World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Convergence of networking and security: A holistic approach

Sharanya Vasudev Prasad *

University of Maryland, USA.

World Journal of Advanced Research and Reviews, 2025, 26(01), 1360-1367

Publication history: Received on 25 February 2025; revised on 07 April 2025; accepted on 10 April 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.1.1123

Abstract

The convergence of networking and security represents a fundamental shift in how organizations build their digital infrastructures. This article explores how security can be integrated directly into network systems rather than being treated as a separate component. Traditional approaches where networking and security teams operate independently create gaps in protection, while integration enables consistent policy enforcement, better visibility, and faster threat response across complex environments. Key technologies like Software-Defined Networking, Secure Access Service Edge, and Zero Trust Architecture provide the foundation for this integrated approach. Organizations that adopt this model benefit from reduced operational costs, faster incident response, improved resilience, and better alignment with business goals. While the benefits are clear, organizations face challenges including skill gaps, outdated infrastructure, and resistance to organizational change. As digital environments continue to evolve, this convergence will reshape both technical systems and operational structures.

Keywords: Network-security convergence; Zero Trust Architecture; Security Service Edge; Integrated infrastructure; Cybersecurity resilience

1. Introduction

The traditional separation between networking and security functions is becoming increasingly obsolete in today's rapidly evolving digital landscape. As cyber threats grow more sophisticated and IT environments more complex, organizations recognize the critical need for a converged approach that weaves security directly into the network fabric. This integration represents a technological shift and a fundamental rethinking of how we design, implement, and manage secure digital infrastructures.

According to IT Pro's comprehensive analysis, network and security convergence can be defined as "the strategic integration of networking infrastructure and security controls into a unified architecture that optimizes efficiency, security, and scalability" [1]. Their research indicates that organizations pursuing convergence strategies experience fewer security incidents than those maintaining traditional siloed approaches. The study emphasizes that this convergence enables enterprises to implement consistent security policies across their entire network infrastructure, eliminating the gaps frequently occurring when networking and security functions operate independently.

The financial implications of this convergence are substantial. IBM's Cost of a Data Breach Report documented that organizations with integrated security and networking teams experienced lower breach costs than those maintaining siloed operations [2]. The report found that the global average data breach cost reached $4.45 million in 2023, a 15% increase over three years, making the economic case for convergence even more compelling. Additionally, companies that had deployed unified security and networking platforms contained breaches faster than those using fragmented solutions, significantly reducing the "dwell time" during which attackers could access sensitive systems.

* Corresponding author Sharanya Vasudev Prasad

From a technological standpoint, the market for converged networking and security solutions continues to expand as adoption accelerates across sectors. IT Pro notes that financial services and healthcare are leading implementation efforts, driven by their need to protect sensitive data while maintaining operational agility [1]. This growth coincides with the increasing complexity of digital ecosystems, where enterprises must manage numerous cloud applications and maintain connections with multiple third-party vendors.

The IBM report highlights that organizations implementing network and security convergence experience higher levels of operational efficiency through automated policy enforcement and reduced management overhead [2]. Their analysis found that those with mature convergence strategies were more likely to exceed their business performance targets and capable of rapidly adapting to emerging threats without disrupting critical business operations. This alignment between security capabilities and business objectives represents the most significant advantage of the converged approach in today's dynamic business environment.

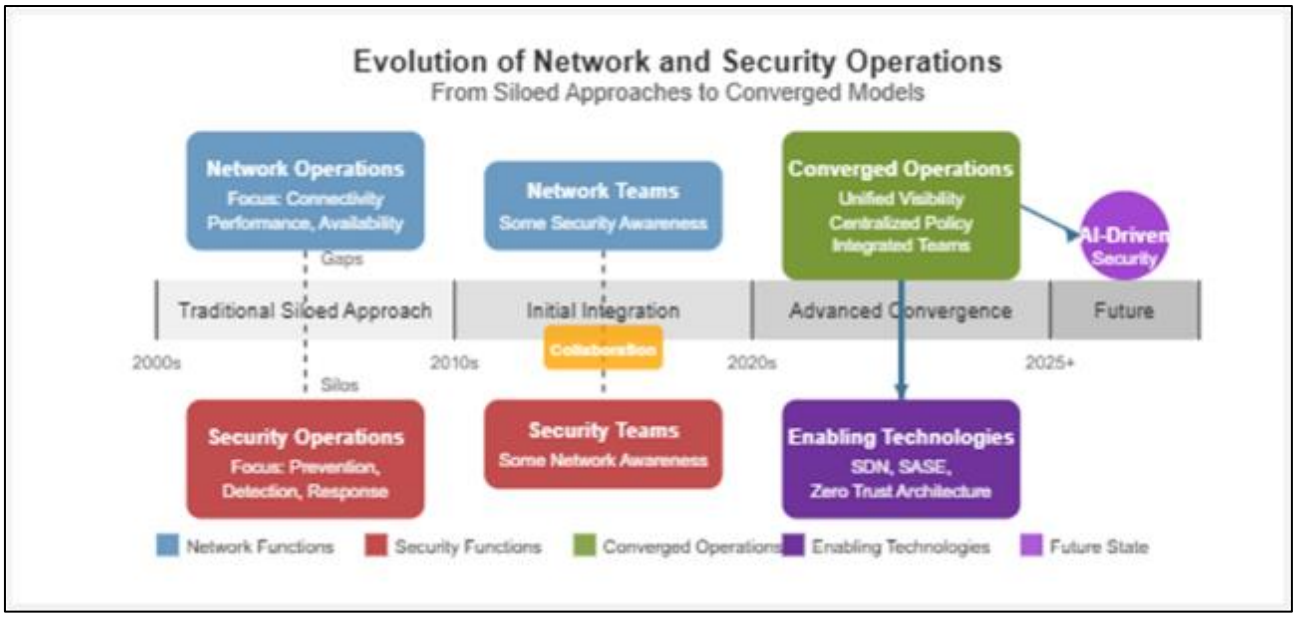

Figure 1 Evolution of Network and Security Operations

2. The End of Siloed Operations

Historically, networking and security teams operated as distinct entities with separate objectives, tools, and methodologies. Network teams focused primarily on connectivity, performance, and availability, while security teams concentrated on threat prevention, detection, and response. This separation created inevitable gaps in coverage and communication, leading to security vulnerabilities and operational inefficiencies.

According to HPE Aruba's "Network Security Today" report, organizations still maintain separate networking and security teams, with only a minority having achieved full integration or meaningful collaboration between these functions [3]. The study revealed that companies with siloed operations experience more security incidents than those with converged approaches. Furthermore, their research showed that network changes in traditional environments often require manual security reviews, adding significant time to deployment cycles and creating bottlenecks in business initiatives.

Recent research and industry trends have highlighted the limitations of this siloed approach. When security is treated as an overlay or afterthought to network design, it creates friction in deployment and management, often resulting in compromised security postures or degraded network performance. The Enterprise Strategy Group's 2024 Technology Spending Intentions Survey found that integrating security tools with IT infrastructure remains a significant challenge for many organizations [4]. The survey also revealed that a substantial percentage of respondents plan to increase spending on network security integration over the next 12 months, underscoring the growing recognition of this issue. Additionally, security leaders reported that maintaining consistent security policies across diverse environments with disconnected teams and toolsets remains exceptionally difficult.

The operational inefficiencies stemming from siloed approaches extend beyond technical issues. HPE Aruba's research indicates that organizations with separated networking and security functions experience increased costs related to tool redundancy and integration efforts compared to those with unified approaches [3]. This fragmentation also impacts workforce productivity, with technical teams spending considerable time in cross-functional coordination meetings rather than addressing core responsibilities. The ESG survey further confirms this trend, with IT leaders citing improved operational efficiency as a primary expected benefit of security and networking convergence investments [4].

These findings underscore the growing consensus that traditional organizational and technological boundaries between networking and security functions are becoming increasingly untenable in today's threat landscape. This is driving the movement toward more integrated approaches that can address the interconnected challenges of modern digital environments.

3. Embedding Security into the Network Fabric

The converged model fundamentally changes this paradigm by designing security controls directly into the network architecture. Rather than implementing security as a series of checkpoints that traffic passes through, this approach distributes security functions throughout the network infrastructure, creating a comprehensive security mesh.

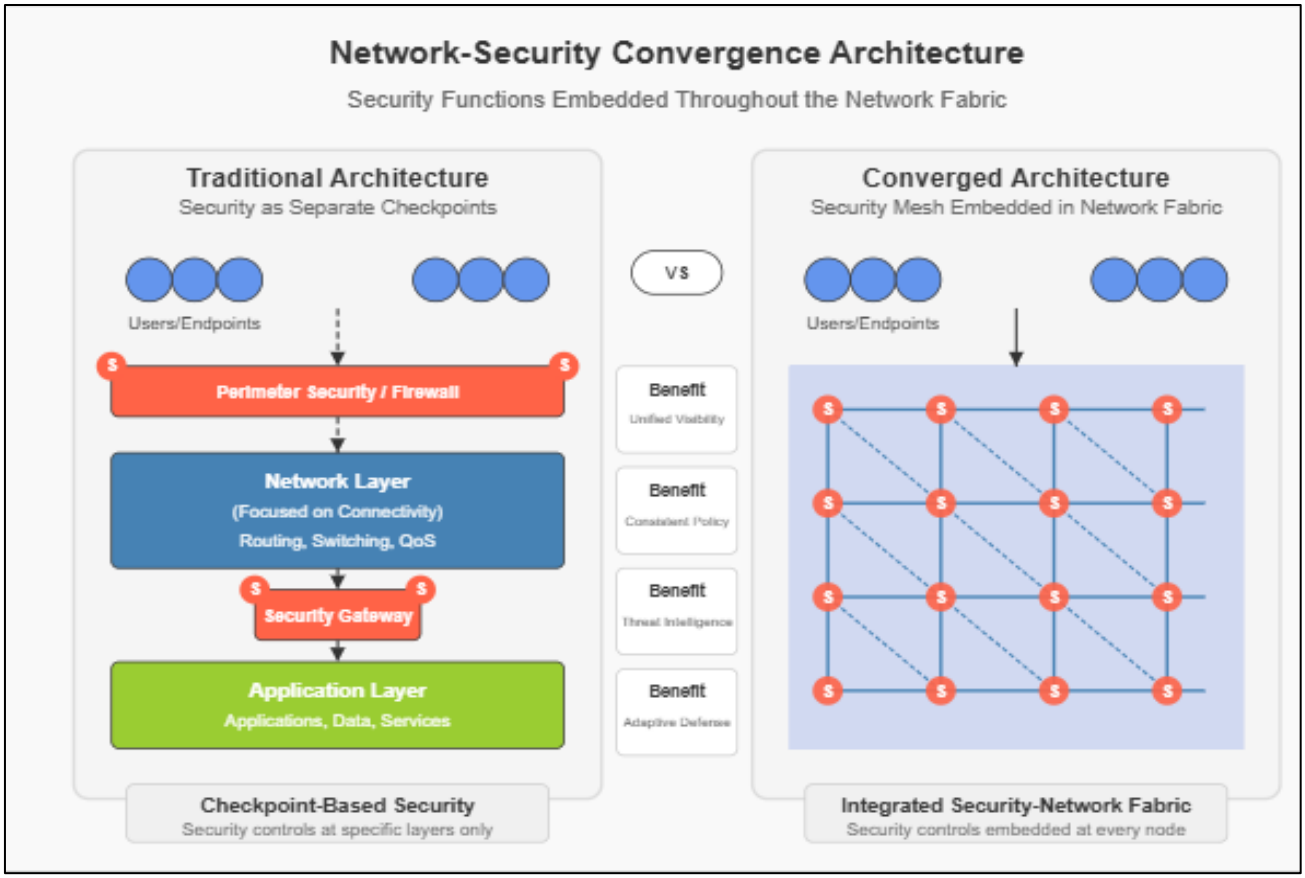

Figure 2 Network Security Convergence Architecture

Cisco's 2023 Security Outcomes Report highlights that organizations with high levels of security-network integration were 2.5x more likely to minimize unplanned work and achieve stronger business outcomes successfully [5]. Their findings show that integrated security programs can reduce downtime and improve mean time to remediation, suggesting that security built into the network fabric provides significant operational advantages. The report also emphasizes that security programs that work well with IT operations have a 31% higher probability of building a strong security culture across the organization.

Key components of this integrated approach include unified visibility and monitoring across all network segments and traffic flows, centralized policy management that ensures consistent security enforcement, automated threat intelligence integration that keeps defenses current, and contextual awareness that adjusts security controls based on

user, device, and application profiles. According to Markets and Markets' research on the Security Service Edge (SSE) market, the global SSE market size is projected to grow from $840 million in 2023 to $2.4 billion by 2028, reflecting the increasing demand for integrated security and networking solutions [6]. Their analysis indicates that organizations are increasingly seeking platforms that combine security functions like Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Zero Trust Network Access (ZTNA) capabilities into the network infrastructure itself.

The distributed nature of embedded security controls provides significant resilience advantages. The system becomes more resistant to targeted attacks when security functions are integrated throughout the network fabric rather than concentrated at specific choke points. Cisco's research found that organizations reporting high levels of IT and security integration were 42% more likely to build an effective and efficient security incident management program [5]. Additionally, these organizations were better positioned to respond to major security events, with the report noting that a well-integrated approach to network security can significantly strengthen overall security resilience.

This architectural shift creates opportunities for more dynamic, responsive security that adapts automatically to changing conditions rather than requiring manual reconfiguration. The Markets and Markets report notes that North America currently dominates the adoption of the SSE market. Still, the Asia Pacific region is expected to grow at the highest compound annual growth rate during the forecast period, indicating the global momentum behind this approach [6]. Their analysis suggests that enterprises across various industries recognize the value of embedding security functions directly into their network infrastructure as they adapt to increasingly distributed work environments and evolving threat landscapes.

4. Enabling Technologies

Several technologies are driving this convergence:

4.1. Software-Defined Networking (SDN)

SDN decouples network control from forwarding functions, enabling centralized network behavior management through software applications. This programmability allows security policies to be dynamically applied across the network, responding to real-time changing conditions and threats. According to Grand View Research, the global network equipment market size was valued at USD 156.16 billion in 2022 and is expected to grow at a compound annual growth rate (CAGR) of 8.5% from 2023 to 2030 [7]. Their analysis notes that the growing adoption of SDN solutions drives this market expansion as organizations seek more flexible, programmable network infrastructures that can adapt to evolving security requirements. The research also highlights that integrating artificial intelligence and machine learning technologies with network equipment enables more sophisticated, automated security responses within SDN environments.

4.2. Secure Access Service Edge (SASE)

SASE combines network security functions with WAN capabilities to support organizations' dynamic, secure access needs. Delivered primarily as a cloud service, SASE identifies sensitive data or malware, decrypts content, and monitors sessions for risk and trust levels. Gartner's review of the Single-Vendor SASE market emphasizes that unified SASE solutions provide significant advantages over fragmented approaches, particularly in securing distributed workforces and cloud applications [8]. Their assessment of customer reviews indicates that organizations implementing comprehensive SASE frameworks report improved visibility across their network footprint and more consistent application of security policies. The research also shows that leading SASE providers increasingly focus on integration capabilities that allow seamless incorporation of existing security and networking investments.

4.3. Zero Trust Architecture

Zero Trust principles complement the converged approach by requiring all users and devices to be authenticated, authorized, and continuously validated before granting access to applications and data. This model integrates seamlessly with policy-driven network controls. Grand View Research notes that Zero Trust Network Access (ZTNA) implementations are becoming a significant component of modern network equipment deployments, particularly as organizations adapt to hybrid work environments [7]. Their market analysis indicates that network equipment vendors increasingly incorporate Zero Trust capabilities into their product portfolios, recognizing the growing demand for security features that extend beyond traditional perimeter-based approaches. Gartner's market guide emphasizes that effective SASE implementations typically incorporate Zero Trust principles, creating a unified approach to network security that addresses both on-premises and cloud-based resources [8].

These enabling technologies are creating the foundation for truly converged network and security architectures. They allow organizations to implement consistent security policies across increasingly distributed and complex environments while maintaining the flexibility needed to adapt to evolving business requirements and threat landscapes.

5. Organizational Benefits

The convergence of networking and security delivers numerous organizational advantages:

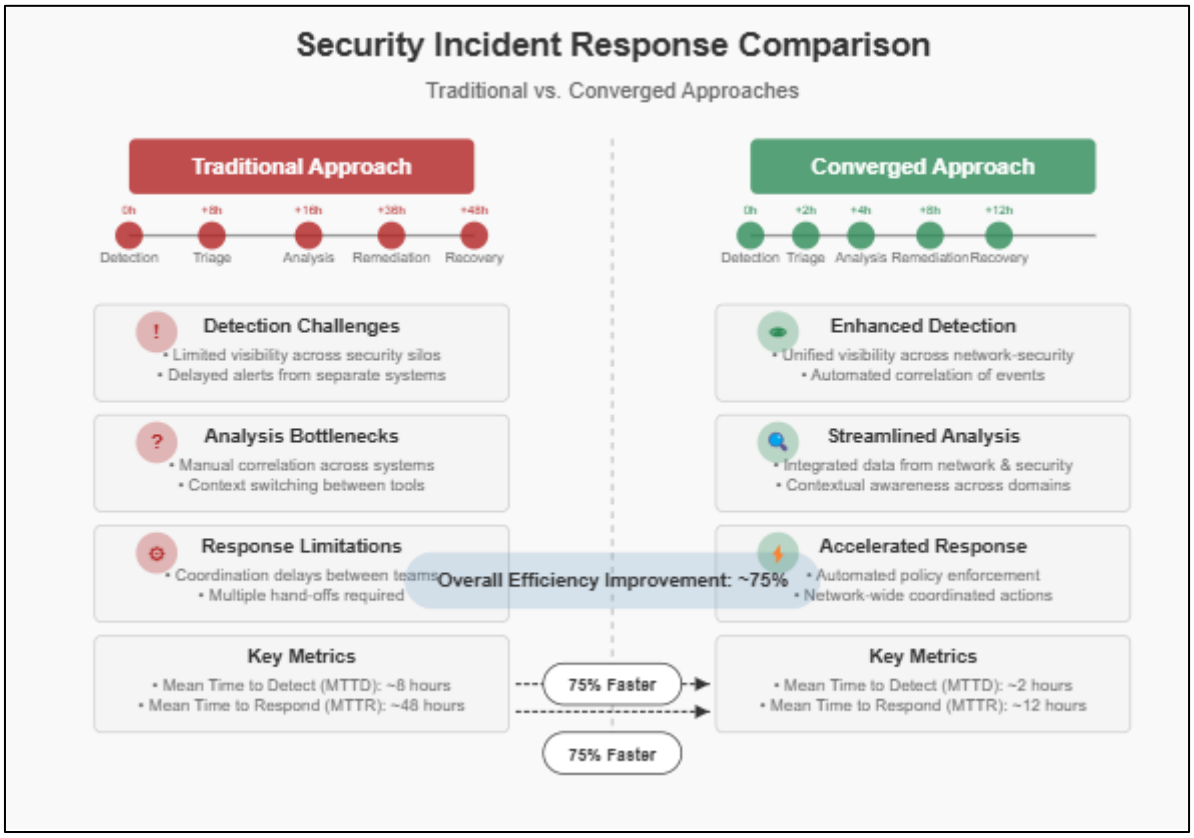

Figure 3 Security Incident Response Comparison

According to the Forbes Technology Council's analysis of the future of cybersecurity, organizations that implement integrated security and networking strategies are better positioned to respond to emerging threats by eliminating operational silos that can slow down detection and response [9]. Their research emphasizes that as attack surfaces expand with the growth of cloud services, IoT, and remote work, converged approaches provide more comprehensive visibility across complex environments. The Council notes that organizations embracing this convergence can more effectively implement defense-in-depth strategies that protect against sophisticated attacks while maintaining operational agility.

Reduced operational overhead through simplified management and fewer discrete systems represents a primary benefit of convergence. McKinsey's analysis of cybersecurity trends indicates that organizations pursuing integrated approaches to security and networking can significantly reduce complexity in their technology environments [10]. Their research points out that technology and security leaders are increasingly seeking ways to streamline their security stacks, noting that excessive complexity often creates vulnerabilities and operational inefficiencies. McKinsey also highlights that when security and networking functions are tightly integrated, organizations can more efficiently allocate resources and reduce redundant capabilities.

Streamlined incident response with unified visibility and control enables organizations to detect and remediate threats more quickly. The Forbes Technology Council emphasizes that converged security and networking functions allow for more rapid identification of anomalous behaviors across the infrastructure, which is particularly important as attack techniques become more sophisticated [9]. Their analysis suggests that unified visibility creates opportunities for more

effective automation of routine security tasks, enabling security teams to focus on more complex threats requiring human expertise.

Implementing consistent security controls throughout the network fabric improves resilience against evolving threats. McKinsey's research indicates that organizations with mature security capabilities increasingly focus on building resilience through integrated approaches rather than trying to prevent every possible attack [10]. Their analysis shows that adapting security controls to changing business demands and threat landscapes is significantly more effective when security is embedded within the network architecture rather than applied as an overlay.

Enhanced security posture with fewer blind spots and gaps, better alignment between security and business objectives, and more efficient resource utilization across networking and security domains complete the picture of organizational benefits. These advantages collectively enable organizations to build more responsive, adaptable, and secure digital environments to support business innovation better while managing ever-evolving security risks.

6. Challenges and Considerations

While the benefits are compelling, organizations pursuing this converged approach must navigate several challenges:

According to Cisco's 2024 Global Networking Trends Report, network teams are increasingly asked to support security functions, with 66% of organizations expecting their network teams to implement security policies [11]. Their research shows that while technical convergence is advancing, organizational structures often lag, creating friction in implementation efforts. The report highlights that network and security professionals frequently have different priorities and metrics for success, complicating coordination between these traditionally separate domains.

Skill gaps between traditional networking and security roles present significant hurdles for many organizations. DXC Technology's research on security operations centers emphasizes that as security and networking converge, SOC teams must develop new competencies to monitor and protect increasingly complex infrastructures [12] effectively. Their analysis suggests that organizations must invest in continuous training and development programs to ensure their teams can adapt to evolving technologies and threat landscapes. The research also highlights the importance of defining clear career paths for professionals who develop cross-functional expertise in networking and security domains.

Legacy infrastructure that may not support integrated capabilities often creates technical barriers to convergence. Cisco's report indicates that many organizations maintain a mix of traditional and modern network components, creating challenges for implementing consistent security policies across heterogeneous environments [11]. Their research shows that successful organizations typically take an incremental approach to modernization, prioritizing critical infrastructure segments for updates while maintaining appropriate security controls across legacy and modern environments.

Organizational resistance to changing established team structures and vendor ecosystems that still reflect the traditional separation represent additional challenges. DXC's analysis notes that effective security operations increasingly require collaboration across multiple domains, including networking, application teams, and business units [12]. Their research suggests that creating formalized processes for cross-functional collaboration can help overcome organizational silos while building the foundation for more integrated approaches to security and networking.

Successful implementation typically requires executive sponsorship, targeted training programs, and a phased approach that incrementally demonstrates value. By acknowledging and addressing these challenges systematically, organizations can effectively navigate the transition to converged network-security architectures, realizing the significant benefits while minimizing disruption to existing operations.

7. The Path Forward

As enterprise IT ecosystems evolve toward greater complexity and distribution, the converged network-security approach promises fewer blind spots, more adaptive defenses, and better alignment with business needs. Organizations that successfully implement this holistic model will be better positioned to meet the security challenges of increasingly sophisticated threat landscapes while maintaining the agility needed in today's digital economy.

According to Gartner's analysis of network security trends, the future of security architecture is moving decisively toward converged platforms that integrate traditionally separate networking and security functions [8]. Their research

highlights that as organizations adopt hybrid and multi-cloud strategies, security must be woven directly into the network rather than added as an overlay. The report emphasizes that the growing complexity of IT environments makes it increasingly difficult to maintain consistent security policies across disparate systems without a unified approach to networking and security. They also note that the accelerating adoption of technologies like SD-WAN and SASE reflects the broader industry movement toward integrated architectures that can adapt more readily to changing business needs and threat landscapes.

The future of secure infrastructure lies not in stronger walls between network segments or more powerful security appliances but in the seamless integration of security into every aspect of the network fabric. This convergence represents a technical evolution and a fundamental reimagining of how we approach digital infrastructure in an age of persistent and sophisticated threats. Cisco's Security Outcomes Research underscores that organizations must balance security effectiveness with business agility, highlighting the importance of integrated approaches that reduce complexity while improving protection [5]. Their analysis indicates that leading organizations increasingly adopt architectures that embed security controls directly into their digital infrastructure, enabling more responsive defense mechanisms that can adapt to evolving threats without impeding business operations.

Industry analysts predict that AI will play an increasingly central role in converged network security architectures, enabling more automated threat detection and response across complex environments. This automation will be essential as the volume and sophistication of attacks continue to outpace the capacity of human security teams to respond manually. The Markets and Markets study similarly notes that security leaders are increasingly focused on building resilient systems that can withstand attacks and recover quickly, which requires tight integration between security controls and the underlying network infrastructure [6].

As this convergence accelerates, it will reshape technical architectures, organizational structures, skill requirements, and operational processes across the IT landscape. Organizations that embrace this evolution proactively will gain significant advantages in security effectiveness and business agility, establishing the foundation for digital trust essential for success in increasingly connected and distributed business environments.

8. Conclusion

The convergence of networking and security represents a technological trend and a necessary evolution in how organizations approach digital infrastructure in an increasingly complex threat landscape. By weaving security directly into the network fabric, organizations can achieve more comprehensive protection while improving operational efficiency and business agility. This integrated approach eliminates the gaps between networking and security functions, enabling consistent policy enforcement and unified visibility across distributed environments. As technologies like SDN, SASE, and Zero Trust mature, the foundations for this convergence are becoming increasingly accessible. Organizations that embrace this holistic model—investing in cross-functional skills, modernizing legacy infrastructure, and redesigning operational processes—will develop more resilient security capabilities that adapt dynamically to evolving threats. The future of secure infrastructure lies not in more rigid boundaries or isolated security controls but in the seamless integration of security throughout the entire network architecture, creating adaptive defense systems that protect digital assets while enabling innovation and growth.

References

[1] Rene Millman, "The convergence of network and security – how it helps achieve business outcomes," IT Pro, 2024. [Online]. Available: https://www.itpro.com/security/the-convergence-of-network-and-security-how-it-helps-achieve-business-outcomes

[2] IBM, "Cost of a Data Breach Report," IBM Security, 2024. [Online]. Available: https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec

[3] Hewlett Packard, "The 2023 Global Study on Closing the IT Security Gap: Addressing Cybersecurity Gaps from Edge to Cloud," HPE, 2023. [Online]. Available:https://www.hpe.com/psnow/doc/a00130892enw

[4] Tech Target, "2024 Technology Spending Intentions Survey," Enterprise Strategy Group by Tech Target. [Online]. Available: https://www.techtarget.com/esg-global/wp-content/uploads/2024/02/Infographic-2024-Technology-Spending-Intentions-Survey.pdf

[5] Cisco, "Security Outcomes Report," Cisco Systems, 2023. [Online]. Available: https://www.cisco.com/c/en/us/products/security/security-outcomes-report.html

[6] MarketsandMarkets, "Security Service Edge Market," Markets and Markets, 2025. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/security-service-edge-market-186280780.html

[7] Grand View Research, "Network Equipment Market Size, Share & Trends Report Network Equipment Market Size, Share & Trends Analysis Report By Component (Hardware, Software), By Connectivity (2G/3G, 4G LTE), By Network Type, By End-user, By Region, And Segment Forecasts, 2023 - 2030," Grand View Research Insights. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/network-equipment-market-report

[8] Gartner, "Single-Vendor SASE (Transitioning to SASE Platforms) Reviews and Ratings," Gartner Research. [Online]. Available: https://www.gartner.com/reviews/market/single-vendor-sase

[9] Jeremy Dodson, "The Future Of Cybersecurity: Emerging Threats And How To Combat Them," Forbes Technology Council, 2024. [Online]. Available: https://www.forbes.com/councils/forbestechcouncil/2024/07/11/the-future-of-cybersecurity-emerging-threats-and-how-to-combat-them/

[10] Jim Boehm et al., "Cybersecurity trends: Looking over the horizon," McKinsey & Company, 2022. [Online]. Available: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon

[11] Cisco, "2024 Global Networking Trends Report," Cisco Systems, 2024. [Online]. Available: https://www.cisco.com/c/dam/global/en_uk/solutions/enterprise-networks/2024-global-networking-trends.pdf

[12] DXC Technology, "How to keep security operations centers relevant through changing times," DXC Technology. [Online]. Available: https://dxc.com/us/en/insights/perspectives/paper/how-to-keep-security-operations-centers-relevant-through-changing-times.