

WHITE PAPER

Top Priorities for Evaluating Microsegmentation Solutions

By John Grady, Enterprise Strategy Group Senior Analyst

January 2023

This Enterprise Strategy Group White Paper was commissioned by Akamai and is distributed under license from TechTarget, Inc.

Contents

Executive Summary	3
The Microsegmentation Paradox	3
Negative Perceptions Have Slowed Microsegmentation Adoption	4
RFP Checklist: Top Priorities When Considering Microsegmentation Solutions	5
Akamai’s Approach to Microsegmentation	7
The Bigger Truth.....	7

Executive Summary

Microsegmentation holds great promise in delivering improved cybersecurity, particularly as a key component in a comprehensive zero trust cybersecurity model. In order for microsegmentation to deliver those benefits, organizations need to do their homework when evaluating solutions and suppliers.

Although microsegmentation usage has been fairly limited to date—due in part to some lingering misconceptions about microsegmentation’s benefits and some organizations’ use of tools that are not purpose-built for the modern cybersecurity risks—that is starting to change. Other historical challenges, such as perceived cost, lack of understanding of the technology’s benefits, and a dearth of hands-on experience in deploying and utilizing microsegmentation, also are being addressed, making microsegmentation a viable and important part of cybersecurity in general and a zero trust model in particular.

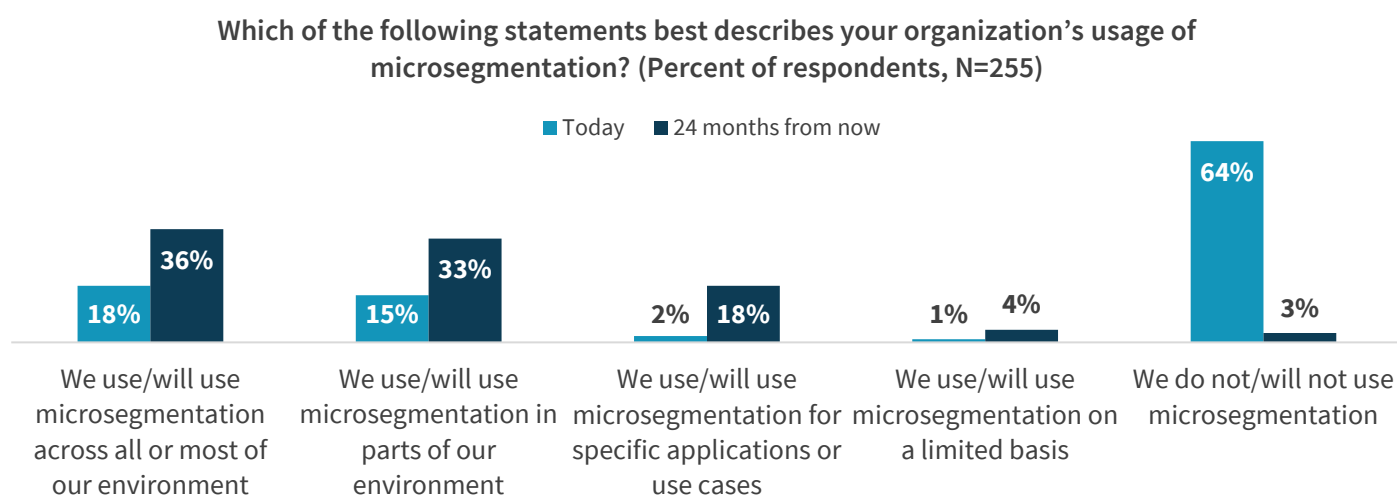
Microsegmentation is both important and relevant because of the technology’s specific ability to thwart attacks by enforcing policy at the network, device, and process levels. Decision makers should build and follow a checklist of top priorities in their journey to successful microsegmentation. Taking this methodical, detailed approach not only can smooth out the inevitable challenges in evaluating solutions and providers, but it can also make it easier for organizations to deploy those solutions quickly and cost-efficiently.

The Microsegmentation Paradox

The importance of zero trust and its applicability to both security and business initiatives makes microsegmentation critical. Yet, despite the many benefits of microsegmentation and its ability to make cybersecurity more robust and flexible, microsegmentation has not yet enjoyed wide and deep adoption at many organizations.

Research from TechTarget’s Enterprise Strategy Group (ESG) points out the beginning of a dramatic and rapid swing toward microsegmentation over the next few years. For instance, while 64% of organizations say they are not currently using microsegmentation, that number will plummet to a mere 3% within two years.¹ Conversely, the percentage of organizations actually using or planning to use microsegmentation across all or most of their environment is expected to double over the next two years, from 18% currently to an anticipated 36%.

Figure 1. Current and Anticipated Adoption of Microsegmentation



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

¹ Source: Enterprise Strategy Group Complete Survey Results, [Network Security Trends in Hybrid Cloud Environments](#), December 2021.

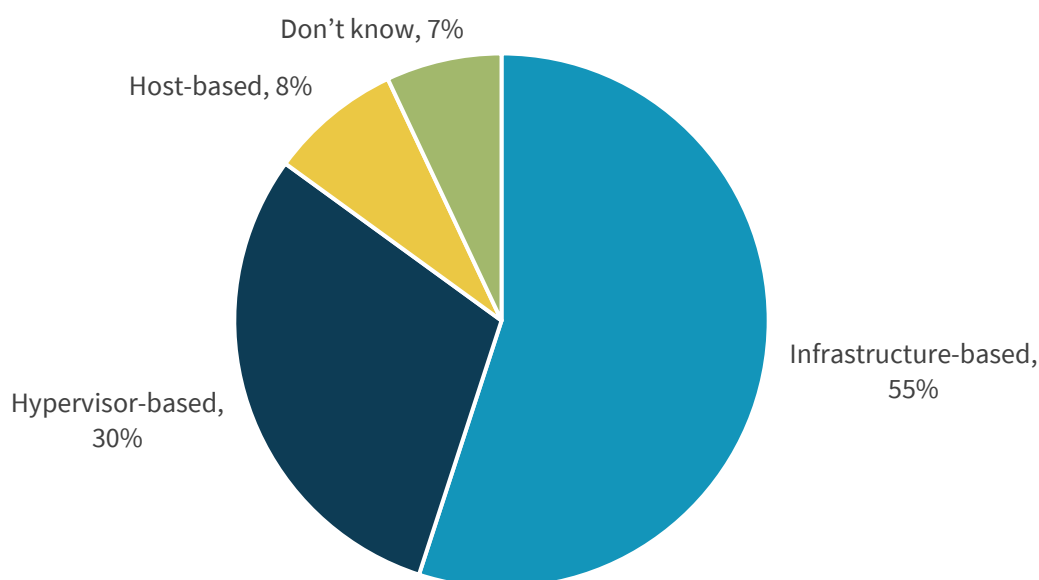
Some organizations are still navigating the landscape of potential segmentation options to determine how best to protect digital assets. Among the different ways organizations are considering implementing proper segmentation are network segmentation, virtual LANs (VLANs), access control lists (ACLs), firewalls, software-defined networking, and microsegmentation. As organizations become increasingly exposed to purpose-built microsegmentation tools and have first-hand exposure to their benefits, the trendlines will likely swing decisively toward broader adoption.

Negative Perceptions Have Slowed Microsegmentation Adoption

Many organizations have attempted to implement microsegmentation with tools that are not purpose-built for the initiative. For instance, there is a wide range of different segmentation approaches, such as ACLs, software-based, host-based microsegmentation, and more (see Figure 2).² While this array of segmentation options is already used to some degree by most organizations, microsegmentation is unique in its ability to pinpoint security by device, data source, cloud gateway, and more.

Figure 2. Types of Tools Used for Microsegmentation

What is the primary technology your organization is using or will likely use to employ microsegmentation? (Percent of respondents, N=255)



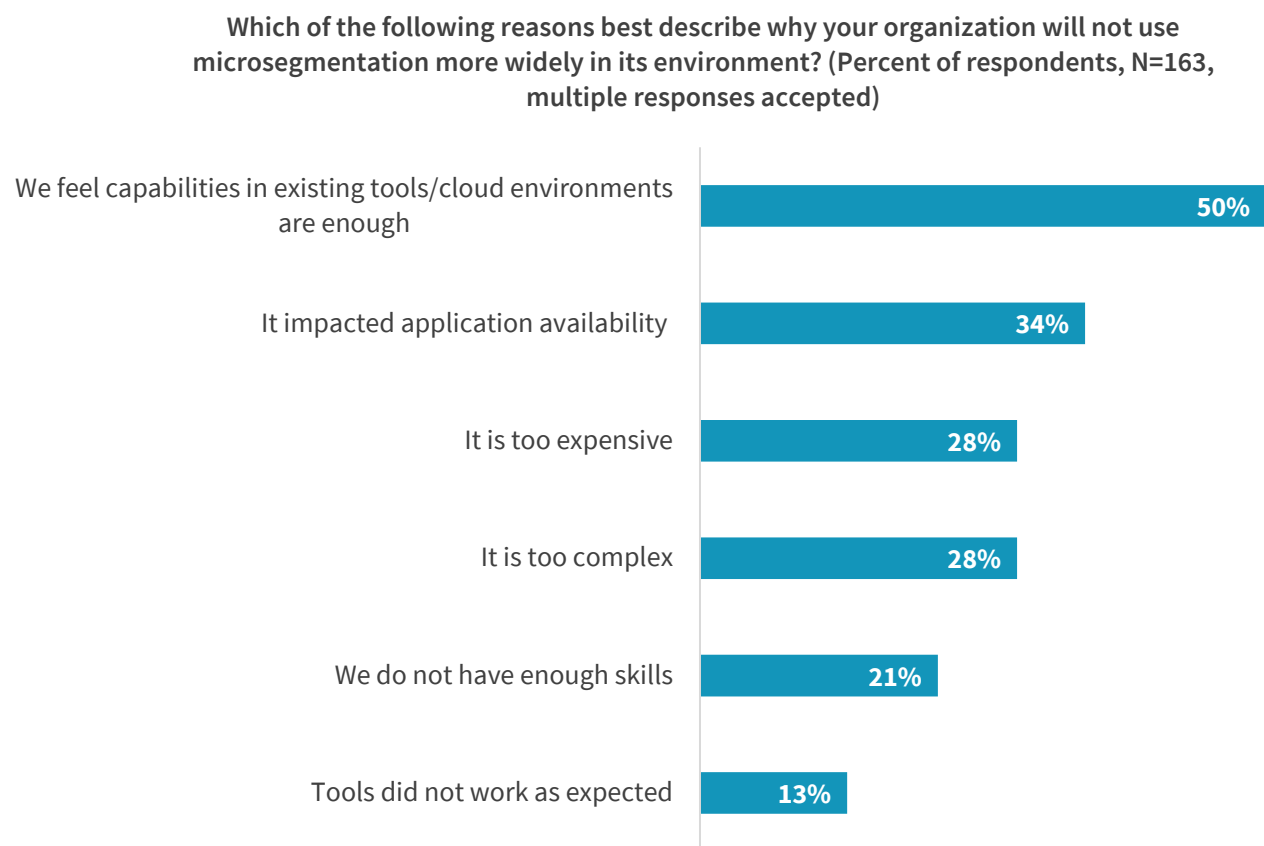
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

According to Enterprise Strategy Group (ESG) research, there are a number of reasons organizations say they have held back on microsegmentation adoption to date, including cost (28%), perceived complexity (28%), and its impact on application availability (34%, see Figure 3).³ It's also important to note that, as organizations increasingly move to a cloud-native profile, lingering misperceptions about the adequacy of cloud providers' native tools are impacting further microsegmentation adoption: 50% of organizations say they believe their existing tools or cloud environments are sufficient cyber defenses.

² Ibid.

³ Ibid.

Figure 3. Reasons Microsegmentation is Not Used More Widely



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

However, there is an important issue to consider: While the different segmentation options each bring their own value to the equation, microsegmentation is one option that organizations should strongly consider. Certainly, decision makers need to weigh how much effort they need to deploy a potential solution, compared with how much potential benefit they hope to achieve. One of the things organizations may not fully realize until they have done an appropriate analysis is that the cost-benefit ratio for microsegmentation is better than they might anticipate—specifically, it provides greater economic and operational value, while requiring less effort to deploy than expected.

RFP Checklist: Top Priorities When Considering Microsegmentation Solutions

Of course, the first step in the process is to understand and prioritize the most important factors to the organization when they are considering adopting a particular microsegmentation solution. In order to get the most from microsegmentation as an enabler of zero trust cybersecurity models and to create a more flexible, adaptable, and scalable cybersecurity framework, organizations need purpose-built, host-based solutions that can alleviate many of the aforementioned issues.

Here are 8 specific attributes organizations should look for when evaluating microsegmentation solutions:

1. **Visualization and mapping.** The first step in any microsegmentation project should be understanding the workloads and entities in the environment and the relationships between them. Establishing this baseline and providing an intuitive and interactive visualization for security teams to work with can help them quickly identify key gaps, potential issues, and areas to prioritize.

2. **Ease of implementation and management.** Enterprise Strategy Group (ESG) research has found that 25% of organizations cited automation of policy creation/management and 23% of organizations cited ease of deployment as top attributes for tools supporting zero trust.⁴ As noted earlier, a perception exists among some organizations that microsegmentation can be complex and difficult to deploy. Compounding this issue, many security teams are overworked and under-resourced. Microsegmentation solutions that alleviate these issues can help organizations execute a zero trust strategy and generate quick wins that help build consensus to expand the initiative. Based on the information gathered during the visibility phase, microsegmentation solutions should deliver automated policy recommendations, which analysts can then review and accept or modify as needed. This should be augmented by templates for simplified and faster policy creation. Additionally, tools that provide flexible labeling options to shift policy orientation away from IP addresses and toward the application itself have become important as environments have expanded and workloads have become more ephemeral.
3. **Coverage for distributed, heterogeneous architectures.** According to ESG research, 31% of organizations cited coverage for cloud and on-premises environments as a top attribute for tools supporting zero trust.⁵ Enterprise environments have clearly become more distributed and cloud-oriented. Further, modern environments often include not only traditional servers and virtual machines, but cloud-native architectures as well. Many organizations also continue to support legacy operating systems for a variety of reasons. To avoid unnecessary complexity, security teams require the ability to consistently apply protections across all aspects of the environment. Microsegmentation solutions that support not only heterogeneous, hybrid multi-cloud environments, but traditional endpoints and other devices across a mix of operating systems, can help security teams effectively expand a microsegmentation project over time.
4. **Application layer visibility and control.** The nature of network traffic has fundamentally changed over time as applications have become more prevalent, a fact evidenced by the shift to next-generation firewalls at the perimeter. Yet the need for visibility at Layer 7 exists inside the network as well. Networks segmented at Layer 4 can allow attackers to exploit open ports to propagate an attack or exfiltrate data. Through Layer 7 policies, organizations can prevent lateral movement and limit the blast radius in the event of an attack.
5. **AI/ML that works.** ESG research has found that 24% cited artificial intelligence (AI) and machine learning (ML) as a top attribute for tools supporting zero trust.⁶ AI/ML are too often buzzwords, but they are essential for modern microsegmentation solutions. AI/ML can help accurately identify application traffic flows, discover anomalies, inform policy recommendations and workflows, and generally ensure microsegmentation tools can keep pace with increasingly dynamic environments.
6. **Risk assessment.** According to ESG research, 29% of organizations point to risk assessment capabilities as a top attribute for tools supporting zero trust.⁷ While understanding that the relationships between applications and what constitutes normal behavior is core to microsegmentation, supporting a zero trust approach requires additional context. When microsegmentation solutions can layer vulnerability information, reputation, and workload context onto Layer 7 access policies, the organization's security posture is made stronger.
7. **Security-focused capabilities.** Especially in the case of ransomware, security teams do not have a lot of time to react to an attack. Microsegmentation solutions that go beyond simply applying allow/block policies and support

⁴ Source: Enterprise Strategy Group Survey Results, [The State of Zero Trust Security Strategies](#), May 2021.

⁵ Ibid.

⁶ Ibid.

⁷ Ibid.

threat hunting and incident response workflows can provide additional value to security teams. The ability to run queries across the environment to quickly assess the potential impact of an attack and apply pre-defined policies to prevent it from spreading further, all from the same console, can improve response efficiency and mean the difference between managing an incident or managing a breach.

8. **Strong technology ecosystem.** While microsegmentation tools can offer quite a lot on their own, they are made even stronger through integrations with complementary tools. Examples may include configuration management databases (CMDB) to assist with asset classification, vulnerability assessment tools for risk assessment, identity tools for user context, DevOps and CI/CD tools to support automation, and other network and endpoint controls additional enforcement capabilities.

Akamai's Approach to Microsegmentation

[Akamai Guardicore Segmentation](#) is a software-based approach to microsegmentation, designed to stop threat actors from achieving lateral movement throughout the digital environment. It uses granular visibility to enforce zero trust principles at the network level, helping organizations visualize activity and movement within the physical and virtual environment.

The solution provides superior visibility via automated application discovery, customizable maps, and granular historical and real-time data. It supports fast time to policy by supporting both denylist and allowlist models, allowing security teams to start small and gain confidence before applying default-deny policies. Additionally, Akamai Guardicore Segmentation provides policy templates and suggestions which are overlaid across historic traffic over a customizable period to display the impact of proposed policies before they are implemented.

Akamai Guardicore Segmentation can be deployed either in the cloud or on-premises and can support legacy operating systems such as Solaris or AS/400, a variety of Linux and Windows operating systems, virtualization platforms, as well as cloud-native container and platform-as-a-service architectures. Guardicore collects extensive data about the underlying infrastructure in several ways, such as agent-based sensors, network-based data collection, virtual private cloud flow logs, and integrations that promote agentless functionality. Dynamic mapping gives administrators an end-to-end view into activities with coarse granularity.

A variety of technology partnerships help Akamai Guardicore Segmentation support data collection and classification, authentication, and IT automation, and extend enforcement beyond Guardicore's purview. These integrations provide Akamai Guardicore Segmentation additional risk context. The solution is informed by artificial intelligence that assists with application identification and policy recommendations.

The Bigger Truth

Although many organizations understand the importance of microsegmentation in supporting zero trust architectures, microsegmentation adoption has not reached widespread levels due to a variety of misperceptions. However, the trend can—and should—change quickly as organizations gain a better grasp on the many benefits of microsegmentation, particularly as an integral component of an overarching zero trust model.

Organizations that know what to look for in a microsegmentation solution, as well as the use cases where microsegmentation can be applied for a better security framework, stand to benefit substantially.

Akamai should be on your list of potential suppliers to be evaluated for microsegmentation solutions, given their experience in network infrastructure, cloud architectures, and security, especially segmentation and zero trust solutions.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.



Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.



www.esg-global.com



contact@esg-global.com



508.482.0188