

WHITE PAPER

Exploring Key Use Cases for Microsegmentation

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
Zero Trust Gains Traction, But Establishing Clear Priorities Is Critical.....	3
Microsegmentation Is Currently Underutilized in Supporting a Zero Trust Model.....	4
Key Use Cases for Microsegmentation.....	5
Preventing Threats.....	6
Promote Efficiency Across the Business	6
Zero Trust Segmentation.....	7
Akamai’s Approach to Microsegmentation.....	7
The Bigger Truth	8

Executive Summary

Zero trust has become ubiquitous across the cybersecurity industry. Yet, the breadth of the initiative and competing viewpoints on what's most important to the strategy have generated confusion as to where to begin and what tools best support the framework. While there is no single path to zero trust, the strategy is ultimately dependent on ensuring that resources and entities are only able to communicate with one another when expressly permitted by policy, pointing to the importance of microsegmentation.

The use of microsegmentation tools is somewhat limited today but is expected to increase significantly in recognition of the criticality of microsegmentation to zero trust and its applicability to a variety of use cases. Whether organizations are considering zero trust to prevent threats, promote efficiency across the business, or modernize their overall security approach, microsegmentation can help. In particular,

Akamai's software-based and artificial-intelligence-supported approach to microsegmentation provides granular visibility and allows organizations to prevent lateral movement, stop ransomware attacks, and enforce zero trust principles consistently across the entire environment.

Whether organizations are considering zero trust to prevent threats, promote efficiency across the business, or modernize their overall security approach, microsegmentation can help.

Zero Trust Gains Traction, But Establishing Clear Priorities Is Critical

Enterprise environments continue to grow in complexity as resources shift to the cloud, digital business models take hold, and users become increasingly distributed. These changes inherently make the job of the cybersecurity team more difficult, as attackers seek to slip through gaps in defenses to launch ransomware attacks, steal customer information, or exfiltrate sensitive intellectual property. Unfortunately, traditional security approaches predicated on heavily permissive, perimeter-based controls can no longer address these realities, forcing security teams to reevaluate their strategies. Additionally, attacks are growing in number and sophistication, making it impossible for security teams to keep up with, address, and patch against every potential threat.

These issues have led many to the concept of zero trust. While not new, zero trust strategies have seen significant interest from organizations as an avenue toward a more dynamic, least-privileged, and risk-based approach to cybersecurity. A zero trust approach eliminates implicit trust from the environment and continuously validates every digital interaction. As a result, a zero trust approach should give security teams higher confidence that their resources, users, and devices will remain secure and available. Yet the broad applicability of zero trust, coupled with sometimes conflicting views and definitions about what it is, has created confusion and can make it difficult for organizations to identify a starting point.

Assessing organizational priorities and desired outcomes can help narrow the focus and determine where to begin with a zero trust initiative. There are a variety of business drivers pushing organizations toward zero trust (see Figure 1).¹ The most common goal is cybersecurity modernization, cited by

51% of respondents. This mindset has been emphasized by the U.S. federal government through the executive orders on cybersecurity issued by the Biden administration, which called out zero trust architecture in its modernization requirements. While not directly targeted at the private sector, these orders can help provide direction for security teams outside of the federal government. Other strategic goals for zero trust include supporting digital transformation (35%) and

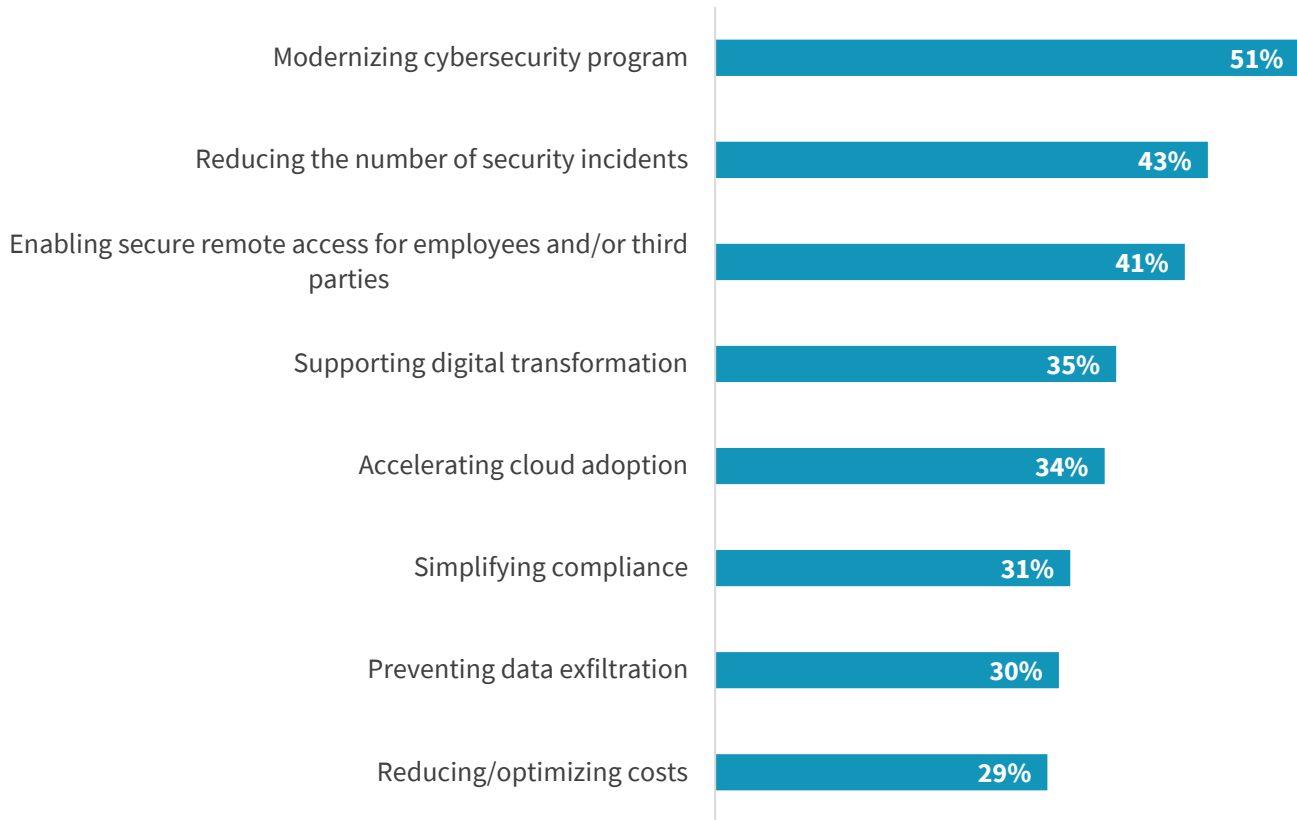
Zero trust is dependent on ensuring that resources and entities are only able to communicate with one another when expressly permitted by policy.

¹ Source: Enterprise Strategy Group Survey Results, [The State of Zero Trust Security Strategies](#), May 2021.

accelerating cloud adoption (34%). These drivers highlight the expectations that many organizations have that the security team should help enable the business, rather than simply protect assets. More tactical goals such as reducing the number of security incidents (43%), enabling secure remote access (41%), simplifying compliance (31%), and preventing data exfiltration (30%) are also common.

Figure 1. Drivers for Zero Trust

Which of the following would you consider to be the top business drivers behind your organization’s adoption or consideration of a zero-trust strategy? (Percent of respondents, N=421, three responses accepted)



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

Narrowing the initial focus of a zero trust project can certainly help the security team identify the tools required to support the strategy, in some cases. For example, if the goal is improving secure remote access for employees and third parties, many will land on zero trust network access (ZTNA). Identity tools such as multifactor authentication (MFA) may also come into play in that scenario. However, some drivers can leave technology requirements open to interpretation, and many organizations, even after narrowing things down, focus on multiple goals. In these situations, it is important for organizations to identify tools and practices that can support a variety of use cases and outcomes.

Microsegmentation Is Currently Underutilized in Supporting a Zero Trust Model

While there is no single path to zero trust, the strategy is ultimately dependent on ensuring that resources and entities are only able to communicate with one another when expressly permitted by policy. This means that a key element to any organization’s zero trust philosophy should be the ability to ensure the proper segmentation of assets to help limit the impact of successful attacks. This could be applicable to a broad goal, such as cybersecurity modernization, or a more focused objective, like preventing data exfiltration.

Yet, in today’s environment, course-grained segmentation is typically not enough, and more granular microsegmentation is required to adequately protect corporate assets. Modern application architectures often rely on workloads distributed across multiple server instances and, in some cases, multiple cloud environments. The practice of segmenting resources based on location has become outdated and does not address the challenges security teams face today.

Historically, organizations have been somewhat hesitant to adopt microsegmentation tools. Research from TechTarget’s Enterprise Strategy Group (ESG) has found that 28% of organizations believe microsegmentation is too complex. However, this is likely due in large part to security teams using the wrong tools for microsegmentation. Specifically, ESG research has found that 55% of organizations report using infrastructure-based tools for microsegmentation, such as firewalls, while only 8% use host-based tools.² Firewalls are unable to enforce the granular policies required for microsegmentation to be successful. In addition, these tools provide limited visibility across application workloads and have difficulty consistently addressing all aspects of the environment across both on-premises and cloud locations.

This has resulted in microsegmentation being underutilized. Despite its criticality to zero trust, only 36% of organizations use microsegmentation today, according to ESG research (see Figure 2). The good news is that many organizations do recognize that this is a significant gap in their defenses. As a result, 91% anticipate using microsegmentation 24 months from now.³ Ultimately, microsegmentation solidifies and reinforces the key benefits of zero trust by buttressing physical, virtual, and cloud networks against both external and internal threats and should be a core component of any zero trust strategy.

Figure 2. Microsegmentation Adoption



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

Key Use Cases for Microsegmentation

² Source: Enterprise Strategy Group Complete Survey Results, [Network Security Trends in Hybrid Cloud Environments](#), December 2021.

³ Ibid.

Microsegmentation is broadly applicable to a variety of zero trust use cases, which is a significant reason why it is being emphasized more than ever. Yet, first and foremost, microsegmentation provides a good starting point to a zero trust journey, as it can secure an organization’s most critical assets, especially if the solution used provides highly granular visibility across workload and entity relationships. Developing a baseline of traffic flows and dependencies is foundational to any zero trust effort as a first step toward removing implicit trust without disrupting the business. This approach allows security teams to quickly secure their most critical assets to help limit the impact in case of a breach while a zero trust implementation is in process. With that assurance in place, security teams can then turn their attention to some of the other use cases microsegmentation supports.

Preventing Threats

Zero trust is a security framework, and the goal of security is to protect the organization against cyber-threats. So, it follows that some of the top microsegmentation use cases center on preventing threats and limiting their impact to corporate resources, specifically:

- **Ring-fencing critical assets.** Security teams must weigh and balance risk when deciding where to prioritize protections. High-value applications that contain regulated customer information, intellectual property, or other sensitive information should receive more attention and heightened security controls due to the potential impact of those systems being compromised. With microsegmentation, security teams can ensure these applications and the workloads that comprise them are completely separated from the rest of the infrastructure.
- **Limiting lateral movement.** An underappreciated tenet of zero trust is working under an “assume breach” mindset by assuming that adversaries have access to the corporate network. The sprawl of traditional endpoints, servers, cloud resources, and even smart devices makes intrusions inevitable. As a result, limiting the blast radius of a potential attack via microsegmentation can deny would-be attackers the ability to move laterally through the network.
- **Threat detection and response.** In the event of an attack, time is of the essence. Microsegmentation tools can help security teams respond rapidly and effectively by quickly understanding potential avenues of attack based on application relationships, blocking the ports attackers use during an attack, and quickly quarantining affected systems from the rest of the network. It also contains the attack to its initial point of entry.

Protecting Against Ransomware

The continued prevalence of ransomware and the impact of these attacks have elevated the issue to an executive, if not board-level, issue. While ransomware preparedness requires not only strong security, but also good data protection and incident response capabilities, microsegmentation can help organizations ensure they are on sound footing to combat an attack. Attackers often target sensitive information and systems in the course of an attack, only after penetrating the environment and taking their time to do reconnaissance. When microsegmentation is used to ring-fence critical assets and limit lateral movement, attackers have less freedom to move throughout the environment. Further, when a ransomware attack is discovered, an organization using microsegmentation can quickly shut down the communication avenues attackers use and isolate infected servers to prevent the attack from propagating further.

Promote Efficiency Across the Business

While the security team’s first goal is to protect the environment, today’s charter also mandates that they do so while not impacting the efficiency of the business. Further, when security teams can actually help enable their colleagues, the business is better for it. This can take on a variety of meanings, but some of the most common include:

- **Supporting cloud adoption.** The shift to the cloud is nothing new, but security concerns do remain top of mind for many organizations. Some of this is due to a lack of familiarity with the native security controls on infrastructure-as-a-service platforms, and some is due to the security inconsistency that can arise in hybrid cloud environments. Microsegmentation gives organizations greater confidence since controls can be used across all aspects of the environment and provide better security consistency in hybrid cloud scenarios.
- **Enabling application modernization.** In addition to the shift to the cloud, the adoption of modern application architectures, such as containers, continues to accelerate. These models allow application teams to design, build, and deploy applications faster than ever. Tools that can ensure these resources are protected, and do so without limiting the speed of developers, create a positive impact on the business. Microsegmentation tools that provide visibility into the traffic flows in container environments and automatically apply segmentation policies as containers are brought online or moved can help development teams ensure their applications are secure.
- **Streamlining compliance.** Regulatory issues take up an increasing amount of an organization's time, budget, and attention. Ensuring that security risks are isolated as much as possible in order to limit the potential for issues, such as data privacy breaches or loss of personally identifiable information, can make the process much less onerous. Microsegmentation can ensure that systems subject to compliance mandates are isolated from the rest of the environment, which can lessen the burden on security teams.

Zero Trust Segmentation

One of the most attractive aspects of microsegmentation is that it can provide immediate value to the organizations when focused on very targeted use cases. The ability to start with denylisting, ringfencing critical applications, environment segmentation, and other less complicated policies that provide quick value with relative ease can be attractive for many. Few, if any, organizations deploy a full microsegmentation strategy across the entire enterprise all at once. But as microsegmentation becomes more broadly deployed throughout the environment in the scope of a zero trust initiative, many organizations will begin to approach zero trust segmentation. This combines the use cases and positive outcomes previously discussed, as organizations are able to maintain comprehensive and granular visibility over traffic flows, protect their most sensitive assets, prevent lateral movement, and respond quickly to threats, all while better enabling the business. While not the starting point for many microsegmentation projects, this should be viewed as a goal to aspire to over time.

Akamai's Approach to Microsegmentation

It is important for organizations to keep in mind that, while microsegmentation is an important aspect of zero trust, there are other key components as well, requiring other technologies supporting threat detection and response, identity, data security, and more. Evaluating, selecting, and working with technology vendors is a detail-oriented, methodical process that can make the difference between

meeting the organization's cybersecurity goals and something that chews up money, time, and labor force resources. As a result, considering microsegmentation tools that offer a broad set of integrations and signal sharing capabilities can help advance a zero trust strategy beyond microsegmentation, as well as reduce operational complexity.

The Akamai Guardicore Segmentation solution is a software-based approach to microsegmentation, designed to stop threat actors from achieving lateral movement throughout the digital environment.

Akamai, a long-established player in network infrastructure, has made [microsegmentation and zero trust core parts of its solutions portfolio](#). The company's knowledge of enterprise infrastructure requirements for both on-premises and cloud environments has included experience in spotting and working through potential cybersecurity challenges.

[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. Its artificial-intelligence-based segmentation framework uses integrated templates to spot and stop incursions, such as ransomware, endpoint-based attacks, and remote workforce-oriented attacks. It can be used on a variety of platforms, including bare-metal servers, virtual machines, containers, IoT devices, and cloud instances.

Akamai Guardicore Segmentation 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. Because of Akamai's experience in enterprise networking environments, Akamai Guardicore Segmentation is designed for enterprise scalability and consistent performance that identifies and side-steps sources of traffic bottlenecks.

The Bigger Truth

Microsegmentation is not a new technology. In reality, it may have been ahead of its time. But the importance of microsegmentation in securing modern hybrid, multi-cloud environments and, specifically, in operationalizing zero trust strategies cannot be overstated. Microsegmentation offers the flexibility, agility, and efficiency necessary to enable zero trust across a number of mission-critical and business-critical use cases, protecting everything from critical infrastructure and intellectual property to identities and credentials. Akamai's experience in network infrastructure, segmentation, and microsegmentation makes it a viable candidate to help plan, build, deploy, and even manage secure infrastructure built upon microsegmentation tools and mindsets.

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