



The State of Network Security in Manufacturing

Key Findings on Visibility,
Resource Constraints, and
Cyber Resilience



CONTENTS

Executive Summary	03
Introduction	04
Who We Surveyed	05
Key Findings	06
Strategic Recommendations	13
Concluding Thoughts	14



Executive Summary

The Network Security Trends in Manufacturing Survey, conducted from August to October 2024, offers a comprehensive look into the priorities, challenges, and future direction for global manufacturing technology leaders. From CxO-level executives to network engineers, these stakeholders play a vital role in shaping their organization's network security.

The findings highlight a shift toward optimizing network visibility, enhancing secure global connectivity, and reducing costs by consolidating network and security functions. For manufacturing's distributed operations—with dozens of networked facilities across regions—effective network security is a strategic imperative. Yet, many respondents face challenges, including resource limitations, managing cyber threats, and modernizing network infrastructure cost-effectively.

While many companies are adopting cloud and hybrid environments, most still operate in mixed data setups due to legacy systems, creating both opportunities and challenges for implementing solutions that support multi-cloud and hybrid data centers, secure site-to-site connectivity, and improved network observability.

A key insight is the rising interest in converging network and security functions, identified as essential for strengthening network security and lightening IT workloads. Despite this, many companies remain in early evaluation stages for Secure Access Service Edge (SASE) solutions.

Cheers,

Team Aryaka

Introduction

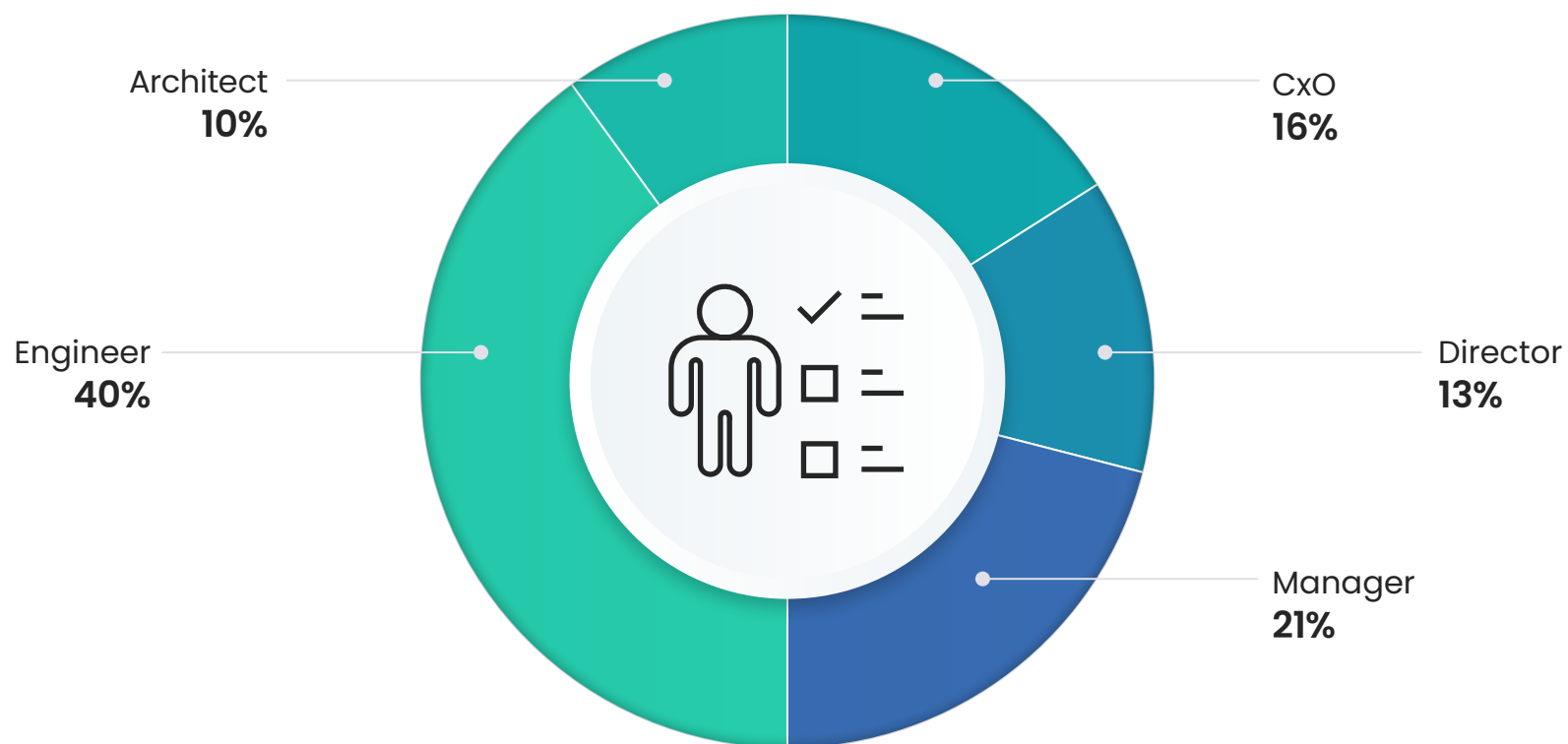
In today's increasingly digital and interconnected world, manufacturing enterprises are tasked with securing complex and distributed networks that support factories, warehouses, branch offices, and a globally dispersed workforce. This paper analyzes insights from senior manufacturing executives on key networking and security trends, challenges, and the potential impact of adopting converged network security solutions. The surveyed responses provide a unique look into the current and future state of network security in manufacturing, with emphasis on cost efficiency, visibility, and secure global connectivity.



Who We Surveyed

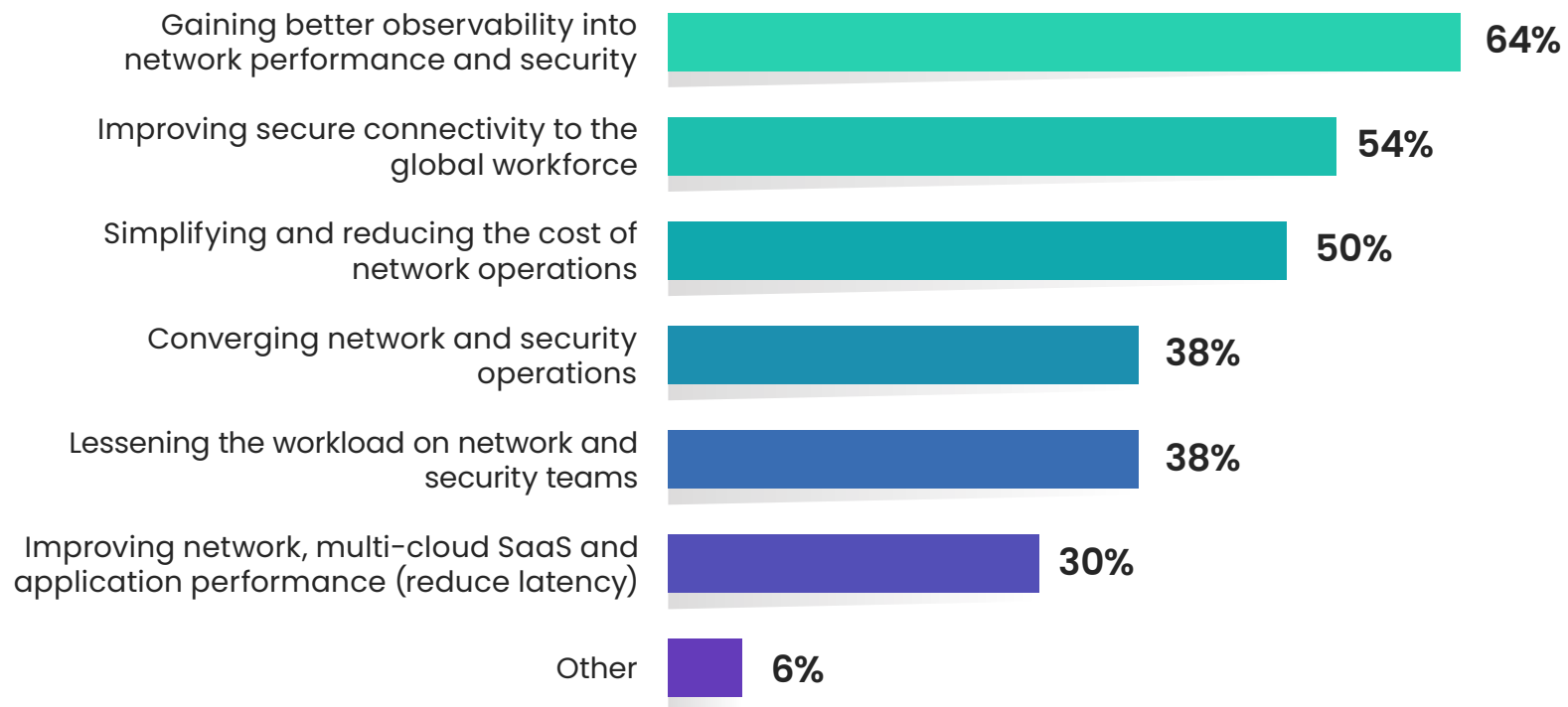
Our survey included a wide range of networking and security professionals from manufacturing companies with connected facilities in North America, Europe, and Asia-Pacific.

Respondents occupy roles central to the progression of converging networking and security. From the leaders who are aligning the IT strategy with the business goals to the ones implementing and managing the secure networking systems, this survey touched multiple stakeholders.



Top priorities for manufacturing industries are operational and cost driven

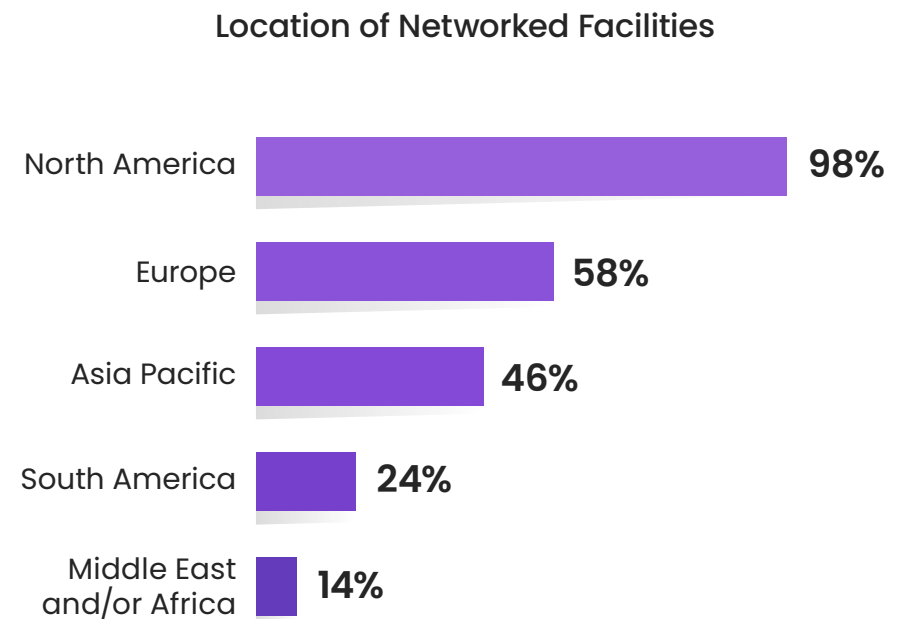
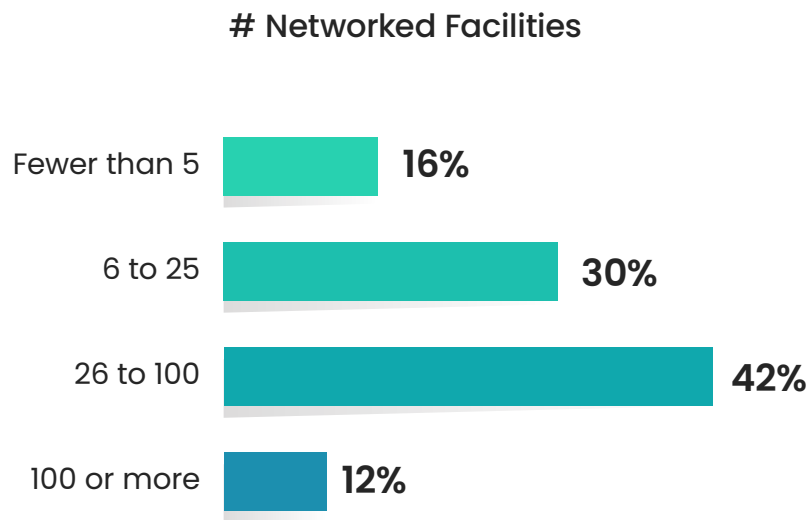
What are your top three networking and network security priorities in the next 12 months?



Implications: As manufacturing networks become more complex, organizations are investing in observability and secure connectivity to protect against cybersecurity threats and operational disruptions. The trend toward integrated solutions (such as Aryaka's Unified SASE as a Service) is fueled by the need for cohesive network management that enhances visibility and reduces the administrative burden

Most manufacturing companies have large global networks creating multiple challenges

How many network facilities do you have and where are they located?

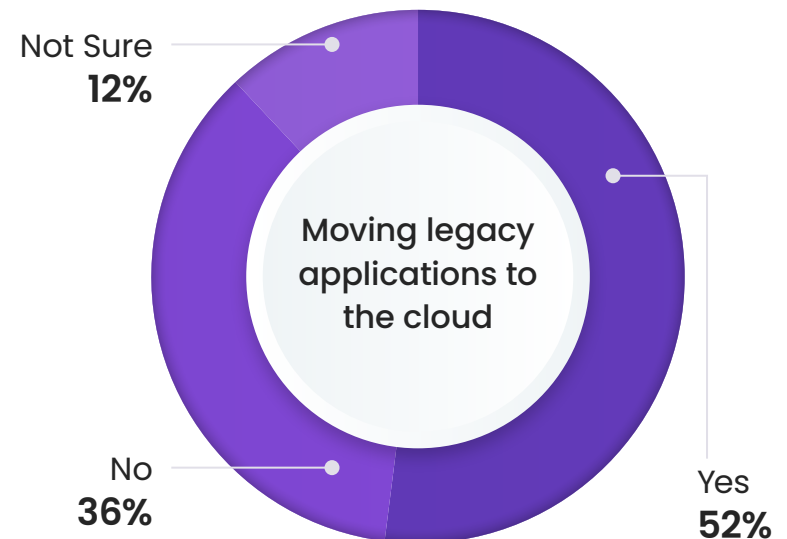
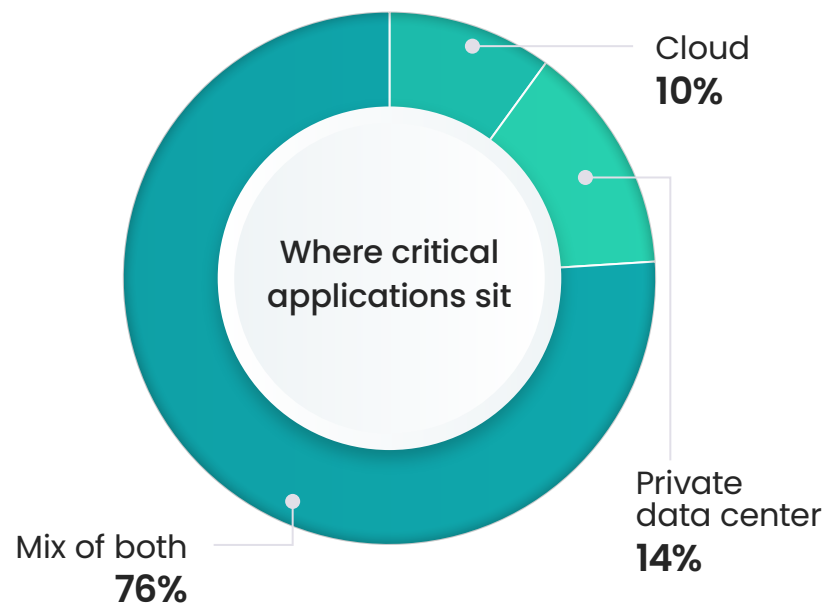


Implications: This broad geographic distribution emphasizes the need for scalable and secure network infrastructure that can support operations across multiple regions.

Application environments will continue to be “hybrid”

Where do your critical applications sit and are you moving legacy applications to the cloud?

A predominant 76% of respondents maintain a hybrid environment, combining cloud and private data centers to support critical applications, while only 10% have fully moved to the cloud. Additionally, over half (52%) are on a migration path for legacy applications, with another 36% maintaining traditional, on-premises solutions.

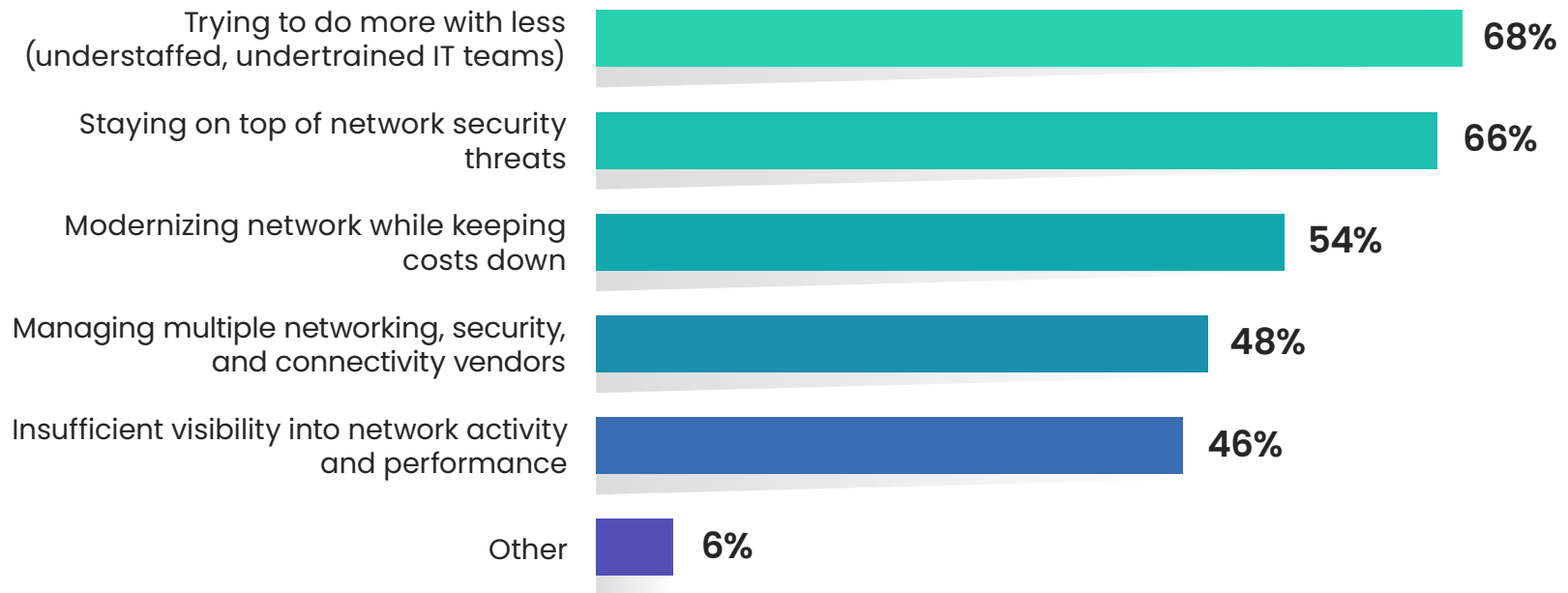


Implications: Manufacturing organizations are gradually moving toward cloud adoption, but hybrid environments remain prevalent due to legacy system requirements. This hybrid model underscores the need for flexible and secure connectivity solutions that can integrate seamlessly across different environments.

Teams face significant operational challenges

What are your top three day-to-day networking challenges?

Teams are facing significant operational challenges including Resource Limitations, Cybersecurity Threats, and Cost-Effective Modernization.

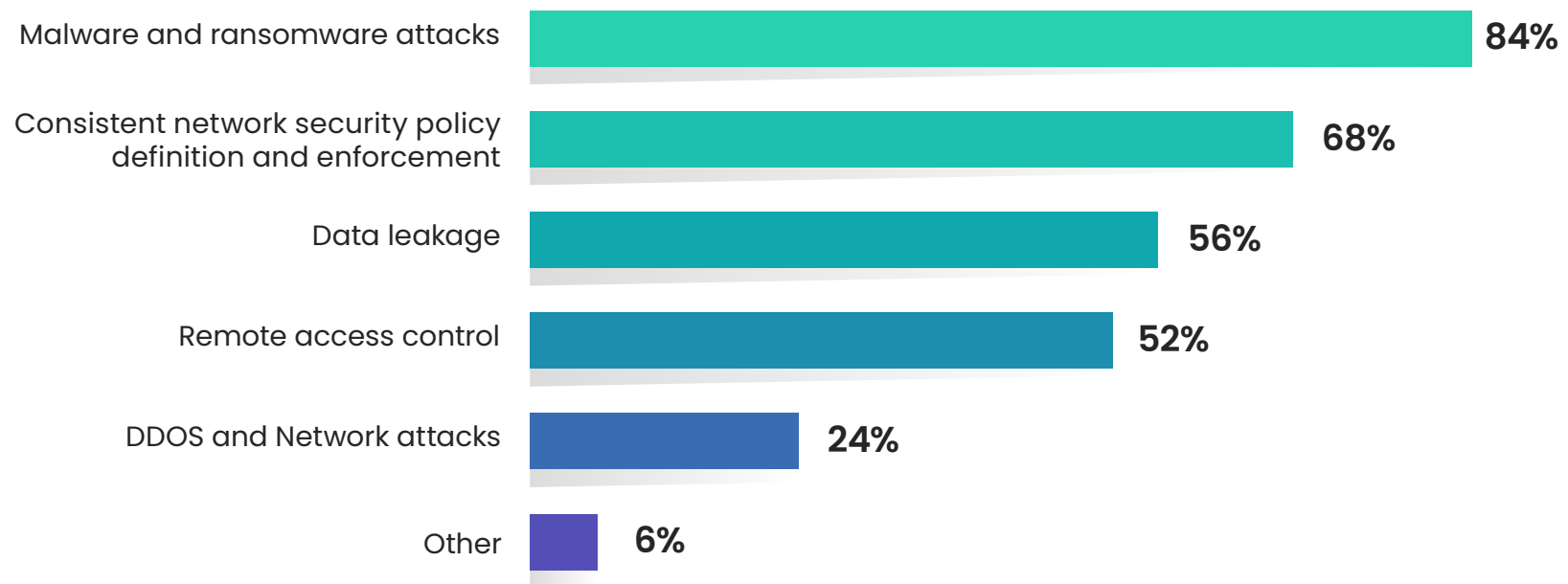


Implications: The reliance on limited IT resources to manage both network operations and cybersecurity risks is a major issue. Integrated management and security functions, along with co-managed services can ease the workload on IT teams while modernizing the secure network in a cost-effective manner.

Organization have significant security concerns

What are your top three networking security concerns?

Among security concerns, malware and ransomware attacks top the list (84%), followed by data leakage and policy enforcement.

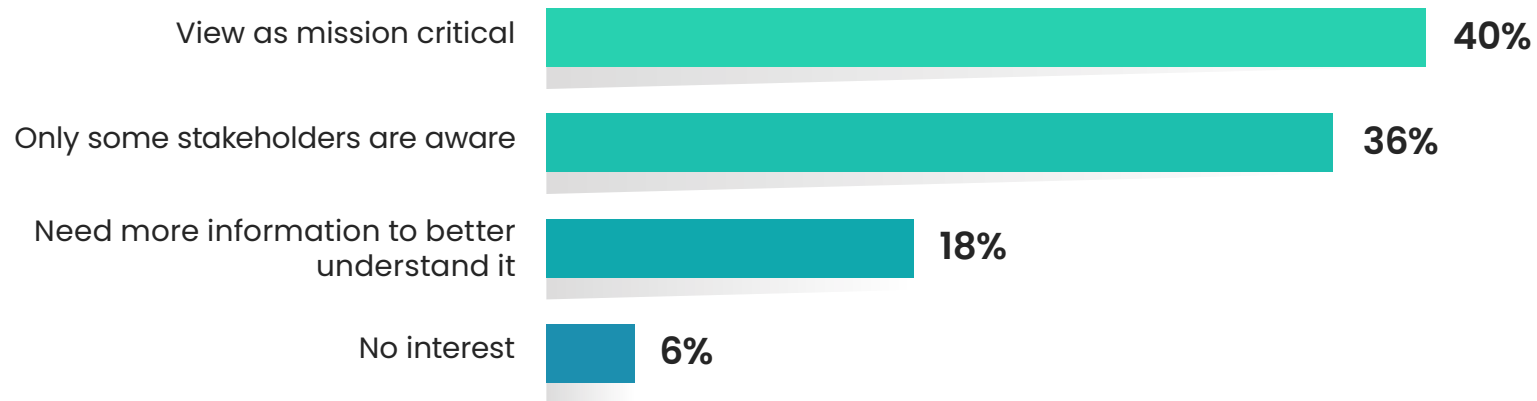


Implications: Manufacturers face rising security threats, despite their limited resources to protect against them. They must increase their readiness and reduce their risk profiles.

There is lagging awareness and priority on the security edge

What is your IT organization's perceived value of implementing application security at the network edge?

The understanding of the value of application security at the network edge is mixed with only 40% considering it mission-critical. However, 36% report that only some stakeholders in their organization are aware of its importance, indicating a need for greater education and alignment around the benefits of edge security

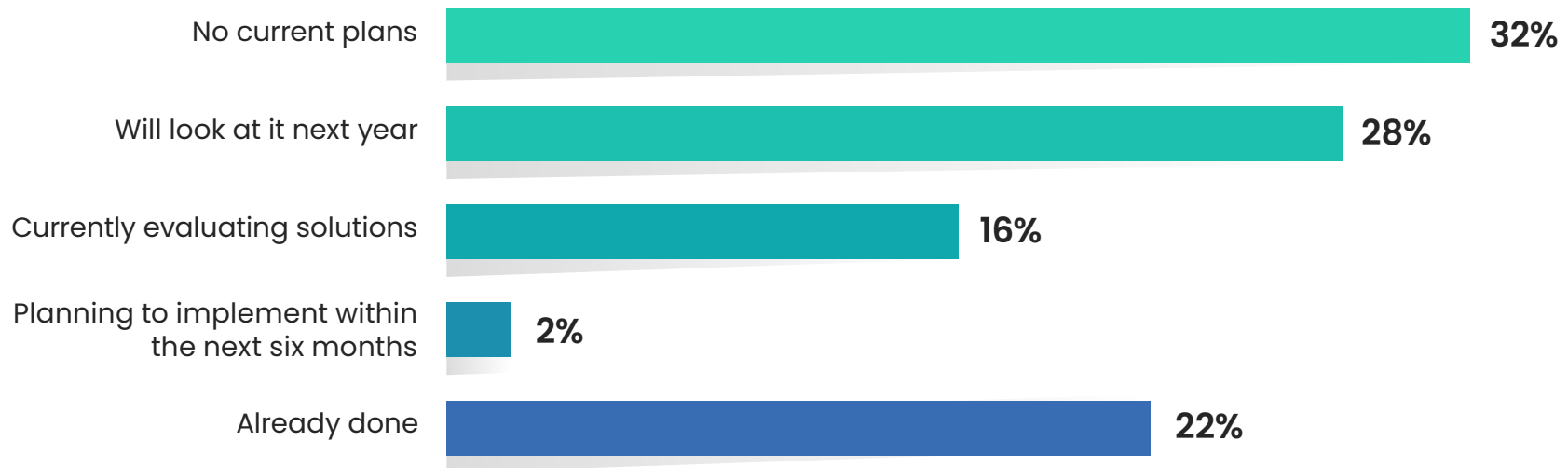


Implications: Unified SASE solutions which integrate application security and performance at the network edge provide manufacturing enterprises with a practical way to secure applications in hybrid environments, protecting against both internal and external threats.

Adoption of converged solutions is a mixed bag

When do you plan to implement a converged networking and security solution such as Secure Access Service Edge (SASE)?

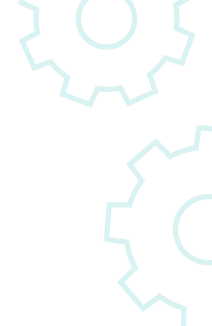
While 22% have reported adoption converged networking and security solutions such as SASE, and another 50% are in some state of investigation, a surprising 32% have no plans to do this.



Implications: Despite the compelling reasons to do so, adoption is lagging. This may suggest that resource and budget limitations, whether real or perceived, are slowing adoption. Many organizations should look at managed or co-managed to mitigate these type of concerns.



Strategic Recommendations



To help manufacturing organizations overcome these challenges and optimize their network security, we recommend:

1

Investing in Visibility Solutions

Enhanced network observability allows organizations to proactively address security risks and improve operational efficiency.

2

Using Managed Security Services

A managed Unified SASE model, such as Aryaka's, reduces the resource burden on internal IT teams, enabling them to focus on strategic initiatives.

3

Strengthening Edge Security

Securing applications at the network edge provides greater resilience against threats in a hybrid environment.

4

Converging Network and Security Tech and Operations

Consolidating network and security functions OR creating more cross-team collaboration can lead to cost savings, reduced operational burden, and improved security outcomes.

Concluding Thoughts

This survey highlights the critical role of network security in manufacturing, with a clear shift toward solutions that emphasize visibility, cost-efficiency, and secure global connectivity. Solutions such as Aryaka Unified SASE as a Service offers a comprehensive solution to these challenges, enabling manufacturing enterprises to strengthen their network infrastructure while supporting digital transformation and cloud adoption. As the manufacturing sector continues to evolve, leveraging converged network and security solutions will be essential for sustained competitiveness and resilience.





About Aryaka

Aryaka is the leader and first to deliver Unified SASE as a Service, the only SASE solution designed and built to deliver performance, agility, simplicity and security without tradeoffs. Aryaka meets customers where they are on their unique SASE journeys, enabling them to seamlessly modernize, optimize and transform their networking and security environments. Aryaka's flexible delivery options empower enterprises to choose their preferred approach for implementation and management. Hundreds of global enterprises, including several in the Fortune 100, depend on Aryaka for cloud-based software-defined networking and security services.

For more on Aryaka, please visit www.aryaka.com.

info@aryaka.com | +1.888.692.7925

