Publication date:
May 2022
Author:
Roy Illsley
Rik Turner

Assessing the Value of Network Segmentation from a Business Application Perspective

Brought to you by Informa Tech

Assessing the Value of Network Segmentation

Omdia commissioned research, sponsored by AlgoSec

Contents

Summary

Introduction

The move to adopt edge, cloud, and cloud-native technologies has brought to the forefront the criticality of security technology alignment. Even more importantly, it has underlined the need to ensure security policies can be applied and enforced. Subsequently, the concept of micro-segmentation as an approach to cloud-native security has gained traction among security experts, but being able to deliver it operationally is still seen as a work in progress by network and SecOps teams. Its adoption is driven by the growing use of cloud computing and, in particular, by the growth of cloud-native workload formats such as containers and serverless.

This research looks at the current state of micro-segmentation and sheds light on the merits of an application-centric approach to its use in enterprise environments.

Introduction to micro-segmentation

As a concept, micro-segmentation offers a proactive approach to security by setting up guardrails around workloads and data stores.

Typically, the ideal deployment for micro-segmentation is done before application production as part of an overall DevSecOps strategy and can be applied to application infrastructure that resides either on or off an organization's premises.

An application can be made more efficient by splitting it up into short-lived components that are used only when needed and then discarded. However, the danger in doing so is that it could expand the target area for cyberattacks, also known as the attack surface. In this scenario, proactive security becomes a necessary cyber-defence tool for security teams, enabling them to reduce that attack surface and, ideally, to focus their reactive security platforms on a smaller number of alerts. The research that underpins this white paper shows that micro-segmentation is the primary type of proactive security in the minds of chief information security officers (CISOs) across the geographies Omdia surveyed.

The technology is not, of course, without its challenges, particularly in the areas of policy management and orchestration. By virtue of its granularity, micro-segmentation tends to promote a proliferation of security policies specific to individual workloads. Given the sheer number of policies, together with the interrelationship between them, this becomes a major challenge in its own right. The question therefore arises whether such technology platforms that support a micro-segmentation approach are sufficient or whether there should be broader guardrails to secure more critical assets such as the applications on which the business runs. That is the question this research paper looks to settle.

The research

Omdia conducted a survey of more than 150 qualified respondents across five countries: the UK, France, Germany, the US, and Canada. The survey was focused on enterprise organizations that had annual revenue in excess of $1bn.

Why network segmentation is critical

Omdia research (IT Enterprise Insights survey 2021, with 4,971 respondents) shows that the use of cloud computing has increased significantly since 2019. Approximately 25% of workloads ran in off-premises public cloud in 2019, with 75% of workloads executing on-premises. However, the impact of the COVID-19 pandemic accelerated organizational workload migration plans, and in 2022 44% of workloads were executing off-premises in some form of public cloud.

This increase in the use of cloud computing has also seen a corresponding increase in the use of cloud-native technologies such as Kubernetes. In fact, adoption of cloud-native technologies, according to Omdia's 2021 IT Enterprise Insight global survey, showed a 6-percentage-point swing from the use by enterprises of virtual machines (VMs) to cloud-native microservices between 2019 and 2022.

The use of cloud, and cloud native in particular, introduces new and different security challenges caused by the complexity and number of services being managed. In the VM monolithic world, the application executed as a single image; in a microservices world the same application is executed as hundreds or thousands of separate images. Therefore, the securing and management of these images requires new and different thinking, such as micro-segmenting the network and adopting the concept of zero trust.

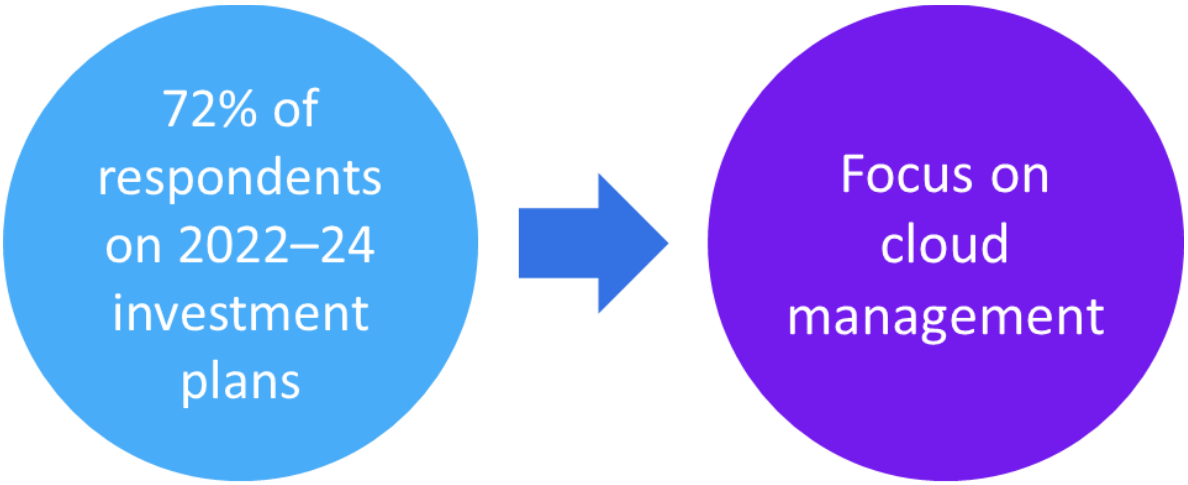
The use of these approaches alone represents a shift in security thinking, but when they are combined with the increased use of edge computing, the application landscape becomes a complex mixture of

- The number of services
- The interrelationship between these services
- The distribution of the services

Figure 1 shows the results from the network segmentation survey, indicating that the top IT investment priority in 2022 is cloud management: 72% of respondents stated they plan to increase investment in the 2022–24 timeframe, while 25% reported that investment would remain flat. Significantly, no respondent reported a decrease in cloud management spending. This response demonstrates that CIOs understand that the main challenge of the move to cloud and cloud-native technologies is how to manage these environments. This focus on cloud management is driven by two key needs:

- The need for the management activities to be simplified so that CIOs can deal with the resource and skills issue they are currently experiencing
- The need to transform the operational activities to become more aligned with the reality that the world is a complex mixture of off-premises and on-premises environments, which must be managed in a holistic and secure manner

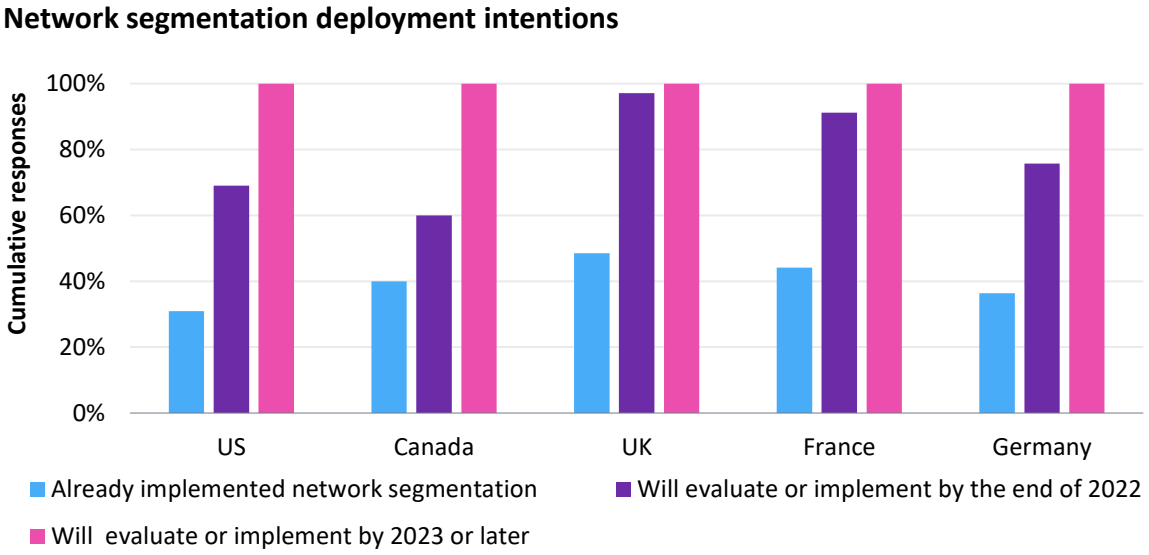
Figure 1: IT investment priorities 2022–24



Source: Omdia

What is the current state in organizations?

Figure 2: All respondents are considering deploying network segmentation in the near future



Source: Omdia

The survey was consistent in that organizations identified network segmentation, and micro-segmentation in particular, as a new and immediate change needed to protect the digital enterprise. On average, Europe reported it has already deployed micro-segmentation in a greater number of organizations than North America. In fact, the survey found 80% of organizations in Europe (see **Figure 2**) expect to have fully implemented network segmentation by the end of 2022. While the North American market is slower to adopt the approach, the majority there (over 60%) report it will be implemented in 2022.

Deeper analysis of the data shows the reason why North America appears to be lagging behind Europe: a number of respondents were not primarily responsible for network management. In the US, the respondents whose primary area is network management overwhelmingly indicated earlier adoption of micro-segmentation: 43% reported they will implement by the end of 2022, whereas only 25% of those whose primary responsibility was not network management said they would

implement it by the end of 2022. The average across all respondents and all geographies between these two groups did not show much difference: 43% of non-network-management respondents expected to implement by the end of 2022, against 41% of those respondents who were primarily responsible for network management.

Why segment the network?

The drivers for network segmentation demonstrated some interesting insights into how CIOs consider the technology. The need to ensure services are not hurt by cyberattacks is a key driver for the use of micro-segmentation, with ransomware being the top concern.

This demonstrates a very serious issue for enterprise organizations, namely the fear that malicious attacks, and ransomware in particular, will have real business impact. CIOs expressed concern over the ability of potential bad actors or malware to move laterally in the network and infect a much wider population. They consider compartmentalisation to be an approach that can restrict any such incursion. Omdia also sees this as a driver behind the move to cloud native, because it is seen as an approach that can distribute or dilute the attack surface.

It may seem counterintuitive that breaking the monolithic application into smaller microservices can improve security. However, because these microservices are segmented, organizations can apply security at this more granular level and thus increase the security of the whole application.

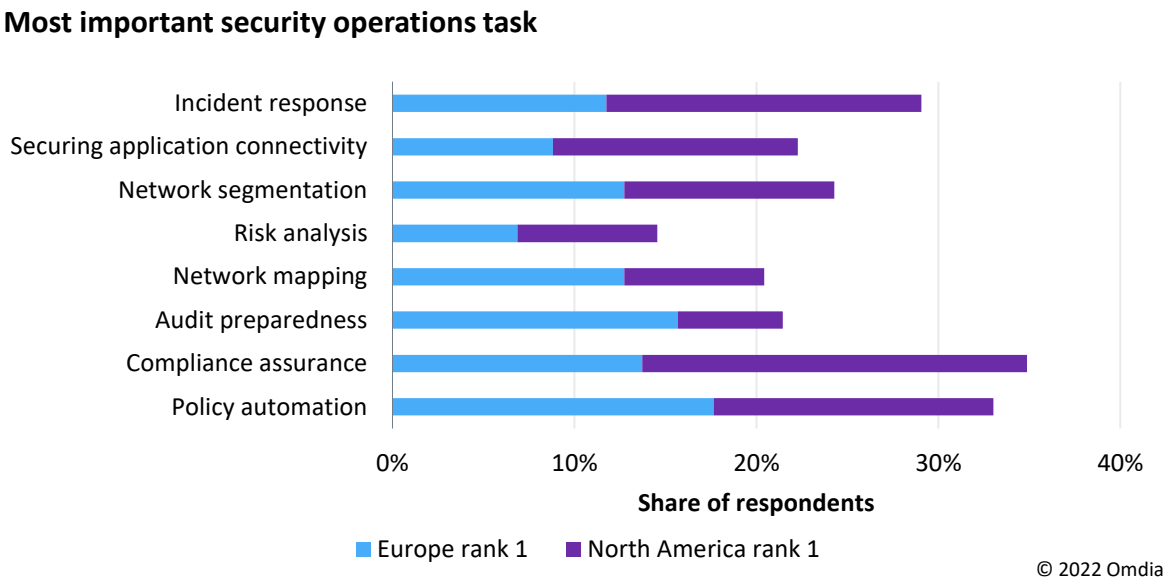
While the use of micro-segmentation is viewed as a pragmatic and easy-to-deploy solution, it is not without its challenges. For example, it can require highly skilled people, and the management of the policies requires tools that can deal with orchestrating the governance.

The sheer number of policies and the interrelationship between them is a major challenge that micro-segmentation introduces to the security management activities. Therefore, what CIOs are expecting from any micro-segmentation solution is a simple approach to policy management and orchestration.

Interestingly, the survey found that the use of micro-segmentation as a solution to help solve the skills gap was the lowest-ranked driver. Omdia considers that this finding fits with the view that bad actors and malware being able to spread through an organization's infrastructure is a threat, and the skills issue can be overcome through the use of tools that simplify the tasks.

The connection between micro-segmentation and security

Figure 3: Respondents' security priorities in Europe and North America



Source: Omdia

Micro-segmentation can be thought of as a proactive approach to security, in that it aims to create specific access rights to a given workload or data store, limiting them to the absolute minimum required for an application to function with the desired effect and business outcome within an organization. The system imposes restrictions a priori, rather than waiting for an attack to take place and remedial action to be taken.

It is no coincidence, in this context, that micro-segmentation is considered to be a manifestation of the zero-trust approach to security. The spirit of zero trust is 'Trust no-one (and nothing, i.e., no system), always verify that the access request is legitimate, and continuously monitor the session to detect any anomalous behaviour after access has been granted,' which clearly coincides with how micro-segmentation approaches the problem of workload security.

By minimally enabling access, micro-segmentation can be used to reduce, as far as possible, an organization's attack surface before any exploit or breach has taken place, and as such it fits within the universe of proactive security technologies that have grown up to complement the reactive ones of the detect-and-respond (DR) approach that have held sway for most of the last decade, such as EDR, NDR, and XDR.

These proactive platforms should not be thought of as a potential replacement for the reactive ones, however, but rather as a complement to them. In other words, by reducing an organization's attack surface before any attack has taken place, they leave the reactive platforms in the DR spectrum free to address a potentially smaller universe of threats and thus can promote greater efficiency from such products.

It is significant that both the top and second-placed SecOps tasks in **Figure 3** (i.e., policy automation and compliance assurance) can be addressed with a proactive approach. Incident response (IR), which is of course reactive, comes in third overall and even lower than that in Europe, where other requirements such as audit preparedness rank higher than IR.

Network segmentation challenges

The biggest challenge for CIOs with the deployment of micro-segmentation is the potential impact on the business: 22% of respondents put it top of the list. This leading concern demonstrates the conundrum that organizations are facing. The threat of bad actors and ransomware and their potential to damage business operations was the top driver for the deployment of micro-segmentation. However, deploying micro-segmentation is not without its own issues, most notably the ability to disrupt business activity because of the sheer scale of the operation.

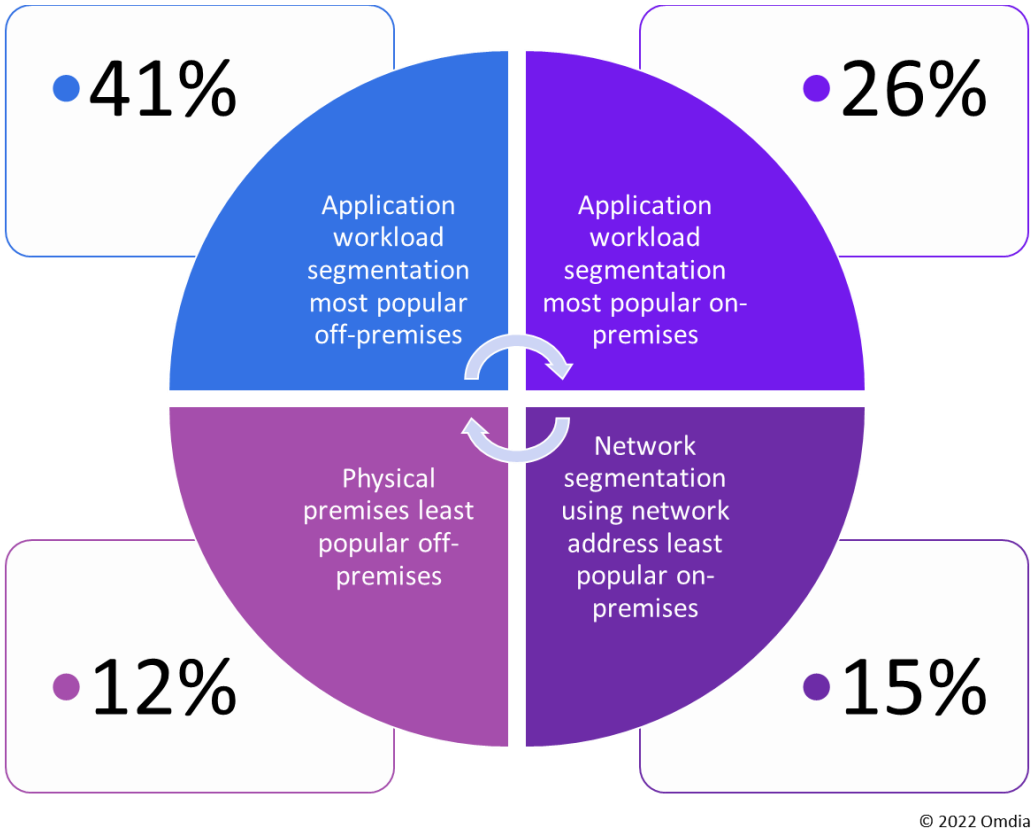
The second most significant challenge was avoiding vendor lock-in, which 18% of respondents put as their top concern. On deeper analysis, we can see this was driven by the US, where it was the most significant challenge for 25% of respondents, while in Europe it was only the third most significant challenge, with a 15% score.

The only other two concerns to record double-digit responses were staff resistance to change, at 12%, and lack of senior management support, at 13%. In Europe, the lack of senior management support was the second most important concern for 16%, while in North America it ranked only fifth, with 8% of respondents.

This difference in support from senior management appears to indicate that North America should be more advanced in the use of micro-segmentation, but as **Figure 2** shows, the opposite is the case. The conclusion to be drawn from this is that senior management support does not have an impact on the deployment of micro-segmentation.

Application-based segmentation is the leading approach to segmentation

Figure 4: How organizations are segmenting the network



Source: Omdia

The survey found (see **Figure 4**) that micro-segmentation, or application workload segmentation, is the most popular approach being considered by organizations. This was the most popular for both off-premises and on-premises workloads. In fact, 41% of respondents reported micro-segmentation

was used for off-premises workloads, and 26% that it was used for on-premises workloads. On-premises is lower, in terms of popularity, than off-premises because the on-premises workloads are a mixture of cloud native and legacy, which means different technologies will be used for network segmentation that is appropriate for different types of applications. Overall, a third of respondents selected micro-segmentation, which is nearly twice the score of the next most popular approach.

France was the biggest user of micro-segmentation off-premises: nearly 50% of respondents reported using it. Canada, with 33% of respondents using micro-segmentation off-premises, was the smallest user of the approach. However, 33% of respondents were using it for on-premises environments, and Canada was the biggest user of micro-segmentation in that scenario. Meanwhile France and the UK, with 20% of respondents, were the smallest on-premises users of the technology.

The reason why the usage rates of on-premises and off-premises use of micro-segmentation should be polar opposites requires deeper analysis, which this survey did not cover. However, Omdia believes that this finding is related to the relative use of cloud-native workload formats by the different countries.

Appendix

Author

Roy Illsley
Chief Analyst, Cloud and Data Center Research
customersuccess@omdia.com

Rik Turner
Senior Principal Analyst, Cybersecurity
customersuccess@omdia.com

Get in touch

www.omdia.com
customersuccess@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalise on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa Tech and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.