

In this report, we will primarily focus on top applicants; however, applicants with a smaller number of patents could reveal different aspects of the cybersecurity landscape.

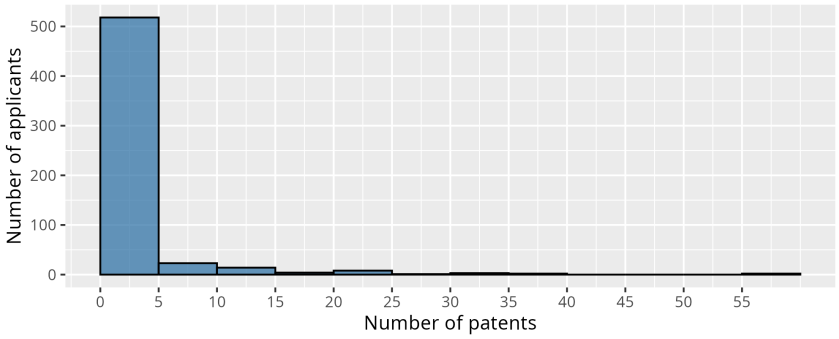


Figure 3: Distribution of published patents across applicants.

Patent grant delay

Patent grant delay refers to the time it takes for a patent application to be processed and approved by a patent office. This delay can occur due to various factors, including a backlog of applications, complexity of the invention, examination procedures, or the need for additional information from the applicant.

Figure 4 illustrates the average grant delay, measured in days, from 2009 to 2023. This information is crucial for understanding the time it takes for inventions in cybersecurity to be publicly recognized. The graph reveals a noticeable plateau between 2014 and 2019, during which the duration consistently ranged between 1024 and 945 days (2 years 10 months to 2 years 7 months approximately). This plateau suggests that, during this period, the processing times for patent applications and their subsequent publications remained relatively stable. After 2019, the graph shows a decline in the duration gap, which can be attributed to patents that are still in the processing stage.

IPC distribution

Table 4 illustrates the IPC distribution of 1,698 patents, revealing that G06F 21 (Security arrangements for protecting computers, components, programs, or data against unauthorized activity) and H04L 9 (Arrangements for secret or secure communications; Network security protocols) are the two primary IPC categories for cybersecurity. Next we will will focus on these two categories to identify firms active in this domain.

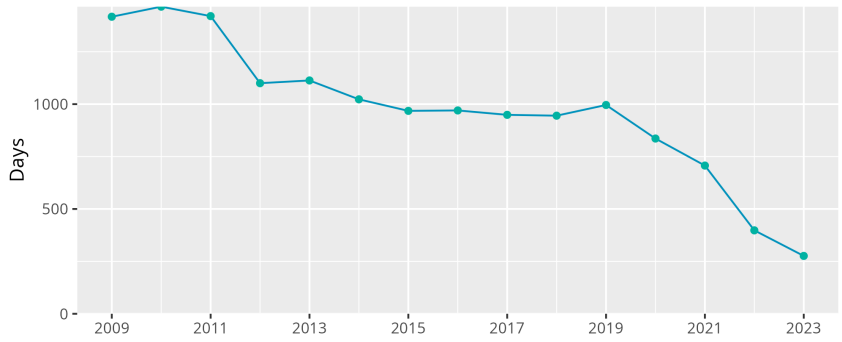


Figure 4: Patent publication delay.

Table 4: Top 10 IPC main class distribution of the published patents in cybersecurity.

IPC		Total
G06F 21	Security arrangements for protecting computers, components thereof, programs or data against unauthorised activity	353
H04L 9	Arrangements for secret or secure communications; Network security protocols	182
G06F 16	Information retrieval; Database structures therefor; File system structures therefor	146
H04L 29	Arrangements, apparatus, circuits or systems, not covered by a single one of groups	142
G06F 11	Error detection; Error correction; Monitoring	112
G06F 9	Arrangements for program control, e.g. control units	83
G06F 3	Input arrangements for transferring data to be processed into a form capable of being handled by the computer; Output arrangements for transferring data from processing unit to output unit, e.g. interface arrangements	73
H04L 12	Data switching networks	52
G06N 20	Machine learning	51
G06F 17	Digital computing or data processing equipment or methods, specially adapted for specific functions	40

Figure 5 illustrates the distribution of granted patents across various applicant names in the IPC groups G06F 21 and H04L 9, spanning the application years from 2002 to 2023. 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 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.

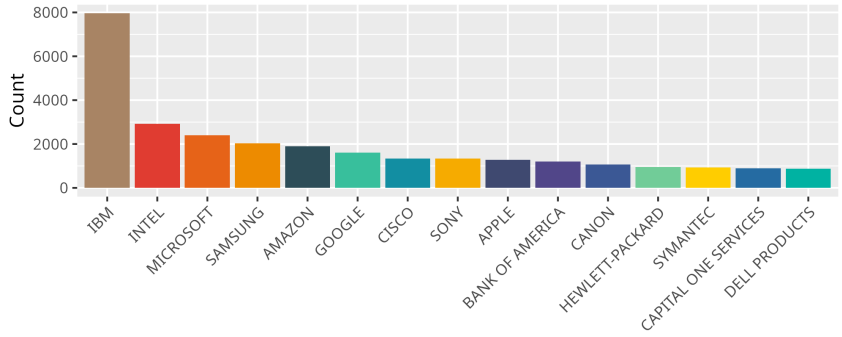


Figure 5: Distribution of granted patents in G06F 21 and H04L 9 across applicants for the period 2002-2023.

3.1.2 Firms with high number of patents in cybersecurity

In this section, we present the applicants which have more than 15 granted patents related to cybersecurity. Table 5 provides a comprehensive list, limited to applicants with more than 15 patents, where the keywords used in this report appear.

Table 5: Number of granted patents of key players (+ 15 patents) in cybersecurity.

Applicant	Total
FIREEYE	59
IBM	58
QOMPLX	38
GE (GENERAL ELECTRIC)	37
HONEYWELL INTERNATIONAL	34
MICROSOFT	34
BANK OF AMERICA	31
BOEING	26
ARCHITECTURE TECHNOLOGY	25
CENTRIPETAL NETWORKS	25
DARKTRACE	23
BIOCATCH	21
DARKTRACE	21
RADWARE	21
SECURITY SCORECARD	21
EMC IP HOLDING	19
T-MOBILE USA	19
RAPID7	18
SAUDI ARABIAN OIL	16
RAYTHEON	15

Figure 6 illustrates the yearly granted patents for the top five firms. FireEye and IBM consistently lead in patent publications since 2016, reflecting their strong commitment to innovation in cybersecurity. Notably, Qomplx made a significant impact in 2020, publishing 15 patents that propelled them to the forefront for that application year.

Figure 7 illustrates the distribution of patent IPC classifications for the top five firms in

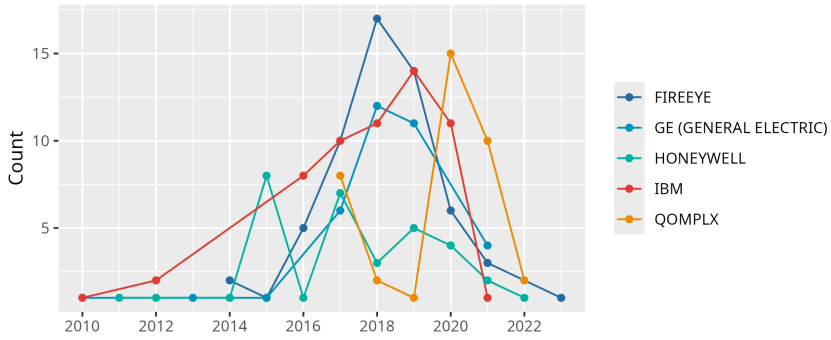


Figure 6: Number of published patents for each application year.

cybersecurity reveals distinct strategic focuses among the companies. While FireEye, Qomplx and IBM exhibit a higher concentration of patents in the G06F category, which pertains to computing systems and methods, indicating a strong emphasis on cybersecurity software solutions, IBM, GE, and Honeywell demonstrate a more diversified portfolio across multiple IPC classes. IBM, for example, shows notable activity in G06N, relevant to artificial intelligence and machine learning, suggesting its commitment to integrating advanced technologies into cybersecurity. Similarly, GE's patents span a broader range, including G05B for control systems and H04L for transmissions, showcasing its focus on industrial applications of cybersecurity. Honeywell also highlights versatility with patents in G05B and G08B, related to building automation and security. In contrast to the more niche approaches of FireEye and Qomplx, which focus primarily on software and cybersecurity technologies, IBM, GE, and Honeywell's diverse classifications reflect a strategic alignment with broader technological innovations and industrial applications, positioning them differently within the cybersecurity landscape.

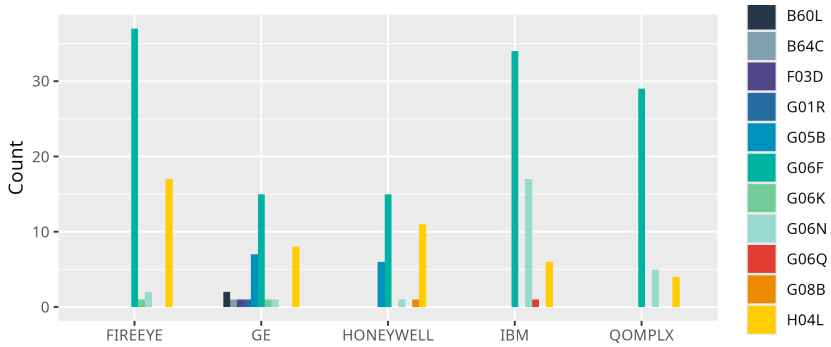


Figure 7: Top five applicant and their technological capabilities shown with their IPC subclasses in cybersecurity.

Key players' patent portfolio

Table 6 lists the patent portfolios of key players in the cybersecurity field. Figure 8 shows the yearly patent publications of firms engaged in cybersecurity, excluding incumbents like IBM, GE, Microsoft, and Honeywell, which are omitted because they do not primarily focus on cybersecurity.

Table 6: Patent portfolio measured with the number of granted patents of key players, application year starts from 2002.

Applicant name	Patent count
IBM	119318
GE (GENERAL ELECTRIC)	26957
MICROSOFT	21515
HONEYWELL	13271
FIREEYE	334
ARCHITECTURE TECHNOLOGY	278
RAPID7	187
RADWARE	107
QOMPLX	102
BIOCATCH	76
CENTRIPETAL NETWORKS	76
SECURITY SCORECARD	29
DARKTRACE	24

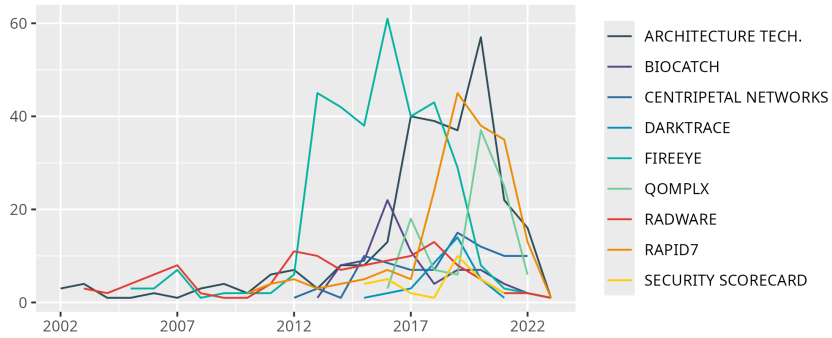


Figure 8: Number of published patents for each application year.

Figure 9 illustrates the firm-level distribution by IPC of key players' granted patents. FireEye stands out with 334 patents, while Architecture Technology Company has the most diverse portfolio with 278 patents. This figure highlights the diversity of firms and provides information about potential mergers and acquisitions (MA) as well as research partnerships depending on the strategical position of the acquirer.

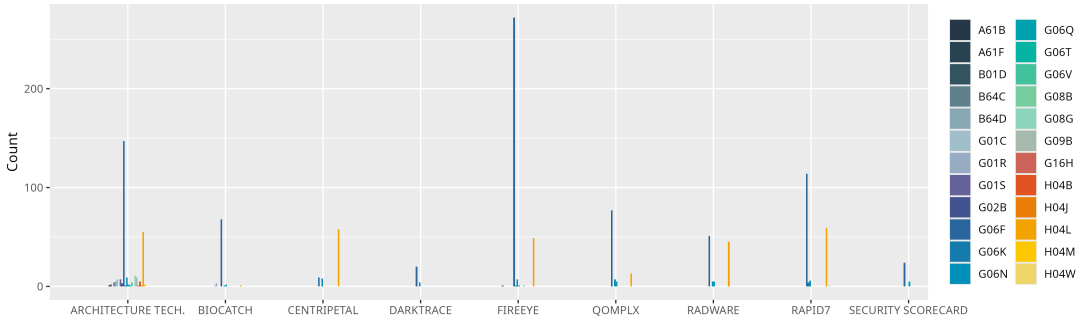


Figure 9: IPC distribution of important firms active in cybersecurity.

3.2 Patent applications from the last four years

Patent publication is a long and tedious process and there is a lag between patent application and patent publication dates. In Section 3.1 we have examined the granted patents. In this section we will search for the patent applications in the last 4 years not necessarily published, to be able to detect emerging players and new directions within technological space.

Patent counts by patent offices

Table 7 shows the top 5 national patent offices. From this table it is obvious that USPTO is still the leading patent office related to cybersecurity. The total number of patent of innovation applications made to USPTO for the years 2019-2023 is 1,600.

Table 7: Number of applications in top 5 national patent offices for the period 2019-2023.

Patent Office	Application
USPTO	1,600
EPO	266
KIPO	142
CNIPA	112
JPO	92

Patent counts by applicant countries

Table 8 lists the top patent applicants to the USPTO for 2019–2023, focusing on patent applications containing cybersecurity-related keywords. Notably, Proofpoint, Expel, Wiz, and Bitsight exhibit a significantly high number of patent applications compared to their presence in the list of granted patent applications in Table 5.

IPC distribution

In addition to the overall trends observed in the graph Figure 10, a closer examination of the data reveals notable increases in the number of patent applications for specific IPC classifications from 2021 to 2022. The IPC code “H04L 9” (Arrangements for secret or secure communications; Network security protocols), saw a significant increase of 54 applications, reflecting heightened innovation in network security technologies within cybersecurity. Similarly, “G06F 21”, (Security arrangements for protecting computers, components thereof, programs or data against unauthorised activity), demonstrated robust growth with an increase of 20 applications. Additional subclasses of “G06F” also experienced increases. This surge indicates a continuous emphasis on advancements in computing solutions for cybersecurity challenges. These increases illustrate the areas of investment and innovation driving research and development in the cybersecurity sector during this period. Results obtained from the analysis indicate that there has not been significant change in the IPC trends derived from the patent applications in cybersecurity compared to the granted patents.

Table 8: Patent applicants with over + 15 patents applications made during the last four years.

Applicant	Total
QOMPLX	67
DARKTRACE	48
IBM	37
BANK OF AMERICA	33
DARKTRACE	32
MICROSOFT	26
T-MOBILE USA	26
CENTRIPETAL NETWORKS	25
FIREEYE	24
GE (GENERAL ELECTRIC)	23
PROOFPOINT	23
RAPID7	22
EXPEL	21
HONEYWELL	20
WIZ	19
ACCENTURE GLOBAL SOLUTIONS	18
BITSIGHT TECHNOLOGIES	18
SECURITY SCORECARD	17
SAUDI ARABIAN OIL COMPANY	16

A further analysis of these two IPC groups (H04L 9 and G06F 21) in relation to patent publications and applications from applicants with a limited number of patents could help us identify emerging and smaller firms entering this sector.

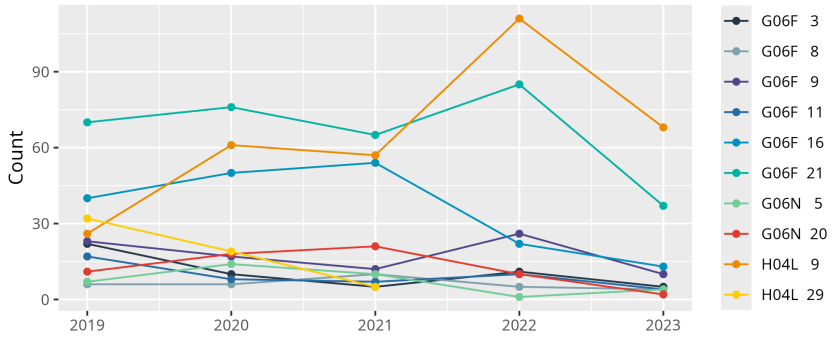


Figure 10: Trends in IPC classifications for cybersecurity patent applications from 2019 to 2023.

3.3 Citation network analysis

The citation network derived from the backward and forward citations of 1,698 published patents forms a directed graph with 4,591 nodes and 10,428 edges. Figure 11 visualizes this citation network, which has been pruned for clarity and aesthetic purposes. 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 9 lists the top 10 patent applicants with the highest betweenness centrality scores.

Out of the 1,698 patents analyzed, 31 were published under the applicant name "Bank of America," as shown in Table 5, based on a search using cybersecurity-related keywords. Despite its relatively small share, Bank of America plays a strategic role in the technology landscape by linking different clusters within the patent citation network. Similarly, FireEye, a pure cybersecurity player with a moderate number of patents, also serves as a key node in the development of cybersecurity-related patents.

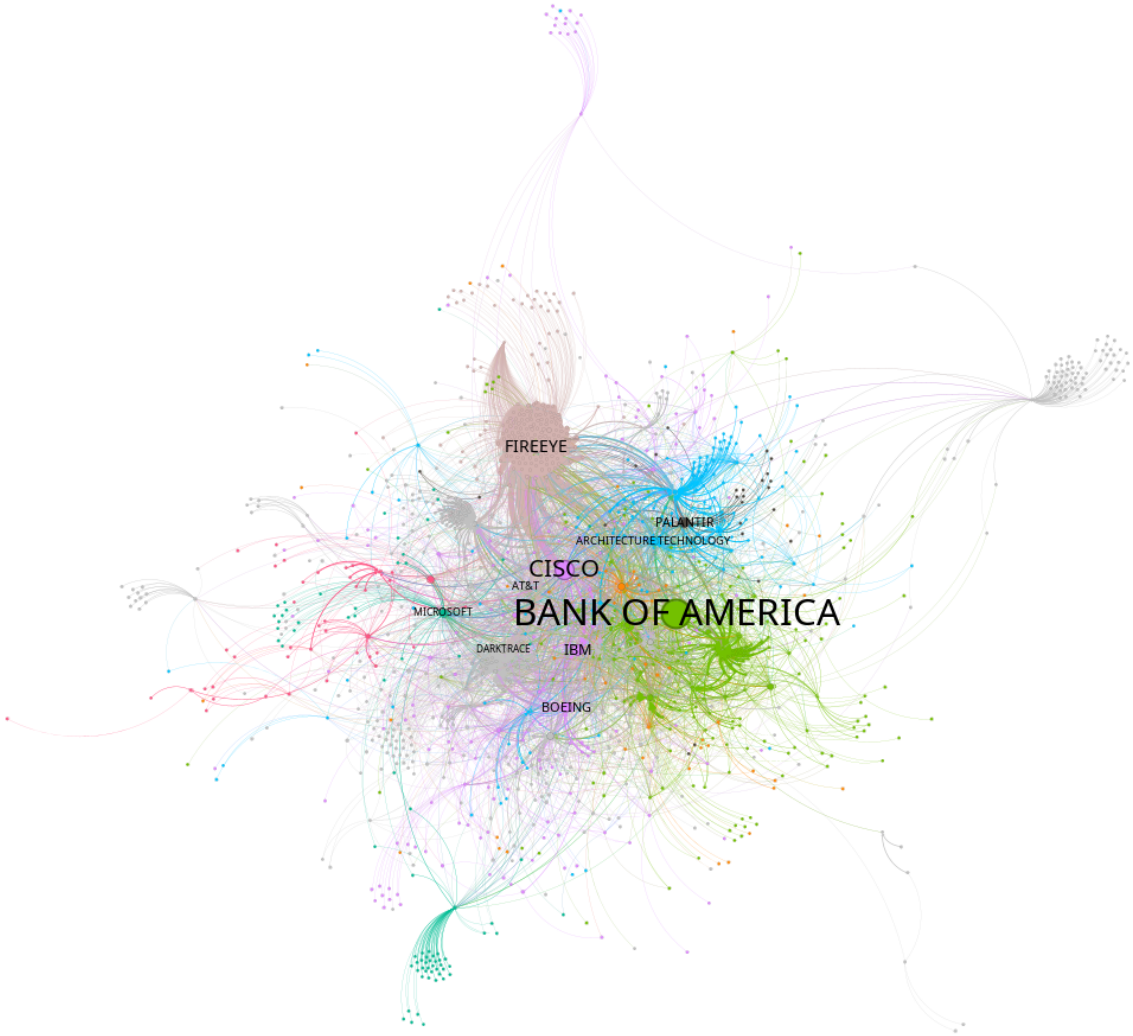


Figure 11: Citation network of patents related to cybersecurity.

Table 9: Betweenness ranking obtained from the patent citation network.

Rank	Applicant name
1	BANK OF AMERICA
2	CISCO
3	FIREEYE
4	IBM
5	BOEING
6	PALANTIR
7	ARCHITECTURE TECHNOLOGY
8	AT&T
9	MICROSOFT
10	DARKTRACE

3.4 Understanding an M&A in cybersecurity

In 2021, Symphony Technology Group merged FireEye and McAfee, creating Trellix, one of the largest pure-play cybersecurity companies (Trellix, 2021). This section examines McAfee as the acquirer, given its size, and evaluates medium-sized firms in the cybersecurity sector as potential targets.

Using patents to obtain certain metrics for evaluating an M&A process for the acquirer is effective, but the same approach can also be applied to anticipate the M&A strategies of competitors.

By systematically evaluating enterprises through these dimensions, firms can identify acquisition targets that align with their strategic goals, such as enhancing existing knowledge, accessing new domains, or achieving technological synergies. Such analyses help firms optimize post-acquisition R&D performance and innovation output.

The graphics on the first row of the Figure 12 show various technology firms' patent counts and technological diversity. The second row shows complementarity, and similarity measures with respect to McAfee, offering insights into potential M&A targets. FireEye, acquired by McAfee in 2022, demonstrates strong alignment in technology diversity and similarity, highlighting its strategic fit. Other firms, such as Rapid7 and Security Scorecard, stand out for their high complementarity and similarity. This type of evaluation helps acquirers prioritize firms that align with their technological and innovation goals, enhancing their capabilities.

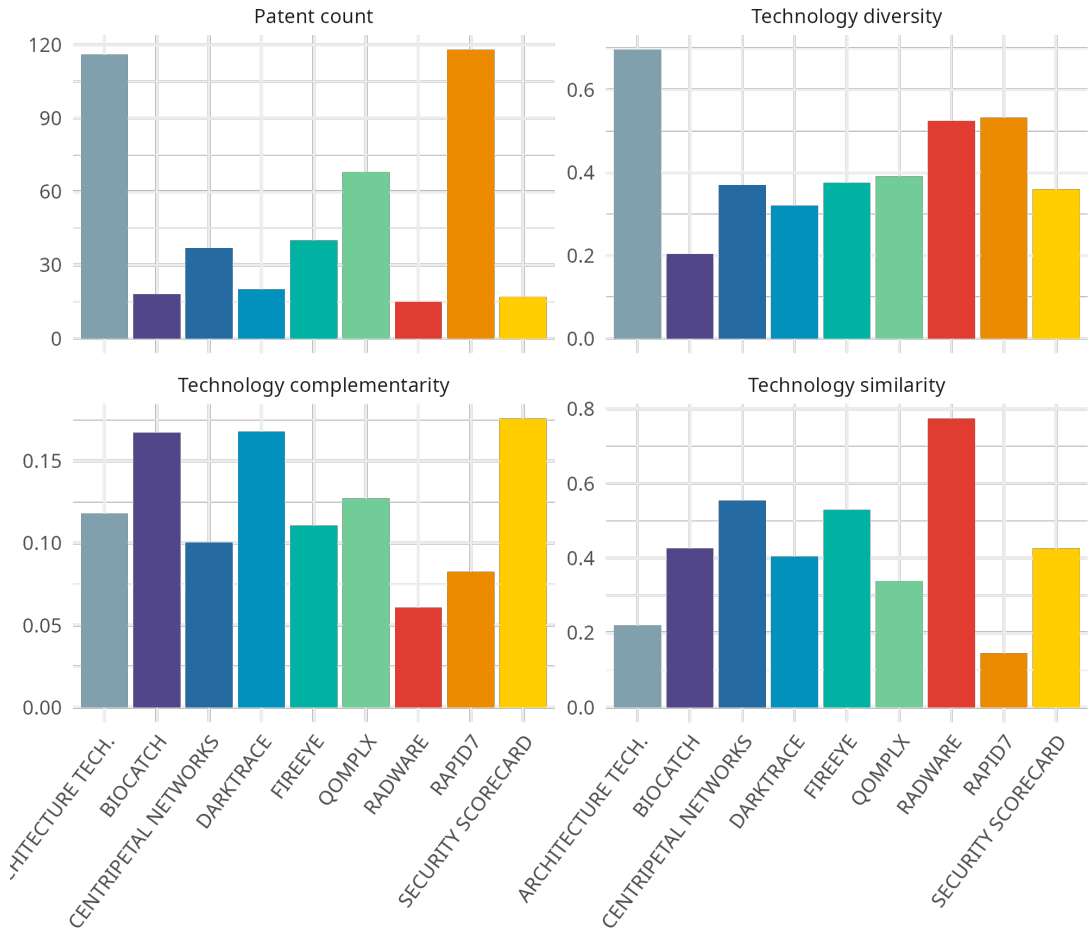


Figure 12: Various parameters which may be used in an M&A acquisition for McAfee.

3.5 Machine learning results

3.5.1 k-nearest neighbors

Patents encompass diverse information, first we used k-nearest neighbors algorithm which we transformed into a 2-D representation using UMAP mapping techniques (McInnes et al., 2020). These 2-D maps feature applicant names and keywords derived from the processing of patent titles and abstracts.

Using machine learning algorithms can help identify words or applicant names that are similar to the search keywords or applicant names, which can then be added to the search space. This approach will enhance the iterative process by adding an additional layer of refinement.

Firms located near McAfee are listed in Table 10. Using a similar approach, we identified cybersecurity-related keywords such as 'encryption,' 'signature,' and 'identifiers.' By incorporating these applicant names and newly identified keywords into the patent portfolio analysis or keyword search, the search space can be expanded. However,

it is important to consider that expanding the search space may lead to a recall problem. As previously mentioned, technology landscape analysis is an iterative process that requires employing all the aforementioned methods at various stages.

Table 10: Technological diversification indexes obtained with IPC main group codes (8 character) with similarity and complementarity values with respect to McAfee.

Amazon Tech.	Symantec Corp.	Bank of America	Ebay
Yahoo!	Alibaba Group	Open Invention Network	Intuit
United Services Automobile Assoc.(USAA)		Verint Systems	Giesecke & Devrient
Trend Micro	Kaspersky Lab	Dell Software	Airwatch
Nagravision	FireEye	Palo Alto Networks	FMR
Verint Americas	Intertrust	Qualcomm	Nice Systems
Wyse Technology	Shape Security	F-Secure	Sophos
Security First Corp	Varonis Systems	Nextbit Systems	Irdeto
Bitdefender	Calgary Scientific	Proton World Int.	Kaseya

3.5.2 Clustering

Using the k-Means algorithm, we obtained clusters based on the results of a keyword search conducted on patents. Figure 13 illustrates the results of this analysis, which identified 10 distinct clusters. These clusters represent thematic groupings of related patents, reflecting common topics or characteristics within the data.

Figure 13: Clustering of the patents obtained with keyword search.

Table 11: Keywords identified in clusters from patent analysis.

Cluster 1	file, object, malware, hash, content, logic, integrity, configuration, data integrity, executable
Cluster 2	enterprise, enterprise network, mobile, element, business, computer network, network element, internet, change, graph
Cluster 3	vehicle, code, incident, physical, key, indicator, parameter, instruction, controller, invention
Cluster 4	monitoring node, node value, monitoring node value, current monitoring, current monitoring node, feature vector, series, abnormal, computer platform, vector
Cluster 5	vector, signal, collection, feature vector, anomalous, security score, anomalous behavior, attack vector, security information, group
Cluster 6	message, email, computerized, legitimate, human user, cyberattacker, human, enduser, phishing, interference
Cluster 7	graph, training, cloud, protected, cyberthreat, simulation, tool, cluster, protection, malware
Cluster 8	anomaly, profile, attribute, company, interaction, user interface, user interaction, respective, anomaly detection, rating
Cluster 9	domain, address, transaction, ip, dns, ip address, solution, identifier, client network, vendor
Cluster 10	packet, packetfiltering, intransit packet, intransit, filtering, packet filtering, filtering rule, packet filtering rule, flow, gateway

The clustering results of cybersecurity patents offer an insightful lens into the diverse thematic areas within this domain. Based on the image and cluster details provided, here's an interpretation:

The visual clustering reveals distinct groupings of patents, signifying thematic similarities within each cluster. The clusters are scattered across the space, with varying densities, indicating that some topics are more concentrated than others. An explanation for each clusters is as follows.

- **Cluster 1 (Malware and Integrity):** This cluster focuses on malware detection and prevention, emphasizing terms such as file integrity, executable content, and hash functions. These patents likely address methods to safeguard data against malicious code by validating and monitoring system components for anomalies.
- **Cluster 2 (Enterprise Networks):** Centered around enterprise cybersecurity, this cluster relates to securing computer networks, mobile environments, and business systems. The emphasis on elements like internet and change suggests solutions aimed at dynamic network security, possibly in response to evolving threats.
- **Cluster 3 (Vehicle and Physical Security):** This grouping seems to relate to cybersecurity in physical and vehicular systems. Terms like vehicle, controller, and incident indicate a focus on securing automotive or industrial systems against cyber-physical attacks, leveraging indicators and parameters to detect breaches.
- **Cluster 4 (Monitoring and Anomaly Detection):** With terms such as monitoring node and feature vector, this cluster appears to address methods for real-time system

monitoring. The focus is on detecting anomalies and maintaining system integrity, which is critical for preemptive threat mitigation.

- **Cluster 5 (Feature Vectors and Attack Analysis):** Closely related to Cluster 4, this group highlights the use of vectors and signals to assess anomalous behavior. Patents in this cluster likely propose quantitative methods to analyze attack vectors and assess security risks.
- **Cluster 6 (Phishing and User Protection):** This cluster tackles human-centric threats such as phishing. Terms like email, legitimate, and cyberattacker suggest a focus on distinguishing legitimate communications from malicious ones to protect end-users.
- **Cluster 7 (Training and Cyberthreat Protection):** This cluster focuses on using tools such as training datasets and simulations to enhance cyber defense systems. The mention of cloud and malware implies solutions for scalable and adaptive protection.
- **Cluster 8 (User Behavior and Anomaly Detection):** Emphasizing anomaly detection in user interactions, this cluster explores profiling and behavioral analysis. It likely relates to tools for monitoring and evaluating user behavior to detect suspicious activities.
- **Cluster 9 (Network Transactions):** With a focus on domains, IP addresses, and DNS transactions, this cluster highlights methods for securing online transactions and protecting against domain-level attacks.
- **Cluster 10 (Packet Filtering):** This technical cluster addresses packet-level security with terms like filtering rules and in-transit packets. The focus is on ensuring secure data flow through networks via packet inspection and filtering.

The clusters are distributed across the visualization, and some appear more tightly grouped, indicating focused research areas, such as Cluster 10 (packet filtering). Other clusters, like Cluster 2 (enterprise networks), are more dispersed, reflecting a broader scope of associated topics. The overlapping regions in the visualization could signify thematic overlaps, such as between anomaly detection (Clusters 4 and 5) and user interaction monitoring (Cluster 8).

The clustering results demonstrate a rich diversity of cybersecurity patent topics, ranging from technical solutions like packet filtering to behavioral and anomaly-based approaches. Based on the results of the clustering, it is possible to expand the keywords used in the search. Table 11 lists the keywords associated with each of the 10 identified clusters. The keywords provide insight into the underlying themes and trends captured in the analyzed patents, facilitating a deeper understanding of the innovation landscape. Additionally, the number of clusters can be increased to achieve more granular categorizations.

4 Conclusion

Technology landscape analysis employs a variety of tools and approaches, as we have partially illustrated in this document. We demonstrated how to conduct different search strategies, including keyword and attribute searches, and how to utilize both granted patent applications and recent patent applications to gain in-depth insights into cybersecurity. Additionally, we showed that various metrics can be used to evaluate firms relative to one another.

The technology landscape analysis is a critical tool in competitive intelligence. To maximize its effectiveness, it must be applied to address a well-defined question with domain experts. Depending on the objective, this analysis can help identify key players, uncover potential opportunities for R&D partnerships, and helps in technological mergers and acquisitions (M&A) decisions. **metis** analytica is here to assist you in conducting a comprehensive technological landscape analysis.

Our analysis reveals that the cybersecurity sector has experienced a significant surge, evidenced by a sharp rise in patent activity. The United States leads in both patent filings and publications, cementing its role as a global innovator in this space, with Israel emerging as a strong second. Patent citation analysis highlights Bank of America as a pivotal node, showcasing how cybersecurity innovation extends beyond traditional ICT firms to sectors such as finance. Among pure players, FireEye stands out with its number of patents and its position in the citation network, underscoring its importance. Using recent patent applications from the period 2020-2023, we identified Proofpoint, Expel, Wiz, and Bitsight as potential new key players in the cybersecurity patent landscape.

Mergers and acquisitions (M&A), though complex, benefit significantly from patent-based metrics like technological diversity, complementarity, and similarity. These metrics provide actionable insights, aiding firms in identifying strategic targets and optimizing M&A outcomes. Integrating citation network analysis further enhances this process by pinpointing firms with critical technological positions and minimizing integration risks. The same approach can be used to anticipate possible strategic moves that competitors might take.

Patents are invaluable tools for assessing a firm's technological capabilities. By leveraging various analytical techniques, organizations can gain insights that provide a competitive edge. This report merely scratches the surface; to maximize the effectiveness of technology landscape analysis, a well-defined question is essential. By aligning strategic objectives with patent evaluations, firms can enhance innovation-driven growth.

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

Cassiman, B., Colombo, M. G., Garrone, P., & Veugelers, R. (2005). The impact of M&A on the R&D process [00487]. *Research Policy*, *34*(2), 195–220. https://doi.org/10/b8jwph

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 cyberattacks (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

McInnes, L., Healy, J., & Melville, J. (2020). UMAP: Uniform Manifold Approximation and Projection for Dimension Reduction [arXiv:1802.03426 [cs, stat]]. https://doi.org/10.48550/arXiv.1802.03426

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

Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V., Vanderplas, J., Passos, A., Cournapeau, D., Brucher, M., Perrot, M., & Duchesnay, E. (2011). Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research*, *12*, 2825–2830.

Renneboog, L., & Vansteenkiste, C. (2019). Failure and success in mergers and acquisitions. *Journal of Corporate Finance*, *58*, 650–699. https://doi.org/10.1016/j.jcorpfin.2019.07.010

Shafique, M., & Hagedoorn, J. (2022). Look at U: Technological scope of the acquirer, technological complementarity with the target, and post-acquisition R&D output. *Technovation*, *115*, 102533. https://doi.org/10.1016/j.technovation.2022.102533

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

Trellix. (2021). Combination of McAfee enterprise and FireEye complete [Accessed: 2024-12-15]. https://www.trellix.com/news/press-releases/combination-of-mcafee-enterprise-and-fireeye-complete/

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.

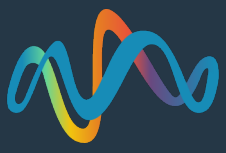
Yang, Y. Y., Akers, L., Yang, C. B., Klose, T., & Pavlek, S. (2010). Enhancing patent landscape analysis with visualization output. *World Patent Information*, *32*(3), 203–220. https://doi.org/10.1016/j.wpi.2009.12.006

Author

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

Important Notice

Version Disclaimer: This report is **Version 1**, prepared in **January 2025**. 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