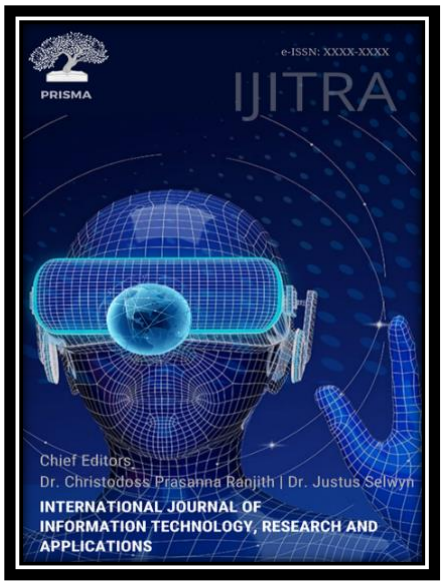


International Journal of Information Technology, Research and Applications (IJITRA)

Deepa Ajish, (2024). Streamlining Cybersecurity: Unifying Platforms for Enhanced Defense, 3(2), 48-57.

ISSN: 2583 5343

DOI: 10.59461/ijitra.v3i2.106

The online version of this article can be found at:
https://www.ijitra.com/index.php/ijitra/issue/archive

Published by:
PRISMA Publications

International Journal of Information Technology, Research and Applications (IJITRA) is a journal that publishes articles which contribute new theoretical results in all the areas of Computer Science, Communication Network and Information Technology. Research paper and articles on Big Data, Machine Learning, IOT, Blockchain, Network Security, Optical Integrated Circuits, and Artificial Intelligence are in prime position.

PRISMA
PUBLICATIONS

https://www.prismapublications.com/

Streamlining Cybersecurity: Unifying Platforms for Enhanced Defense

Deepa Ajish[1]
[1]IT Security and Compliance, ServiceNow Automation, Los Angeles, California, USA

deepajish@gmail.com

Article Info

Article history:

Received April 28, 2024
Accepted June 10, 2024
Published June 22, 2024

Keywords:

Cyberattack
Cybersecurity
Cybersecurity Framework
Platform Consolidation
Integrated Platform

ABSTRACT

Cybersecurity leaders face the challenges of complexity, tool overlap, and blind spots resulting from using multiple cybersecurity vendors and tools. In response, adopting a cybersecurity platform consolidation framework simplifies security operations by streamlining products and improving risk posture. Cybersecurity platform consolidation offers various benefits such as improved efficiency, cost savings, and better integration of security tools. However, concerns exist regarding potential limitations in flexibility and agility, increased dependency on a single vendor, and the complexity of migration processes. This review aims to analyze the advantages and drawbacks of cybersecurity platform consolidation to provide a comprehensive understanding of its implications for organizations. As the adoption of cybersecurity platform consolidation continues to grow, it becomes essential to delve deeper into the implications for organizations. By offering a comprehensive analysis of both the advantages and potential drawbacks of cybersecurity platform consolidation, this review aims to provide valuable insights for organizations considering or undergoing this transformation. This will enable organizations to make informed decisions and develop strategies to maximize the benefits while mitigating the concerns associated with platform consolidation. This paper explores the key findings, benefits, and best practices associated with consolidating security solutions.

Corresponding Author:

Deepa Ajish
IT Security and Compliance, ServiceNow Automation,
Los Angeles,
California, USA
Email: deepajish@gmail.com

1. INTRODUCTION

In the current era of cloud computing and amidst a constantly evolving threat landscape, organizations face the challenge of handling a diverse set of security tools sourced from different vendors. Researchers observe ongoing changes in both nation-state-affiliated and criminal adversaries. These shifts manifest as heightened sophistication in cyberattacks, which now employ novel and intrusive methods to compromise even the most astute targets [1].

According to a study by Cybersecurity Ventures, there was a significant increase in cybercrime in 2023, with cyberattacks occurring approximately every 39 seconds, resulting in over 2,200 cases per day. This frequency contrasted with the data from 2022, when incidents happened every 44 seconds [2]. Notably, the US State Department was targeted in major cyberattacks during 2023, and ransomware attacks gained prominence, impacting global organizations significantly. Furthermore, the projected global cost of cybercrime is staggering: it is expected to reach $23.84 trillion by 2027, a substantial increase from the $8.44 trillion recorded in 2022 [3]. 2023 marked a period of dynamic changes in the cyber threat landscape. Organizations

faced heightened scrutiny regarding regulatory compliance, and there was a notable surge in the adoption of Artificial Intelligence (AI) and Machine Learning (ML) technologies. These developments prompted organizations to navigate the intricacies of privacy regulations and meet stringent compliance requirements [4]. Organizations directed their efforts toward establishing agile and responsive ecosystems to bolster their preparedness. Simultaneously, strategic approaches evolved, emphasizing the adoption of more effective solutions and wider coverage against potential cyberattacks [5].

The proliferation of standalone solutions often leads to inefficiencies, increased costs, and gaps in security coverage. It will lead to data silos, manual workarounds, and fragmented processes. The presence of data silos impedes smooth integration, resulting in challenges when attempting to access and utilize data across the entire organization [6]. Cybersecurity platform consolidation emerges as a strategic approach to address these challenges. In the realm of cybersecurity technology, there are generally two prevailing paradigms: the 'best-of-breed' approach and the 'platform' approach. The former entails organizations selectively adopting security tools based on specific business requirements [7]. In contrast, the latter involves deploying a comprehensive suite of security tools that collectively offer end-to-end protection. Cybersecurity platform consolidation involves the strategic integration of diverse security tools and systems into a unified platform within an organization. By doing so, organizations achieve a comprehensive overview of their security posture and streamline the management of their cloud security infrastructure and operations. AI plays a crucial role in platform consolidation. AI-driven security solutions act as a force multiplier for contemporary security teams, allowing organizations to enhance scalability, speed, and depth of insight in their cybersecurity endeavors [8]. By utilizing machine learning (ML) algorithms, these AI-powered tools can identify activity patterns and anomalous behaviors that would pose challenges for human detection, even in the context of novel or previously unseen attacks [8]. In recent years, numerous research studies have explored the intersection of cybersecurity and AI [9] [10].

This consolidation addresses several challenges, including redundancy caused by overlapping functionalities in separate tools and gaps in security coverage due to ineffective communication between tools. Additionally, it contributes to cost reduction by eliminating the need to purchase, implement, and maintain multiple standalone security solutions. Ultimately, working with a single platform simplifies the monitoring of security status and enhances responsiveness to threats.

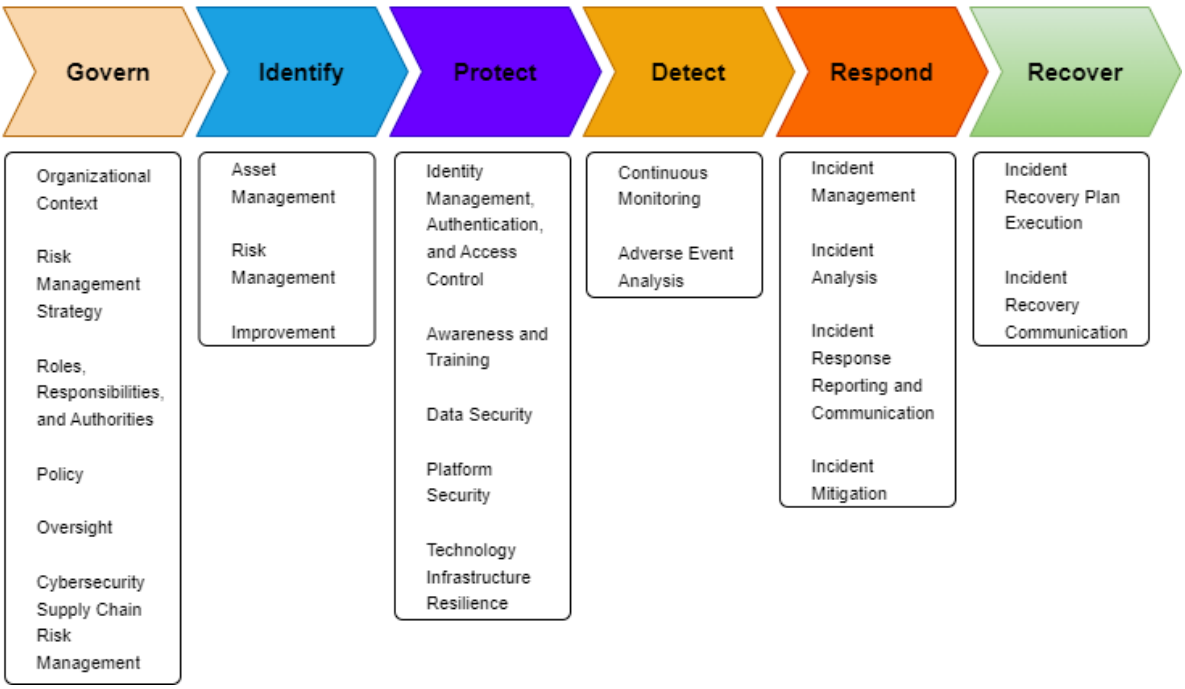
Cybersecurity encompasses a comprehensive set of strategies, protocols, and technical measures designed to safeguard, identify, rectify, and shield against harm, unauthorized access, alterations, or misuse of information and communication systems, along with the data they house [11]. The NIST Cybersecurity Framework, a widely recognized standard, was employed to comprehend the essential solution categories required for safeguarding, identifying, responding to, and defending against cyberattacks. This framework encompasses six core functions: Govern, Identify, Protect, Detect, Respond, and Recover. Figure 1 shows the NIST cybersecurity framework.

Fig. 1. NIST Cybersecurity Framework Functions

Source: NIST

Within these overarching functions, organizations can tailor their cybersecurity practices by referring to existing standards, guidelines, and best practices. [12]. Figure 2 shows the core functions and categories of the NIST security framework.

Fig. 2. Cybersecurity Framework - Core Functions and Categories



Forward-thinking enterprises have actively embraced digital transformation (DX), aiming to generate novel value streams through digital offerings, services, and immersive experiences. Projections from the International Data Corporation (IDC) indicate that global DX expenditures are poised to surge, reaching a staggering $3.4 trillion by 2026, with a robust five-year compound annual growth rate (CAGR) of 16.3%1 [13]. In the dynamic digital transformation environment, where security threats evolve rapidly, cybersecurity platform consolidation plays a crucial role in fortifying an organization's defenses. As digital transformation accelerates, organizations must adapt. Cybersecurity platform consolidation is not a one-time project; it's an ongoing journey. Regular assessments, threat modeling, and technology updates are essential. By embracing consolidation, organizations fortify their defenses, mitigate risks, and thrive in the dynamic digital era.

2. LITERATURE REVIEW

As organizations utilize an increasing number of security tools and platforms to protect their digital assets, the complexity and inefficiency of managing multiple systems have become apparent. The consolidation of cybersecurity platforms offers the promise of streamlined operations, improved visibility, and reduced costs. This literature review aims to explore the current state of cybersecurity platform consolidation, including its benefits, challenges, and best practices for implementation. By examining existing research and industry practices, this review will contribute to a comprehensive understanding of the implications and strategies associated with cybersecurity platform consolidation.

Due to the increase in cyberattacks like Advanced Persistent Threats (APTs), Distributed Denial of Service (DDoS) attacks, and spear-phishing campaigns led to the development of robust security protocols, refining encryption algorithms, and implementing multi-factor authentication methods [14]. The emergence of cloud computing, the Internet of Things (IoT), and mobile devices has significantly heightened the complexity of the cybersecurity landscape [15].

In the realm of cybersecurity, artificial intelligence (AI), machine learning (ML), and deep learning (DL) techniques have demonstrated considerable potential in identifying zero-day vulnerabilities and sophisticated malware. These approaches leverage extensive datasets to enhance their detection capabilities [16] [17].

The evolving cybersecurity landscape has prompted the development of various tools to tackle its challenges effectively. Based on a Securus360 report, organizations deploy an average of 45 cybersecurity tools to safeguard their infrastructures [18]. However, this seemingly comprehensive approach paradoxically weakens their overall cybersecurity posture. The report reveals a concerning trend: businesses that go beyond deploying 50 cybersecurity tools experience an 8% reduction in threat detection effectiveness and a 7% decline in defensive capabilities. In contrast, companies that strategically employ fewer tools, alongside a team of experienced experts, establish a more resilient and effective defense mechanism [18].

Several studies have highlighted the potential benefits of cybersecurity platform consolidation. A report by Gartner emphasized that integrated security platforms can help organizations reduce security gaps and improve overall security posture [19]. Similarly, a study by Forrester Research found that consolidating security tools can lead to cost savings and better alignment with business objectives [20].

In the context of today's extensive tool landscape, security operations center (SOC) teams face a significant challenge: the lack of a centralized view of the enterprise threat landscape. These teams find themselves constantly toggling between various displays and dashboards, attempting to assemble a coherent picture of ongoing events. Unfortunately, this often involves managing a flood of repetitive and unrelated alerts [21]. The absence of a consolidated perspective hinders their ability to respond effectively to security incidents. By integrating various technologies and accommodating them within a unified framework, this approach accelerates the identification of threats and enhances the efficiency of SOC teams [21].

However, it's important to acknowledge the potential challenges associated with platform consolidation. Some experts have raised concerns about integration issues, vendor lock-in, interoperability issues, and the impact on specialized security requirements. Organizations deeply entrenched in their existing workflows must evaluate whether a consolidated platform aligns effectively with their current architecture. Implementing new solutions is rarely a straightforward process instead, it necessitates collaboration with a cybersecurity provider who closely collaborates with the security team to ascertain whether consolidation is the optimal approach [22]. Vendor lock-in refers to a scenario when someone is forced to continue using a product or service because switching to a different product or service is not practical. Consequently, the customer remains obligated to use a potentially inferior product or service [23]. A study by [24] says that interoperability is achieved when multiple cloud platforms possess the authorization to distribute data to an authorized user within a cloud-based authorized environment. This hinges on the interplay of authorized users, authorized environments, and the right to distribute [24]. Additionally, organizations must carefully consider the implications for their existing infrastructure and the potential for disruption during the consolidation process. Ensuring that different tools communicate effectively, share data, and work harmoniously is crucial for successful consolidation [25].

One significant challenge encountered during the Systematic Literature Review (SLR) in this domain is the scarcity of empirical studies specifically addressing cybersecurity platform consolidation. While theoretical frameworks and conceptual discussions exist, empirical evidence is limited. Researchers often rely on anecdotal evidence, case studies, or expert opinions rather than robust empirical data. The absence of comprehensive studies hinders our understanding of the practical implications, benefits, and drawbacks of consolidation [25].

As the cybersecurity landscape continues to evolve, it's clear that platform consolidation will remain a topic of interest and debate within the industry. Future research should focus on identifying best practices for effective platform consolidation, as well as evaluating the long-term impact on organizational security and resiliency.

3. METHODOLOGY

When conducting the literature review for this study, a thorough and systematic approach was taken to ensure that all relevant sources were identified and analyzed. The methodology involved searching academic databases, online libraries, and scholarly journals to gather a comprehensive range of literature on the topic. Careful consideration was given to the selection criteria for including relevant studies, and a systematic process was followed to analyze and synthesize the information obtained from the literature. This approach ensured that the literature review provided a comprehensive and well-rounded understanding of the existing research and knowledge in the field.

3.1. Data Collection

In order to guarantee the accuracy and comprehensiveness of the gathered data, a systematic and focused method was employed for the data collection procedure. A thorough search of the databases was conducted using specific terms such as “Cybersecurity”, “Platform”, “Consolidation”, and "Best-of-breed". These terms were utilized in conjunction with the logical operators ‘AND’ and ‘OR’ to refine the search outcomes. More precisely, the search term was formulated as: “cybersecurity” AND “platform consolidation” OR "cybersecurity" AND “best-of-breed”. This search term was crafted to retrieve articles that discuss the importance of cybersecurity platform consolidation. The search was not restricted to the body of the articles but also encompassed the article titles and keywords. This ensured a broad coverage of pertinent literature, encompassing articles where the primary focus was on the selected topic.

3.2. Data Processing

After the data extraction, it was acknowledged that some impurities might be present in the extracted data, and not all the data obtained using the specified keywords would be directly related to the research goals. To address this issue, a manual sorting procedure was carried out after the extraction. This entailed a thorough examination of the extracted data to filter out any irrelevant or impure data. The sorting process adhered to the research objectives and the predetermined criteria for inclusion and exclusion, guaranteeing that only data relevant to the research was kept for subsequent analysis.

4. RESULTS

4.1. Benefits of Cybersecurity Platform Consolidation

Numerous discrete tools exhibit similarities or redundancies in their capabilities, leading to inefficiencies. Security coverage gaps arise due to ineffective communication or collaboration among disparate tools, leading to deficiencies in overall protection. Cost reduction can be achieved through consolidation, which mitigates the expenses related to procuring, deploying, and managing multiple security solutions. Streamlined management is facilitated by utilizing a unified platform, which simplifies the processes and workflows associated with monitoring an organization’s security posture and addressing potential threats. Figure 3 symbolizes the concept of cybersecurity platform consolidation.

Fig. 3. Security Platform Consolidation

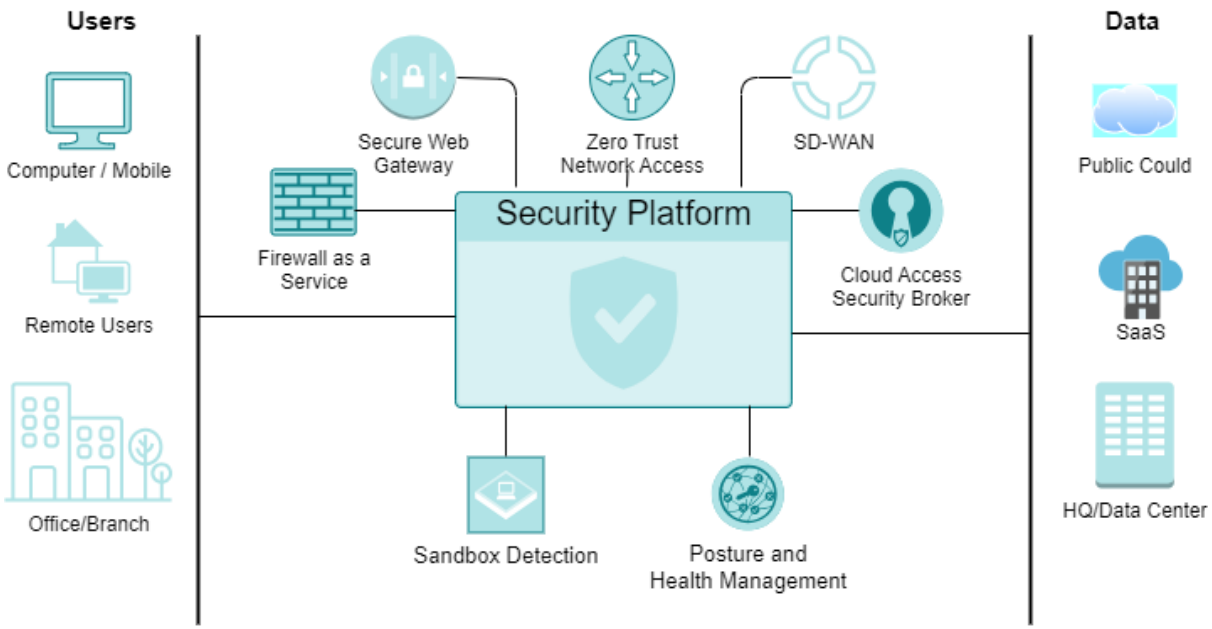


Table 1 presents a contrast between cybersecurity consolidation and the best-of-breed approach.

Aspect	Platform Consolidation	Best-of-Breed
Functional Overlap	Minimal overlap, as tools are designed to work together seamlessly.	Potential overlap due to disparate tools with similar capabilities.
Coverage Gaps	Comprehensive coverage due to unified tools and communication. Mitigation of security vulnerabilities arising from isolated solutions and human mistakes. By integrating disparate security tools and leveraging advanced technologies, organizations can minimize the chances of gaps in their security posture, ensuring a more robust defense against cyber threats.	Risk of gaps in protection due to lack of coordination among separate tools. The lack of data integration capability can cause data silos by preventing different systems from communicating with each other, resulting in disconnected data sources. This can lead to poor data management, inaccurate insights, and slow decision-making.
Cost Efficiency	Economical in terms of procurement, implementation, and maintenance.	May incur higher costs due to purchasing multiple standalone tools.
Unified Protection	Consolidated platforms protect organizations across various attack surfaces (network, cloud, IoT, endpoints, SD-WAN, etc.) using shared technologies and intelligence.	This approach offers optimal security protection for individual security domains, allowing customization through the selection of specialized tools.
Management Complexity	Simplified management with a single platform for monitoring and response.	Requires managing multiple tools, each with its own interface and workflows.
Scalability	Scalable, but limited to the capabilities of the chosen platform.	Flexible scalability by adding or replacing tools as needed.
Customization	Limited customization, as tools are part of a pre-defined suite.	The high degree of customization, tailored to specific organizational needs.
Threat Detection	Enhanced threat detection and response are achieved through the synergy of automation, machine learning, and artificial intelligence. These advanced technologies empower organizations to swiftly identify and mitigate emerging risks, ensuring a proactive approach to cybersecurity.	In the best-of-breed approach, organizations select security tools based on specific business needs. Each tool is chosen for its effectiveness in a particular security domain.
Threat Analysis	Centralized threat detection allows for comprehensive analysis, enabling quicker identification and mitigation of risks.	The process of threat detection involves identifying various types of security threats using distinct tools. Subsequently, the identification and mitigation of these threats can be a time-consuming endeavor.
Vendor Dependency	Depends on the vendor's selected strategic plan and subsequent updates.	Independent choice of vendors.
Integration Challenges	Integration difficulties may emerge if the selected platform lacks compatibility with pre-existing systems.	Requires integration efforts to ensure seamless communication among tools.
Risk Tolerance	Suitable for organizations seeking a holistic security approach.	Ideal for organizations with specific requirements and risk tolerance.
Incident Detection	Accelerated incident detection, analysis, and response are achieved through centralized cyber threat detection and response.	It is time-consuming because security tools are based on specific business needs and organizations will have several individual security tools.

Security Policy Updates	Reduced Time for Security Policy Updates. By streamlining security tools and unifying threat prevention and response, organizations can swiftly update security policies across all environments.	Each individual security tool operates under distinct security policies and requires separate updates.
Patch Implementation	Consistent Patch Implementation. A consolidated approach ensures consistent patch deployment, minimizing vulnerabilities and enhancing overall security.	In a best-of-breed setup, each security tool (such as firewalls, antivirus, and intrusion detection systems) is responsible for its own patch management. Coordinating patch cycles across multiple tools can be complex.
User Experience	Enhanced user experience, facilitated by a streamlined route toward zero-trust architectures. By embracing Zero Trust principles, organizations can create a security framework that prioritizes continuous verification and minimizes trust assumptions, ultimately enhancing overall cybersecurity posture.	Users need training on each tool, which can be time-consuming.
Productivity	Enhanced productivity and boosted morale among SOC and cybersecurity teams.	Often grapple with excessive workloads and extended hours, lead to decreased turnover rates.

Table 1: Comparison of platform consolidation with best-of-breed method.

4.2. Challenges of Platform Consolidation

- Legacy Systems: Many organizations operate legacy systems or applications that depend on specific security tools. The process of integrating these systems into a consolidated platform can pose challenges, particularly when these legacy systems lack modern APIs or adequate support.
- Stakeholder Alignment: Ensuring congruence among diverse stakeholders, including IT teams, security professionals, and business leaders, holds paramount importance. Given the potential divergence in priorities across these teams, achieving consensus becomes imperative for the successful execution of consolidation efforts.
- Data Migration: Efficiently consolidating data from various tools onto a single platform necessitates meticulous planning. Key considerations include ensuring data integrity, effective mapping, and seamless transformation. Failing to execute a comprehensive and accurate data migration process can result in vulnerabilities within security coverage.
- Vendor Lock-In: In the context of organizational security, dependence on particular vendors for existing security tools is commonplace. However, transitioning away from these tools presents considerable challenges, including contractual commitments, licensing expenses, and potential compatibility issues.
- Change Management: Organizational employees who are familiar with particular tools may exhibit reluctance during transitions. Effective change management approaches are crucial for addressing apprehensions, delivering training, and facilitating seamless adoption.
- Interoperability: Effective communication among distinct security components is crucial. Challenges related to integration may emerge when consolidating tools that utilize diverse protocols, data structures, and communication channels.
- Performance Impact: Consolidation can affect system performance. Organizations must assess the impact on network latency, response times, and overall system efficiency.
- Customization and Flexibility: While consolidating security tools, organizations must strike a delicate balance between standardization and customization. Although some tools offer significant customization options, the process of consolidation may result in the loss of specific features or flexibility.

- Risk Assessment: Organizations need to conduct a comprehensive risk assessment when considering consolidation. This evaluation should address whether the new platform effectively mitigates existing threats and identifies any potential blind spots.
- Compliance and Regulations: Different tools may comply with specific regulations (e.g., GDPR, HIPAA). Consolidation should not jeopardize compliance. Ensuring the new platform meets legal requirements is essential.

5. FUTURE PERSPECTIVE

Security and risk management leaders are grappling with increasing demands for service, rapidly evolving threat landscapes, and a shortage of technical talent. Platform consolidation emerges as a strategic solution to address these challenges. By integrating disparate security tools into unified platforms, organizations can thrive even in hostile environments. The consolidation approach doesn't necessarily mean sourcing everything from a single vendor; rather, it emphasizes harmonizing systems for better efficiency and effectiveness [19]. Consolidated security platforms should adopt a proactive, data-driven, and business-centric approach. Leveraging the existing security configuration as a reference point for threat analysis is crucial. Organizations must automatically identify misconfigurations and security gaps to enhance their cybersecurity posture [26]. Embracing platform consolidation marks a strategic shift from a fragmented array of solutions to a more cohesive integration of systems. This transformation goes beyond relying solely on a single vendor; it's about streamlining and optimizing security tools. As threats evolve, consolidated platforms offer agility, scalability, and improved threat detection capabilities. In summary, the future of cybersecurity lies in integrated, streamlined, and adaptive security platforms that empower organizations to navigate the ever-changing threat landscape effectively.

6. LIMITATIONS

In the scholarly discourse, the limited existing research on cybersecurity platform consolidation presents a challenge when attempting to compare and draw generalizable conclusions. The scarcity of studies addressing this topic complicates the assessment of rarely mentioned experiences, necessitating additional research to gauge the extent and impact of these issues. While cybersecurity platforms often share similar features, the specific platform chosen can significantly influence the benefits evaluated in a study. Nonetheless, the exploration conducted by this research contributes to the broader understanding of cybersecurity platform consolidation and lays the groundwork for future researchers to investigate and compare the significance of cybersecurity platform consolidation.

7. CONCLUSION

In conclusion, the consolidation of cybersecurity platforms presents a dual perspective for organizations to deliberate. On one hand, centralizing security tools can yield benefits such as enhanced visibility, streamlined processes, and cost savings. However, this approach also introduces risks, including a potential single point of failure and complexities in integrating diverse systems. Consequently, the decision to consolidate cybersecurity platforms should be grounded in a comprehensive assessment of an organization's specific requirements, risk tolerance, and capacity to effectively manage a unified environment. It is crucial for organizations to weigh the potential advantages against the associated challenges, ensuring an informed decision that aligns with their overarching cybersecurity strategy and objectives.

Moreover, cybersecurity platform consolidation extends beyond the mere reduction of tool proliferation; it represents a strategic maneuver toward improved risk management, operational efficiency, and heightened security. Organizations must meticulously evaluate their distinct needs, account for intangible factors, and prioritize seamless integration to fully capitalize on the benefits of consolidation.

FUNDING INFORMATION

The author declares that this work was not funded.

REFERENCES

[1] Chithaluru, P., Al-Turjman, F., Kumar, M., & Stephan, T. (2023). Computational-intelligence-inspired adaptive opportunistic clustering approach for industrial IoT networks. *IEEE Internet of Things Journal*, *10*(9), 7884–7892.

[2] WatchGuard (2024) There was a cyberattack every 39 seconds in 2023. Available at: https://www.watchguard.com/wgrd-news/blog/there-was-cyberattack-every-39-seconds-2023 (Accessed: 02 March 2024)

[3] World Economic Forum (2024) 2023 was a big year for cybercrime – here's how we can make our systems safer. Available at: https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/ (Accessed: 02 March 2024)

[4] ISACA (2023) An Executive View of Key Cybersecurity Trends and Challenges in 2023. Available at: https://www.isaca.org/resources/news-and-trends/industry-news/2023/an-executive-view-of-key-cybersecurity-trends-and-challenges-in-2023 (Accessed: 03 March 2024)

[5] Gartner (2023) Top Strategic Cybersecurity Trends for 2023. Available at: https://www.gartner.com/en/articles/top-strategic-cybersecurity-trends-for-2023 (Accessed: 03 March 2024)

[6] Boina, R., Achanta, A., & Mandvikar, S. (2023). Integrating data engineering with intelligent process automation for business efficiency. *International Journal of Science and Research (IJSR)*, *12*(11), 1736–1740.

[7] Enterpriseitworldmea (2024) Best of Breed vs. Best Fit: Navigating Cybersecurity Solutions. Available at: https://enterpriseitworldmea.com/best-of-breed-vs-best-fit-navigating-cybersecurity-solutions/ (Accessed: 10 March 2024)

[8] Crowdstrike (2023) WHAT IS CYBERSECURITY PLATFORM CONSOLIDATION?. Available at: https://www.crowdstrike.com/cybersecurity-101/secops/cybersecurity-platform-consolidation/ (Accessed: 10 March 2024)

[9] Mohammed, I. A. (2020). Artificial intelligence for cybersecurity: A systematic mapping of literature. *Artif. Intell*, *7*(9), 1–5.

[10] Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K.-K. R. (2022). Artificial intelligence in cyber security: Research advances, challenges, and opportunities. *Artificial Intelligence Review*, 1–25.

[11] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 101804.

[12] NIST (2024) NIST Cybersecurity Framework 2.0: Resource & Overview Guide. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.pdf (Accessed: 17 March 2024)

[13] IDC (2022), IDC Spending Guide Sees Worldwide Digital Transformation Investments Reaching $3.4 Trillion in 2026. Available at: https://www.idc.com/getdoc.jsp?containerId=prUS49797222 (Accessed: 17 March 2024)

[14] Alizadeh, M., Andersson, K., & Schelen, O. (2020). A survey of secure internet of things in relation to blockchain. *Journal of Internet Services and Information Security (JISIS)*, *10*(3), 47–75.

[15] Schwab, W., & Poujol, M. (2018). The state of industrial cybersecurity 2018. *Trend Study Kaspersky Reports*, *33*.

[16] Ali, S., Rehman, S. U., Imran, A., Adeem, G., Iqbal, Z., & Kim, K.-I. (2022). Comparative evaluation of ai-based techniques for zero-day attacks detection. *Electronics*, *11*(23), 3934.

[17] Hindy, H., Atkinson, R., Tachtatzis, C., Colin, J.-N., Bayne, E., & Bellekens, X. (2020). Utilising deep learning techniques for effective zero-day attack detection. *Electronics*, *9*(10), 1684.

[18] Securus360, So Many Cybersecurity Tools Deployed. Available at: https://www.securus360.com/blog/so-many-cybersecurity-tools-deployed (Accessed: 17 March 2024)

[19] Gartner (2021) Consolidated Security Platforms Are the Future. Available at: https://www.gartner.com/en/documents/4008930 (Accessed: 17 March 2024)

[20] Forrester (2018) Improve Business Agility Through Platform Consolidation. Available at: https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/analyst-report/servicenow-forrester-platform-consolidation.pdf (Accessed: 23 March 2024)

[21] TrendMicro (2023) Strategic Tips to Optimize Cybersecurity Consolidation. Available at: https://www.trendmicro.com/en_hk/ciso/23/j/reduce-complexity-cybersecurity-consolidation.html (Accessed: 23 March 2024)

[22] Palo Alto Networks - What is Cybersecurity Consolidation? Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-cybersecurity-consolidation (Accessed: 24 March 2024)

[23] Weldemicheal, T. (2023). *Vendor lock-in and its impact on cloud computing migration*.

[24] Grossman, R. L., Boyles, R. R., Davis-Dusenbery, B. N., Haddock, A., Heath, A. P., O'Connor, B. D., Resnick, A. C., Taylor, D. M., & Ahalt, S. (2024). A Framework for the Interoperability of Cloud Platforms: Towards FAIR Data in SAFE Environments. *Scientific Data*, *11*(1), 241.

[25] Nyasha, G., Nwosu, L. I., Bereng, M. C., Mahlaule, C., & Segotso, T. (2024). A Systematic Literature Review on the Impact of Cybersecurity Threats on Corporate Governance During the Covid-19 Era. *ICABR Conference*, 157–174.

[26] Security Boulevard (2024) Rethinking Cybersecurity: Why Platform Consolidation is the Future. Available at: https://securityboulevard.com/2024/02/rethinking-cybersecurity-why-platform-consolidation-is-the-future/ (Accessed: 31 March 2024)