https://doi.org/10.58086/0myf-4a66

BIBLIOMETRIC STUDY ON THE IMPORTANCE OF ENDPOINT SECURITY IN COMPANIES

João Gonçalves[1]

Mário Lousã[2]

José Morais[3]

Abstract

This bibliometric study addresses the importance of endpoint security in companies, considering the growing use of information technologies, both in business and personal use. It highlights the need to protect endpoints such as computers, mobile devices, servers, and IoT devices. Endpoint security encompasses measures such as monitoring the files and binaries on and running on the machine using antivirus, data encryption, and threat detection solutions. The literature review highlights the importance of terminology and best practices, highlighting the application of graph-based approaches to strengthen security in medical information networks. Tools such as EDR are cited as essential, especially for small and medium-sized companies. The study emphasizes the importance of business continuity in the face of cyber threats, highlighting the role of artificial intelligence, machine learning, and frameworks. It takes a bibliometric approach, using a specific database to collect bibliometric data on scientific publications published between 2017 and 2023. As a basis for the study, the words “cybersecurity”, “endpoint security”, “business continuity”, and “business” were used. Various analyses of bibliometric results are also presented, including the number of publications by type of document, the scientific journals with the highest number of publications, the countries with the highest number of publications, the number of publications per author, the most cited articles, and the occurrence of identified keywords.

Keywords: Endpoint Security; Business continuity; Vulnerability; Risk; Security threats.

ESTUDO BIBLIOMÉTRICO SOBRE A IMPORTÂNCIA DA SEGURANÇA DE ENDPOINT NAS EMPRESAS

Resumo

Este estudo bibliométrico aborda a importância da segurança de endpoint nas empresas, considerando o crescente uso de tecnologias de informação, tanto no uso empresarial quanto pessoal. Ele destaca a necessidade de proteger terminais como computadores, dispositivos móveis, servidores e dispositivos IoT. A segurança de endpoint abrange medidas como monitoramento de arquivos e binários e em

[1] ISPGaya /Instituto Superior Politécnico Gaya, Portugal

[2] CID ISPGAYA; ISPGaya /Instituto Superior Politécnico Gaya, Portugal

[3] CEOSP.PP; ISPGaya /Instituto Superior Politécnico Gaya, Portugal

execução na máquina usando antivírus, criptografia de dados e soluções de detecção de ameaças. A revisão da literatura destaca a importância da terminologia e das melhores práticas, destacando a aplicação de abordagens baseadas em gráficos para fortalecer a segurança nas redes de informação médica. Ferramentas como o EDR são citadas como essenciais, principalmente para pequenas e médias empresas. O estudo enfatiza a importância da continuidade dos negócios diante das ameaças cibernéticas, destacando o papel da inteligência artificial, do aprendizado de máquina e dos frameworks. Adota uma abordagem bibliométrica, utilizando uma base de dados específica para coletar dados bibliométricos sobre publicações científicas publicadas entre 2017 e 2023. Como base para o estudo, foram utilizadas as palavras "cibersegurança", "endpoint security", "businesscontinuity" e "business" foram usados. São também apresentadas diversas análises de resultados bibliométricos, incluindo o número de publicações por tipo de documento, as revistas científicas com maior número de publicações, os países com maior número de publicações, o número de publicações por autor, os artigos mais citados, e a ocorrência de palavras-chave identificadas.

Palavras-chave: Segurança de Endpoint; Continuidade dos negócios; Vulnerabilidade; Risco; Ameaças à segurança.

Introduction

The growing use of information technology has made endpoint security a major concern for companies. Also, with the increase in devices connected to the internet and the rise in cyber threats, it has become essential to guarantee the security of endpoints on a company's network (Shao et al., 2023). Endpoint security encompasses a series of measures designed to protect the various entry points into a network, such as computers, mobile devices, servers, and IoT devices. As companies continue to embrace digital transformation in their businesses, the need to apply robust security measures to their endpoints becomes essential to safeguard sensitive data and ensure business continuity in whatever area of the business it falls under (Yevseiev et al., 2023). With the help of antivirus installed directly on the endpoints, data encryption software, IPS (Intrusion Prevention Systems), Endpoint Threat Detection and Response solution, and NGFW (Next Generation Firewall), greater security of an organization's endpoints is possible, ensuring a greater likelihood of a minimum of false positives or false negatives (Chochliouros et al., 2021).

In this bibliometric study, the main objective is to explore the importance of endpoint security in companies, based on several bibliographic analyses carried out in various scientific articles related to this topic. To this end, a review was carried out of the existing literature on endpoint security, business continuity, and cybersecurity. The number of publications by type of document, the scientific journals with the highest number of publications, the countries with the highest number of publications, the number of publications per author, the most cited articles, and the occurrence of identified keywords were analyzed.

1. Literature review

1.1. Endpoint Security

The endpoint security approach refers to the act of protecting the devices used by end users, such as computers, mobile devices, servers, and IoT devices, from potential security threats. It involves implementing measures to protect these devices from unauthorized access, data breaches, malware, and other cyber threats (Sharma et al., 2021). The history of endpoint security goes back to the early days of network computing, when the priority was to protect endpoints connected to the network from external attacks. As technology has evolved, the number of mobile devices and the growing sophistication of cyber threats have increased significantly, causing this concept to evolve to encompass a wide range of security measures aimed at protecting end users' devices and the data they contain (Sarker, 2023). The importance of terminology and good practices in the general IT field was highlighted by Coravos et al. (2020). It is relevant for endpoint security, since the terminology used in this field is crucial for understanding and applying effective security measures.

It is also essential to guarantee the security of endpoints, as this is something with a high level of criticality within cybersecurity, especially in the context of emerging technologies such as the Internet of Things (IoT) and cyber-physical systems (CPS). The increasing complexity and connectivity of endpoints has raised some concerns about the vulnerability of these devices to cyber threats (Ibrahim et al., 2022). According to Angel (2022), the application of graph-based approaches has been proposed to strengthen the security of medical information networks against cyber threats, demonstrating the potential of these methods to significantly improve the performance and capacity of security operations teams. On the other hand, the use of EDR (Endpoint Detection and Response) tools has been referred to as an essential component of information security policies and strategies, particularly in small and medium-sized companies (Noronha et al., 2022). Companies can adopt some approaches combined with some physical tools and equipment to ensure greater endpoint protection, such as EDR, antivirus, NGFW, Domain Name System (DNS) protection and email gateway security (Houhamdi & Athamena, 2021).

1.2. Business continuity

Business continuity is a critical aspect for companies to ensure that their operations are not interrupted, especially by cyber threats caused by malicious agents (Zheng & Omote, 2022).

Based on the literature review on this concept, the importance of assessing the robustness of computer systems to prevent and mitigate risks and computer attacks is emphasized, highlighting the need to implement and apply effective business continuity measures (Kafi & Akter, 2023). Some of these measures involve creating and applying incident response plans to protect financial information and maintain business continuity. Additionally, Simonovich (2020) presents the challenges that companies face in defending their assets, indicating the need for sustainable cybersecurity practices to achieve business continuity in an organization.

In the context of cybersecurity, Sarker (2023) stresses the important role of artificial intelligence (AI), particularly machine learning, in recognizing patterns and predicting malicious activity to avoid disruption and ensure business continuity. Furthermore, George et al. (2021) emphasizes the need for companies, regardless of their involvement in cybersecurity, to adopt sophisticated detection and response mechanisms so that their operations and business continuity are safeguarded.

The evolving nature of cybersecurity threats in general, such as ransomware, malware, and social engineering, requires proactive recovery measures and continuous readiness.

This highlights the importance of recovering from a ransomware attack and planning considerations to mitigate downtime and ensure business continuity (Chen et al., 2021). Rizvi et al. (2022) also stresses the need for progressive frameworks and machine learning techniques to effectively classify and detect malware, especially in zero-day attacks, contributing to the overall goal of maintaining business continuity.

It should also be noted that with the exponential increase in employees working remotely, new challenges have been introduced, as Škiljić (2020) discusses Croatia's response to the increase in cyber threats in the context of remote work, highlighting the risks to business continuity. By implementing real-time monitoring of network traffic in these companies, files that possibly contain viruses or whose corresponding hash is unknown, activities in modern network environments gain a more robust layer of protection, providing not only reactive action on the part of information security analysts but also proactive (Kebande et al., 2021).

1.3. Vulnerability

Vulnerability in the context of cybersecurity refers to a weakness in computer systems, networks, or applications that can be exploited by malicious agents, thus compromising the confidentiality, integrity, or availability of information and resources (Walker-Roberts et al., 2020). These vulnerabilities can come from various sources, such as software failures, incorrect configurations of computer programs, network equipment, or even computers and human errors, thus posing significant risks to the security of organizations and employees themselves (Victor et al., 2023). The constant increase in the use of IoT devices within companies has made them an attractive target for hackers, who are actively trying to exploit these vulnerabilities to launch attacks in a wide variety of ways and techniques.

To reduce the risk of a company being the target of a cyber-attack because its systems and software contain vulnerabilities, various approaches and technologies have been developed. Machine learning, in particular AI based on machine learning, has shown promise in recognizing patterns and predicting potential malicious activities, thus helping to prevent and detect threats to the proper functioning of systems (Mandal et al., 2021). Additionally, Jia et al. (2022) points out that another measure has been developed that will contribute to advances in cybersecurity. Specifically, the development of lightweight DDoS (Distributed Denial-of-Service) schemes in software-defined networking (SDN) contexts has demonstrated reduced false alarm rates, thus improving the ability to effectively identify and respond to DDoS attacks.

In the event of a computer attack, such as ransomware, recovery and imaging operations are crucial. Learning from these incidents can improve planning to prevent and mitigate future attacks, highlighting the importance of preparedness and response strategies. In addition, the robustness of malware detection models is a critical area of study, since evaluating the resilience of these models is essential to ensuring their effectiveness in real-life scenarios (Shahhosseini et al., 2022).

1.4. Endpoint Security, Business Continuity and Vulnerability

Within the area of cybersecurity, the concepts of Endpoint Security, Business Continuity, and Vulnerability complement each other and are all related, although they are different. Endpoint security plays a fundamental role in a company's business continuity. If endpoints are compromised due to vulnerabilities in systems or software, the normal operation of the organization can be interrupted and even incur losses for the company. Therefore, ensuring the security of these endpoints by identifying and correcting known vulnerabilities is a proactive measure to maintain continuity of operations (Ayub et al., 2023).

Table 1 presents descriptions of the three concepts of Endpoint Security, business continuity and vulnerability.

Table 1
Concepts of Endpoint Security, Business Continuity and Vulnerability

Concept	Description	Authors
Endpoint Security	Described as the approach of protecting the various endpoints, such as computers, mobile devices, servers, and IoT devices, that are connected to a network. It involves protecting these endpoints from unauthorized access, data breaches, ransomware attacks, and other threats. Endpoint security solutions are crucial for organizations to protect the integrity, confidentiality, and availability of the network and data.	Gao et al. (2021) Goldsack et al. (2020) Heino et al. (2022)
Business Continuity	Refers to the strategic and tactical capacity of an organization to ensure the continuity of its operations during and after a catastrophe or any other significant disruption. It involves a proactive plan to ensure that critical operations continue to function, even after serious security incidents or disasters have occurred, and is considered a fundamental aspect of cyber resilience. This concept becomes important within cybersecurity since organizations need to guarantee the continuity of their operations even in the face of cyber threats and attacks.	Bolpagni (2022) Teichmann et al. (2023) Yang et al. (2022)
Vulnerability	Described as a weakness in a computer system or program that can be exploited by malicious agents to compromise the confidentiality, integrity, or availability of the systems or data processed. Vulnerabilities can come in many forms, including software, hardware, and human factors. They can also be exploited through different attack vectors, such as malware, phishing, social engineering, and DDoS (Distributed Denial-of-Service). Identifying and mitigating vulnerabilities is crucial to maintaining system security and preventing unauthorized access and data breaches.	Baiardi & Tonelli (2021) Taddeo (2019) Tan et al. (2020)

2. Methodology

Bibliometric analysis is an important method for assessing the impact and influence of scientific articles in a specific field. It involves the quantitative analysis of publications, including citation counts, authorship patterns, and journal impact factors. This approach provides information on the productivity and impact of researchers and the evolution of scientific knowledge in each discipline. For a concise analysis, bibliometric data is usually collected from databases such as The Lens, Scopus, or the Web of Science (Aapro et al., 2020).

Taking the theme of this article as a reference, a series of research questions were posed:

- RQ1: How has the topic of endpoint security evolved in academic research over the last six years?
- RQ2: Who are the main authors, countries, and articles in scientific publications related to the topic of endpoint security?
- RQ3: What are the main areas of research in the field of endpoint security?

For this bibliometric study, the PRISMA method was used, which consists of a verification of 27 items and a four-phase flowchart, thus helping to guide the researcher through the systematic review process, from the definition of relevant studies to the final inclusion of studies (Zhang et al., 2022).

The database "The Lens" was used, which is widely used as a cost-free platform with millions of patents and scientific articles in the most varied fields of study. This data can then be exported so that it can be processed as the researcher sees fit (The Lens, n.d.). The keywords used in “The Lens” as search categories were “cybersecurity”, “endpoint security”, “business continuity”, and “business”.

With these search criteria, a total of 158 publications were obtained. However, to further delimit the desired publications, with the aim of making them current, some filters were used. In particular, the publication dates of the articles were limited to 2017–2023, and only articles, books, book chapters, and conferences were considered. With these filters, 141 publications were obtained.

To aid this research, the Boolean operators "AND" and "OR" were used strategically with the search terms mentioned in Table 2 (2nd step). Several graphs generated by "The Lens" platform were extracted and included in this document for a more in-depth bibliometric study. Version 1.6.20 of the "VOSviewer" software was also used to carry out the analysis and visualization of the most used terms, referring to the bibliometric data extracted. The following table shows the methodology used in this bibliographical study, in which the PRISMA method was used.

Table 2.
PRISMA methodology applied to bibliometric studies

1st step	Select the database	The Lens
2nd step	Define the search term(s)	cybersecurity AND (endpoint AND (security AND (business AND (continuity OR business))))
3rd step	Specify the search criteria	Time period: 2017-2023; Type of publications: articles, books, book chapters, conference: Field of study: cybersecurity, business.
4th step	Select analysis software	VOSviewer
5th step	Present and analyze the results	Analysis resulting from the results of the bibliometric data collected, regarding scientific publications, authors, number of citations, articles, and keywords.
6th step	Summarizing the results	Based on the results of the graphs and tables, summarize and present conclusions.

3. Bibliometric analysis

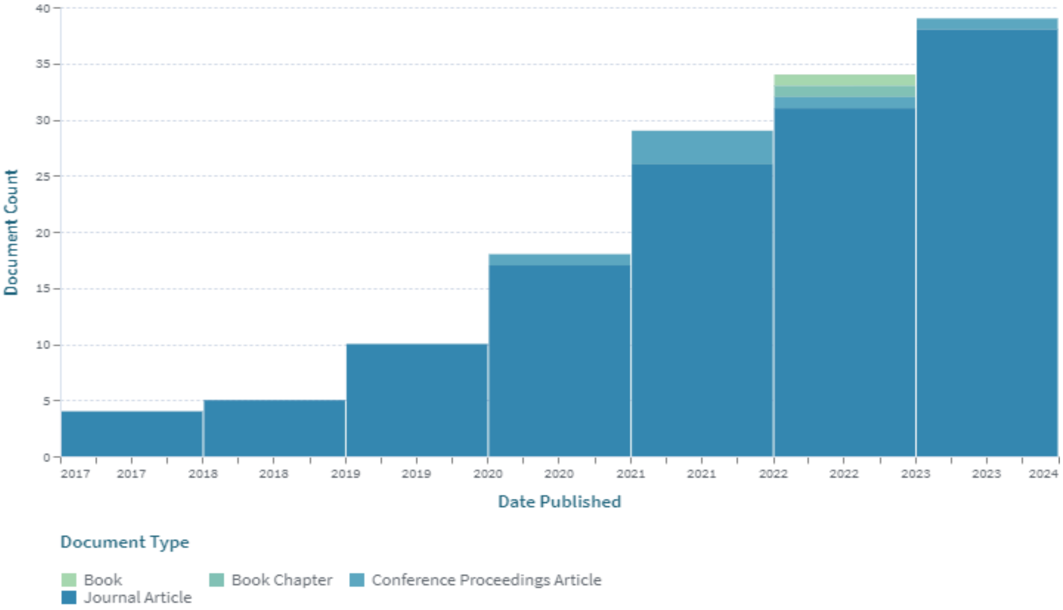
3.1. Evolution of academic research over the last six years on the topic of endpoint security (RQ1)

In the six-year period between 2017 and 2023, 141 publications were recorded. According to Figure 1, there has been an increase in the number of publications on the topic’s “cybersecurity”, “endpoint security”, “business continuity”, and “business” over the past six years, especially between 2020 and

2021. This period coincided with the increase in cyber-attacks on companies around the world, thus creating the need to publish in this area (Wan et al., 2022).

Figure 1

Number of publications by type of document

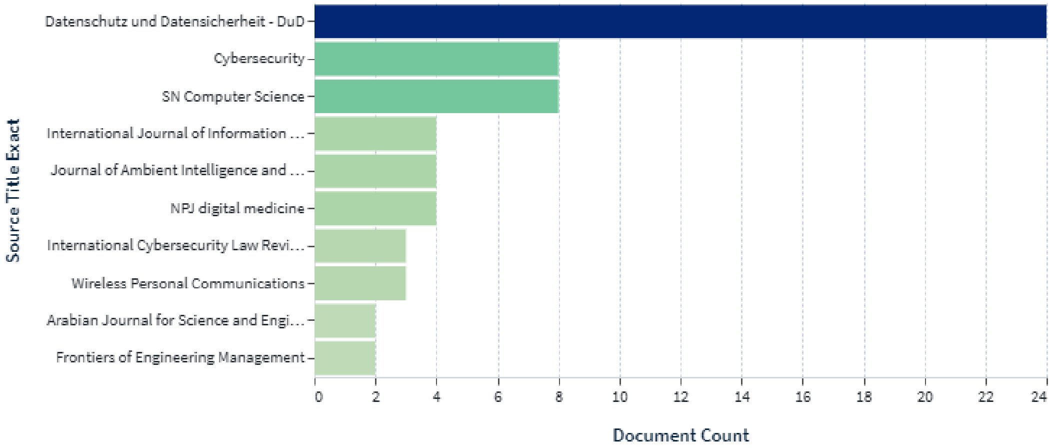


3.2. Main authors, countries, and articles in scientific publications related to the topic of endpoint security (RQ2)

Figure 2 presents the 10 scientific journals with the most publications, with "Datenschutz und Datensicherheit - DuD" leading the list with 24 publications.

Figure 2

10 Journals with the most publications



Among the 10 countries with the highest number of publications of scientific material, the United States appears with 18 publications, followed by India with 17 (cf. Table 3).

Table 3
Countries with the most publications

Country	Number of publications
United States of America	18
India	17
China	10
United Kingdom	10
Italy	7
Saudi Arabia	7
Australia	6
Spain	5
Spain	4
Ireland	4

Figure 3 shows the 10 authors with the most publications, with no major difference between them. The author with the most publications under the defined terms is Andrea Coravos, with three from the Harvard-MIT Center for Regulatory Science, associated with digital medicine. The following six authors have two publications, showing that there is no author or authors who stand out with many publications in this area.

Figure 3
Number of publications per author

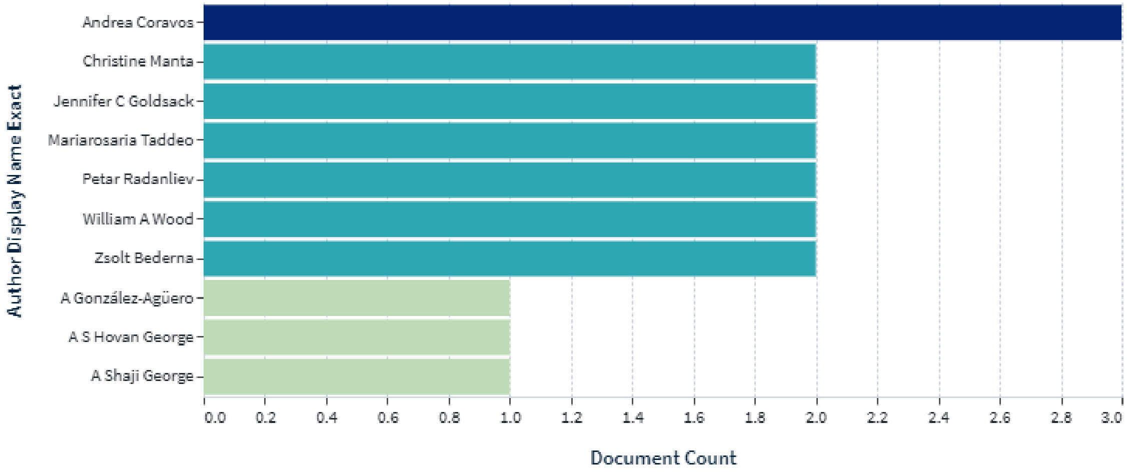


Table 4 presents the data corresponding to the 10 publications with the highest number of citations. The first article on the list was cited 217 times and published in 2020. The second and third articles on the list were cited 181 and 140 times, respectively. Next, the fifth most cited publication has 73 citations, almost half compared to the previous publication. It appears that the three articles with the highest number of citations are associated with the health area, more specifically digital medicine.

Table 4.
10 most cited articles

Title	DOI	Year of publication	Number of times cited
Verification, analytical validation, and clinical validation (V3): the foundation of determining fit-for-purpose for Biometric Monitoring Technologies (BioMeTs)	10.1038/s41746-020-0260-4	2020	217
Developing and adopting safe and effective digital biomarkers to improve patient outcomes	10.1038/s41746-019-0090-4	2019	181
Digital health for optimal supportive care in oncology: benefits, limits, and future perspectives	10.1007/s00520-020-05539-1	2020	140
Internet of Things: information security challenges and solutions	10.1007/s10586-018-2823-6	2018	73
A Systematic Review on AI-based Proctoring Systems: Past, Present and Future	10.1007/s10639-021-10597-x	2021	56
Modernizing and designing evaluation frameworks for connected sensor technologies in medicine	10.1038/s41746-020-0237-3	2020	54
Threats on the horizon: understanding security threats in the era of cyberphysical systems	10.1007/s11227-019-03028-9	2019	46
A Review on the Security of the Internet of Things: Challenges and Solutions	10.1007/s11277-021-08348-9	2021	39
Self-Service Cybersecurity Monitoring as Enabler for DevSecOps	10.1109/access.2019.2930000	2019	34
Provenance-Aware Knowledge Representation: A Survey of Data Models and Contextualized Knowledge Graphs	10.1007/s41019-020-00118-0	2020	33

3.3. Main areas of research in the field of endpoint security (RQ3)

Analyzing the keywords of scientific publications is important to understand the focus and scope of the work. By examining the keywords used by authors, researchers can gain insights into key themes, concepts, and areas of interest in each field of study. According to Ghadi et al. (2021), this process can help find and identify relevant literature, understand current trends, and establish connections between different pieces of research.

Based on the collection of bibliometric data and its processing in the "VOSviewer" software, 12 keywords cited by the authors of the analyzed publications were identified, as can be seen in Figure 4. The most frequent keywords were "security" with 33 occurrences and "attack" with 32. Considering the theme of this study and the two most cited keywords, these terms are linked to the scope of the study since the importance of endpoint security is intrinsically linked to security and attack, because when trying to defend or protect something, there is a risk of some type of attack (Rao & Deebak, 2023).

As a result of analyzing the occurrences of keywords, three clusters were identified, as shown in Table 5 and Figure 4.

Figure 4.
Keyword occurrences

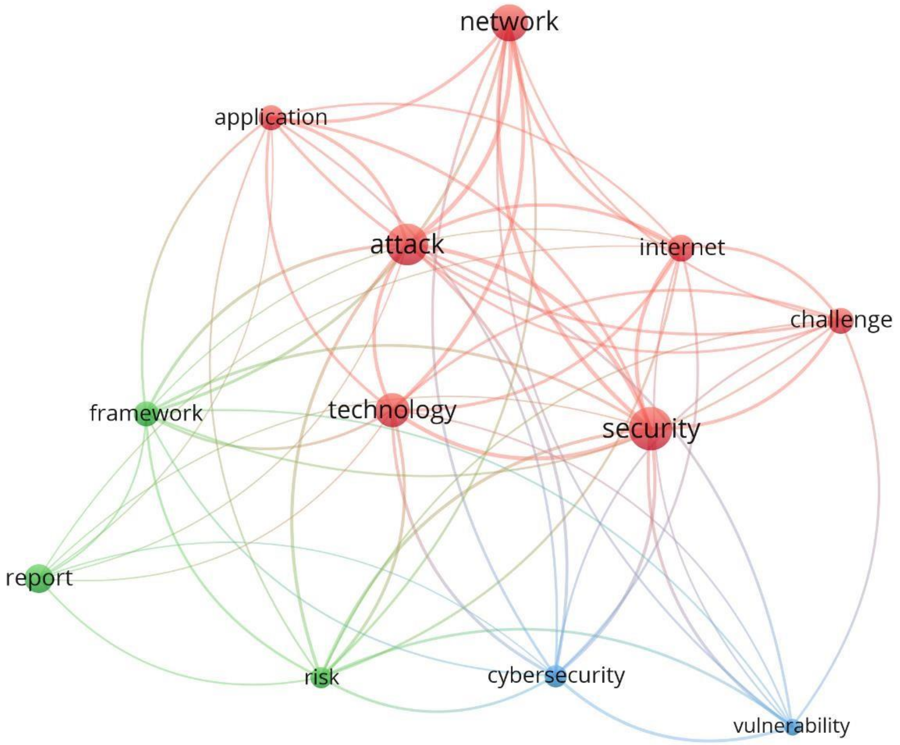


Table 5
Keywords for each Cluster

Cluster	Keywords
Red	"application", "attack", "challenge", "internet", "network", "security", "technology"
Green	"framework", "report", "risk"
Blue	"cybersecurity", "vulnerability"

3.3.1. Red cluster

In this cluster, the keywords "application", "attack", "challenge", "internet", "network", "security" and "technology" were identified, which are connected and important in the role of endpoint security in organizations.

The keyword "application" is widely discussed in the context of semantic web applications, provenance, and knowledge representation. Applications play a very active role in endpoint security (Sikos & Philp, 2020).

Regarding "attack", several articles delve into different aspects of cyber-attacks, including strategies for attacking precision timing protocols, attacks on SCADA systems, and detecting zero-day attacks (Alghamdi & Schukat, 2021).

The “challenge” is addressed in the context of cybersecurity considerations for the health area, robotic surgery, IoT applications, and the ethical challenges of AI applications in cybersecurity, which highlight the challenges posed by cybersecurity threats in various domains (Bhavsar et al., 2023).

"Internet" and "network" are interconnected keywords discussed in the context of IoT applications, cloud-based access control policies, and the design of dynamic, self-adaptive systems for predictive risk analysis in cyberspace (Nagajayanthi, 2022).

Regarding “security”, this is a central theme in several publications, including those that focus on precision timing protocol attack strategies, cybersecurity monitoring, and strengthening the continuous integration workflow (Elhag et al., 2022).

The keyword "technology" is addressed in the context of extracting knowledge from unstructured information, antivirus applications for the detection of JAR malware, and the creation of a dynamic and self-adaptive system for the predictive analysis of cyber risk (Takko et al., 2023). These articles highlight the role of technology in knowledge extraction, malware detection, and predictive risk analysis in cybersecurity.

3.3.2. Green cluster

In the green cluster, the keywords “framework”, “report”, and “risk” are mentioned. "Framework" has been widely mentioned in the literature. Several frameworks have been proposed, particularly to analyze the predictability of cyber risks in critical environments where a cyber-attack must be avoided at all costs (Krishnan et al., 2023).

The keyword “report” is also significant in the context of cybersecurity in the sense that endpoint security incident reports and vulnerability reports are important and fundamental in this area. (Radanliev et al., 2020).

“Risk” is a key word in this area of cybersecurity, as it is essential to identify and plan the mitigation of risks associated, in this case, with endpoints (Aghamohammadpour et al., 2023).

3.3.3. Blue Cluster

The blue cluster includes the keywords are “cybersecurity” and “vulnerability”.

“Cybersecurity” refers to the protection of information technology assets against threats that may compromise their confidentiality, integrity, and availability. According to Diaz et al. (2019), with increasing dependence on technology, several sectors, including healthcare, face new risks, making cybersecurity considerations essential.

“Vulnerability” is a key concept in this cybersecurity context, particularly regarding detecting and mitigating potential weaknesses in systems. One of the main objectives of this area and the theme presented in this study is to try to reduce existing vulnerabilities in physical systems and devices. One way to do this is to update the operating system versions to the most recent and restrict the user to certain access and functionalities of the software or the system itself.

4. Conclusions

The bibliometric study carried out on the importance of endpoint security in companies provided a comprehensive view of trends, challenges, and advances in this crucial area of cybersecurity. The growing digital transformation of companies and the increase in cyber threats reinforce the importance of endpoint security. Protecting the various entry points into the network, such as computers, mobile devices, and servers, is crucial to safeguarding sensitive data and ensuring the continuity of the company's business.

In this study, the literature review highlights the diversity of security measures, from antivirus to advanced solutions such as EDR, IPS, and NGFW. The combination of these measures helps strengthen endpoint security by minimizing false positives and negatives. Business continuity stands out as one of the key points in this area. Incident response plans, the adoption of artificial intelligence and machine learning, and the need for sustainable cybersecurity practices are measures highlighted to help ensure operational resilience.

Endpoint security, business continuity. and vulnerability, although distinct concepts, are interlinked in cybersecurity. Endpoint security plays a crucial role in business continuity, and the identification and proactive correction of vulnerabilities are fundamental to avoiding interruptions in operations.

The bibliometric analysis carried out showed an increase in the number of publications over the last six years, reflecting the importance of endpoint security in several areas (e.g., medicine, industry, and commerce) to guarantee business continuity. Countries such as the United States of America, India, and China have led in terms of the number of applications in this area.

As with any study, this research has some limitations that need to be recognized. However, they may represent a starting point for future work. The search terms, the area of the most cited articles, and the number of articles themselves can be considered limitations of this bibliometric study.

Taking the present study as a starting point, new lines of investigation can be outlined. For example, exploring detection strategies and evaluating the effectiveness of endpoint security practices. Another line of investigation may focus on security techniques and mechanisms, depending on the operating systems and the different types of endpoint devices used, to guarantee business continuity.

Bibliographic references

Aapro, M., Bossi, P., Dasari, A., Fallowfield, L., Gascón, P., Geller, M., Jordan, K., Kim, J., Martin, K., & Porzig, S. (2020). Digital health for optimal supportive care in oncology: Benefits, limits, and future perspectives. *Supportive Care in Cancer*, *28*(10), 4589–4612. https://doi.org/10.1007/s00520-020-05539-1

Aghamohammadpour, A., Mahdipour, E., & Attarzadeh, I. (2023). Architecting threat hunting system based on the DODAF framework. *The Journal of Supercomputing*, *79*(4), 4215–4242. https://doi.org/10.1007/s11227-022-04808-6

Alghamdi, W., & Schukat, M. (2021). Precision time protocol attack strategies and their resistance to existing security extensions. *Cybersecurity*, *4*(1), 12. https://doi.org/10.1186/s42400-021-00080-y

Angel, D. (2022). Application of graph domination to defend medical information networks against cyber threats. *Journal of Ambient Intelligence and Humanized Computing*, *13*(8), 3765–3770. https://doi.org/10.1007/s12652-022-03730-2

Ayub, M., Lajam, O., Alnajim, A., & Niazi, M. (2023). Use of Machine Learning for Web Denial-of-Service Attacks: A Multivocal Literature Review. *Arabian Journal for Science and Engineering*, *48*(8), 9559–9574. https://doi.org/10.1007/s13369-022-07517-7

Baiardi, F., & Tonelli, F. (2021). Twin Based Continuous Patching To Minimize Cyber Risk. *European Journal for Security Research*, *6*(2), 211–227. https://doi.org/10.1007/s41125-022-00079-7

Bhavsar, M., Roy, K., Kelly, J., & Olusola, O. (2023). Anomaly-based intrusion detection system for IoT application. *Discover Internet of Things*, *3*(1), 5. https://doi.org/10.1007/s43926-023-00034-5

Bolpagni, M. (2022). Cyber risk index: A socio-technical composite index for assessing risk of cyber attacks with negative outcome. *Quality & Quantity*, *56*(3), 1643–1659. https://doi.org/10.1007/s11135-021-01199-3

Chen, P.-H., Bodak, R., & Gandhi, N. S. (2021). Ransomware Recovery and Imaging Operations: Lessons Learned and Planning Considerations. *Journal of Digital Imaging*, *34*(3), 731–740. https://doi.org/10.1007/s10278-021-00466-x

Chochliouros, I. P., Spiliopoulou, A. S., Kostopoulos, A., Kourtis, M.-A., Lazaridis, P.I., Zaharis, Z. D., & Prasad, N. R. (2021). Security Threat Analysis of the 5G ESSENCE Platform. *Wireless Personal Communications*, *120*(3), 2409–2426. https://doi.org/10.1007/s11277-021-08554-5

Coravos, A., Doerr, M., Goldsack, J., Manta, C., Shervey, M., Woods, B., & Wood, W. A. (2020). Modernizing and designing evaluation frameworks for connected sensor technologies in medicine. *Npj Digital Medicine*, *3*(1), 37. https://doi.org/10.1038/s41746-020-0237-3

Diaz, J., Perez, J. E., Lopez-Pena, M. A., Mena, G. A., & Yague, A. (2019). SelfService Cybersecurity Monitoring as Enabler for DevSecOps. *IEEE Access*, *7*, 100283–100295. https://doi.org/10.1109/ACCESS.2019.2930000

Elhag, S., Alghamdi, A. M., & Al-Shomrani, N. A. (2022). Toward an Improved Security Performance of Industrial Internet of Things Systems. *SN Computer Science*, *4*(2), 131. https://doi.org/10.1007/s42979-022-01566-3

Gao, R., Li, S., Gao, Y., & Guo, R. (2021). A lightweight cryptographic algorithm for the transmission of images from road environments in self-driving. *Cybersecurity*, *4*(1), 3. https://doi.org/10.1186/s42400-020-00066-2

George, A. S., George, A. S. H., Baskar, T., & Pandey, D. (2021). XDR: The Evolution of Endpoint Security Solutions - Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), 8*(1). https://doi.org/10.48175/IJARSCT-1888

Ghadi, M., Sali, Á., Szalay, Z., & Török, Á. (2021). A new methodology for analyzing vehicle network topologies for critical hacking. *Journal of Ambient Intelligence and Humanized Computing*, *12*(7), 7923–7934. https://doi.org/10.1007/s12652-020-02522-w

Goldsack, J. C., Coravos, A., Bakker, J. P., Bent, B., Dowling, A. V., Fitzer-Attas, C., Godfrey, A., Godino, J. G., Gujar, N., Izmailova, E., Manta, C., Peterson, B., Vandendriessche, B., Wood, W. A., Wang, K. W., & Dunn, J. (2020). Verification, analytical validation, and clinical validation (V3): The foundation of determining fit-for-purpose for Biometric Monitoring Technologies (BioMeTs). *Npj Digital Medicine*, *3*(1), 55. https://doi.org/10.1038/s41746-020-0260-4

Heino, J., Hakkala, A., & Virtanen, S. (2022). Study of methods for endpoint aware inspection in a next generation firewall. *Cybersecurity*, *5*(1), 25. https://doi.org/10.1186/s42400-022-00127-8

Houhamdi, Z., & Athamena, B. (2021). IoT Framework for Effective and Fine–Grain Access Control. *2021 8th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)* (pp. 1-6). https://doi.org/10.1109/IOTSMS53705.2021.9704977

Ibrahim, R. F., Abu Al-Haija, Q., & Ahmad, A. (2022). DDoS Attack Prevention for Internet of Thing Devices Using Ethereum Blockchain Technology. *Sensors*, *22*(18), 6806. https://doi.org/10.3390/s22186806

Jia, K., Liu, C., Liu, Q., Wang, J., Liu, J., & Liu, F. (2022). A lightweight DDoS detection scheme under SDN context. *Cybersecurity*, *5*(1), 27. https://doi.org/10.1186/s42400-022-00128-7

Kafi, M. A., & Akter, N. (2023). Securing Financial Information in the Digital Realm: Case Studies in Cybersecurity for Accounting Data Protection. *American Journal of Trade and Policy*, *10*(1), 15–26. https://doi.org/10.18034/ajtp.v10i1.659

Kebande, V. R., Karie, N. M., & Ikuesan, R. A. (2021). Real-time monitoring as a supplementary security component of vigilantism in modern network environments. *International Journal of Information Technology*, *13*(1), 5–17. https://doi.org/10.1007/s41870-020-00585-8

Krishnan, P., Jain, K., Aldweesh, A., Prabu, P., & Buyya, R. (2023). OpenStackDP: A scalable network security framework for SDN-based OpenStack cloud infrastructure. *Journal of Cloud Computing*, *12*(1), 26. https://doi.org/10.1186/s13677-023-00406-w

Mandal, S., Khan, D. A., & Jain, S. (2021). Cloud-Based Zero Trust Access Control Policy: An Approach to Support Work-From-Home Driven by COVID-19 Pandemic. *New Generation Computing*, *39*(3–4), 599–622. https://doi.org/10.1007/s00354-021-00130-6

Nagajayanthi, B. (2022). Decades of Internet of Things Towards Twenty-first Century: A Research-Based Introspective. *Wireless Personal Communications*, *123*(4), 3661–3697. https://doi.org/10.1007/s11277-021-09308-z

Noronha, G.M.S., Silva, A. A., & Pinheiro, J. S. S. (2022). Information Security Policies and Strategies and Practices Adopted in It: the Importance of Consultancy in Small and Medium-sized Companies. *International Journal of Advanced Research*, *10*(11), 779–786. https://doi.org/10.21474/IJAR01/15730

Radanliev, P., De Roure, D., Page, K., Van Kleek, M., Santos, O., Maddox, L., Burnap, P., Anthi, E., & Maple, C. (2020). Design of a dynamic and self-adapting system, supported with artificial intelligence, machine learning and real-time intelligence for predictive cyber risk analytics in extreme environments – cyber risk in the colonisation of Mars. *Safety in Extreme Environments*, *2*(3), 219–230. https://doi.org/10.1007/s42797-021-00025-1

Rao, P. M., & Deebak, B. D. (2023). Security and privacy issues in smart cities/industries: Technologies, applications, and challenges. *Journal of Ambient Intelligence and Humanized Computing*, *14*(8), 10517–10553. https://doi.org/10.1007/s12652-022-03707-1

Rizvi, S. K. J., Aslam, W., Shahzad, M., Saleem, S., & Fraz, M. M. (2022). PROUDMAL: Static analysis-based progressive framework for deep unsupervised malware classification of windows portable executable. *Complex & Intelligent Systems*, *8*(1), 673–685. https://doi.org/10.1007/s40747-021-00560-1

Sarker, I. H. (2023). Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects. *Annals of Data Science*, *10*(6), 1473–1498. https://doi.org/10.1007/s40745-022-00444-2

Shahhosseini, M., Mashayekhi, H., & Rezvani, M. (2022). A Deep Learning Approach for Botnet Detection Using Raw Network Traffic Data. *Journal of Network and Systems Management*, *30*(3), 44. https://doi.org/10.1007/s10922-022-09655-7

Shao, X., Xie, L., Li, C., & Wang, Z. (2023). A Study on Networked Industrial Robots in Smart Manufacturing: Vulnerabilities, Data Integrity Attacks and Countermeasures. *Journal of Intelligent & Robotic Systems*, *109*(3), 60. https://doi.org/10.1007/s10846-023-01984-2

Sharma, R., Dangi, S., & Mishra, P. (2021). A Comprehensive Review on Encryption based Open Source Cyber Security Tools. *2021 6th International Conference on Signal Processing, Computing and Control (ISPCC)*, 614–619. https://doi.org/10.1109/ISPCC53510.2021.9609369

Sikos, L. F., & Philp, D. (2020). Provenance-Aware Knowledge Representation: A Survey of Data Models and Contextualized Knowledge Graphs. *Data Science and Engineering*, *5*(3), 293–316. https://doi.org/10.1007/s41019-020-00118-0

Simonovich, L. (2020). Cyber Security Incident Response in the Utility Sector. *Day 2 Tue, November 10, 2020*, D021S042R003. https://doi.org/10.2118/203220-MS

Škiljić, A. (2020). Cybersecurity and remote working: Croatia's (non-)response to increased cyber threats. *International Cybersecurity Law Review*, *1*, 51–61. https://doi.org/10.1365/s43439-020-00014-3

Taddeo, M. (2019). Is Cybersecurity a Public Good? *Minds and Machines*, *29*(3), 349–354. https://doi.org/10.1007/s11023-019-09507-5

Takko, T., Bhattacharya, K., Lehto, M., Jalasvirta, P., Cederberg, A., & Kaski, K. (2023). Knowledge mining of unstructured information: Application to cyber domain. *Scientific Reports*, *13*(1), 1714. https://doi.org/10.1038/s41598-023-28796-6

Tan, Z., Beuran, R., Hasegawa, S., Jiang, W., Zhao, M., & Tan, Y. (2020). Adaptive security awareness training using linked open data datasets. *Education and Information Technologies*, *25*(6), 5235–5259. https://doi.org/10.1007/s10639-020-10155-x

Teichmann, F., Boticiu, S. R., & Sergi, B. S. (2023). The evolution of ransomware attacks in light of recent cyber threats. How can geopolitical conflicts influence the cyber climate? *International Cybersecurity Law Review*, *4*(3), 259–280. https://doi.org/10.1365/s43439-023-00095-w

The Lens. n.d. Explore Global Science and Technology Knowledge: Aggregated Metadata. Lens.org. Available online: https: //www.lens.org/ (accessed on 27 December 2023).

Victor, P., Lashkari, A. H., Lu, R., Sasi, T., Xiong, P., & Iqbal, S. (2023). IoT malware: An attribute-based taxonomy, detection mechanisms and challenges. *Peer-to-Peer Networking and Applications*, *16*(3), 1380–1431. https://doi.org/10.1007/s12083-023-01478-w

Walker-Roberts, S., Hammoudeh, M., Aldabbas, O., Aydin, M., & Dehghantanha, A. (2020). Threats on the horizon: Understanding security threats in the era of cyber-physical systems. *The Journal of Supercomputing*, *76*(4), 2643–2664. https://doi.org/10.1007/s11227-019-03028-9

Wan, B., Xu, C., Mahapatra, R. P., & Selvaraj, P. (2022). Understanding the Cyber-Physical System in International Stadiums for Security in the Network from Cyber-Attacks and Adversaries using AI. *Wireless Personal Communications*, *127*(2), 1207–1224. https://doi.org/10.1007/s11277-021-08573-2

Yang, F., Han, Y., Ding, Y., Tan, Q., & Xu, Z. (2022). A flexible approach for cyber threat hunting based on kernel audit records. *Cybersecurity*, *5*(1), 11. https://doi.org/10.1186/s42400-022-00111-2

Yevseiev, S., Tolkachov, M., Shetty, D., Khvostenko, V., Strelnikova, A., Milevskyi, S., & Golovashych, S. (2023). The concept of building security of the network with elements of the semiotic approach. *ScienceRise*, *1*, 24–34. https://doi.org/10.21303/2313-8416.2023.002828

Zhang, H., Feng, B., & Tian, A. (2022). A systematic review for smart identifier networking. *Science China Information Sciences*, *65*(12), 221301. https://doi.org/10.1007/s11432-022-3577-8

Zheng, W., & Omote, K. (2022). A study on robustness of malware detection model. *Annals of Telecommunications*, *77*(9–10), 663–675. https://doi.org/10.1007/s12243-021-00899-z