Akamai

Akamai Impact Study 2025

Segmentation Impact Study

Why microsegmentation now defines enterprise cybersecurity, risk, and resilience

Foreword

Global enterprises are accelerating adoption of microsegmentation to guard against growing threats

Smarter, faster-moving cyberthreats, tighter regulations, and rising insurer demands have put network segmentation strategy back in the spotlight, but many enterprises are struggling to keep pace.

In short, enterprise segmentation adoption is high, at a basic level. However, maturity, in the form of microsegmentation, remains low. What is the reason for this disconnect?

Independent research commissioned by Akamai reveals a clear gap between segmentation intent and execution, a gap leaving many enterprises exposed where it matters most. More than 90% of organizations report using some form of segmentation, yet only around 35% have implemented microsegmentation — the level of control needed to contain lateral movement and reduce operational risk.

Many enterprises still rely on legacy north–south segmentation approaches, leaving them vulnerable to growing cyberattacks. Enterprising adversaries are taking advantage of an expanding digital attack surface by using generative artificial intelligence (AI) to develop and sharpen attacks or agentic AI to probe for gaps — or simply purchasing ransomware-as-a-service or malware toolkits on the dark web. As a result, CISOs are allocating a budget to expand segmentation strategies to include east–west approaches to match pace with an explosion in cyberthreats and increased demand from insurers for microsegmentation.

Traditional network segmentation creates broad zones to manage north–south traffic — the traffic flow between external users and internal systems. In contrast, microsegmentation enables enterprises to control east–west traffic and prevent the lateral movement of threats inside the network perimeter. By applying fine-grained policies at the level of individual workloads, applications, and assets, enterprises can prevent attackers from moving freely within their network, strengthen resilience by enabling continuous operations, and reduce the damage of any intrusion.

The good news is that our data shows that awareness of microsegmentation's value is growing. Enterprises increasingly associate segmentation maturity **with lower insurance premiums, faster claims processing, stronger audit readiness, and better ransomware outcomes**. Early adopters, particularly large organizations with mature security operations, are already realizing these advantages.

Yet adoption remains uneven. Many organizations face entrenched barriers: complexity, resource constraints, competing priorities, and cultural resistance. These frictions slow progress, but the direction of travel is clear. **Half of non-adopters plan to implement microsegmentation within two years. Two-thirds of current adopters expect to increase their investment**. The market is shifting decisively from experimentation to strategic deployment.

Microsegmentation has long been recognized as a foundational control for Zero Trust architecture. Our research reinforces this established role, highlighting how microsegmentation enables workload-level security that aligns with Zero Trust principles of continuous verification and least privilege.

As cyberthreats grow more dynamic and the perimeter dissolves, organizations need embedded security that scales at the workload level. Microsegmentation delivers that control without adding operational burden.

Our research highlights the drivers, barriers, and benefits shaping adoption — and why microsegmentation is now essential to build lasting resilience in a threat landscape where delay is fraught with risk.

Mani Sundaram
EVP & GM Security Technology Group

Seven key research findings

- Public-facing apps remain critically under-segmented
- Microsegmentation cuts ransomware containment time significantly
- Insider threats now rank among top-three microsegmentation drivers
- Cost, control, and compliance gains are driving faster adoption
- Visibility is gaining ground as a core motivator
- Insurers are rewarding segmentation maturity with lower premiums
- Microsegmentation measurably improves regulatory compliance

Section 1.

The expanding attack surface: Why legacy segmentation is no longer enough

As enterprise infrastructure expands across hybrid, cloud, and SaaS environments, conventional segmentation is struggling to keep up. The network perimeter is no longer a fixed boundary. It is fluid, porous, and constantly shifting. Every connected workload, API, or unmanaged device increases the risk of lateral movement when breaches occur.

While more than 90% of organizations report using some form of segmentation, the reality is often superficial. In most cases, segmentation simply separates high-level zones or asset groups. This may satisfy minimum compliance standards, but it often falls short of what regulators and insurers now expect from mature cyber defenses.

Microsegmentation is emerging as a foundational control for containing this risk. It applies granular security policies to individual workloads, applications, and user contexts.

This level of control is essential to achieve Zero Trust, an approach which assumes compromise and requires continuous verification at every interaction.

Meanwhile, attackers are evolving faster than defenses. Modern breaches often begin with stolen credentials or phishing, then escalate through privilege abuse and multistage lateral movement. Public-facing applications and IoT assets are particularly exposed. Our research reveals 79% of organizations have experienced or detected at least one ransomware attack in the last 24 months — underlining the pervasiveness of this threat.

The latest Verizon 2025 Data Breach Investigations Report supports these findings. Lateral movement now features in a significant number of high-impact breaches. Once bad actors gain access to complex environments, they are often free to quietly escalate privileges, locate high-value assets, and launch ransomware or data exfiltration campaigns without detection.

This dynamic environment is forcing security leaders to reassess legacy network controls. Microsegmentation gives defenders the ability to isolate workloads, restrict east–west traffic, and respond to threats in an agile manner. The good news is microsegmentation provides this capability without requiring a full network redesign.

What does market-leading microsegmentation offer?

- Granular policy enforcement
- Lateral movement prevention
- Workload-level visibility
- Cloud native flexibility
- Compliance-ready architecture
- Significantly improved operational resilience

Layered does not mean secure

Most enterprise security environments are fragmented. As this chart shows, nearly all organizations use firewalls (97%) and VPNs (93%), and more than 70% have adopted cloud security platforms such as CNAPP. But these tools often function in isolation. Siloed controls and overlapping policies create blind spots, making it easier for attackers to move laterally and harder for defenders to respond with precision. Microsegmentation enables a more robust defense posture.

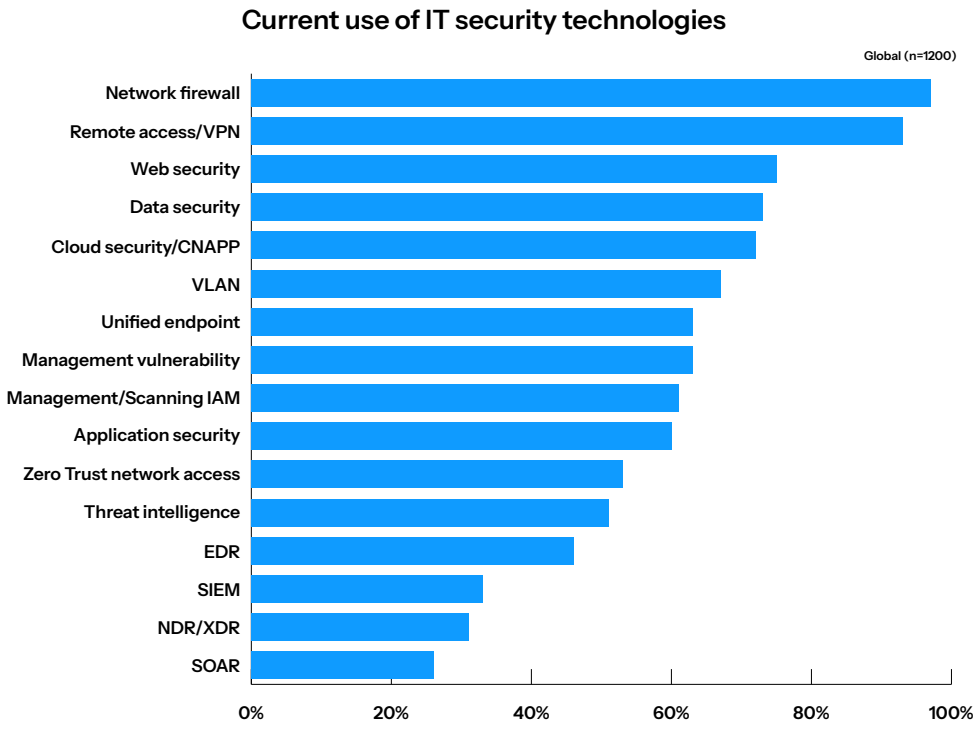

Fig. 1: In today's threat landscape, breaches are inevitable, but uncontrolled movement inside the network isn't. Microsegmentation turns inevitable breaches into containable events.

Section 2.

The gap between adoption and maturity

As revealed earlier in this report, network segmentation may be ubiquitous, but only about one-third of organizations (35%) have progressed beyond superficial measures to achieve microsegmentation.

The execution gap

- 90% of enterprises report some form of segmentation
- Only 35% have implemented microsegmentation
- Microsegmentation reduces ransomware containment time up to 33%

Most regions mirror global adoption rates, with Asia-Pacific (APAC)/Japan (38%) and Europe, the Middle East, and Africa (EMEA) (36%) outpacing global averages. North America (34%) and Latin America (31%) lag incrementally. China is the true outlier, leading with around half of all national enterprises adopting microsegmentation.

Several factors help explain geographic disparities:

- Regulatory pressure is more acute in markets such as China, where national cybersecurity laws require extensive visibility into network traffic and data flows.
- Many APAC enterprises are cloud native from the outset, making it easier to implement workload-level controls.
- EMEA organizations often rely on more complex, compliance-driven security models that slow the path to microsegmentation maturity.
- LATAM companies may be hampered by lower security budgets, slower cloud migrations, and limited internal talent, reducing their impetus to adopt microsegmentation approaches.
- North American enterprises typically have large security budgets and teams but often have complex legacy environments and high regulatory burdens, hindering progress towards microsegmentation adoption.

Organizational scale is another predictor. Enterprises with more than 5,000 employees and more than US$1 billion in annual revenue account for the majority of current microsegmentation adopters. These companies are more likely to have the operational capacity, dedicated resources, and strategic buy-in required to push segmentation deeper into the environment.

Security operating models also matter. The presence of a dedicated Security Operations Center (SOC) is consistently associated with higher segmentation maturity. For example, 46% of organizations with a SOC apply microsegmentation to applications, compared to 31% who do not. These organizations typically have the visibility, automation, and governance frameworks needed to execute fine-grained policy enforcement at scale.

Sector trends follow a similar pattern, with financial services (44%), public sector (43%), and energy and utilities (38%) leading microsegmentation adoption. Their regulatory need for strict access control, operational continuity, and ransomware containment has driven faster progress than other industries.

Among non-adopters of microsegmentation, momentum is building. Half of organizations plan to implement microsegmentation within the next 24 months. The transition from broad to fine-grained control is no longer a question of if, but when.

The segmentation gap in numbers

Many organizations have embraced segmentation, but maturity remains limited. Akamai data shows that 92% apply basic network segmentation, yet only 35% have implemented microsegmentation — the level of control needed to stop lateral movement. Despite growing awareness, most security strategies still rely on coarse-grained controls that can't keep up with today's hybrid, fast-moving environments.

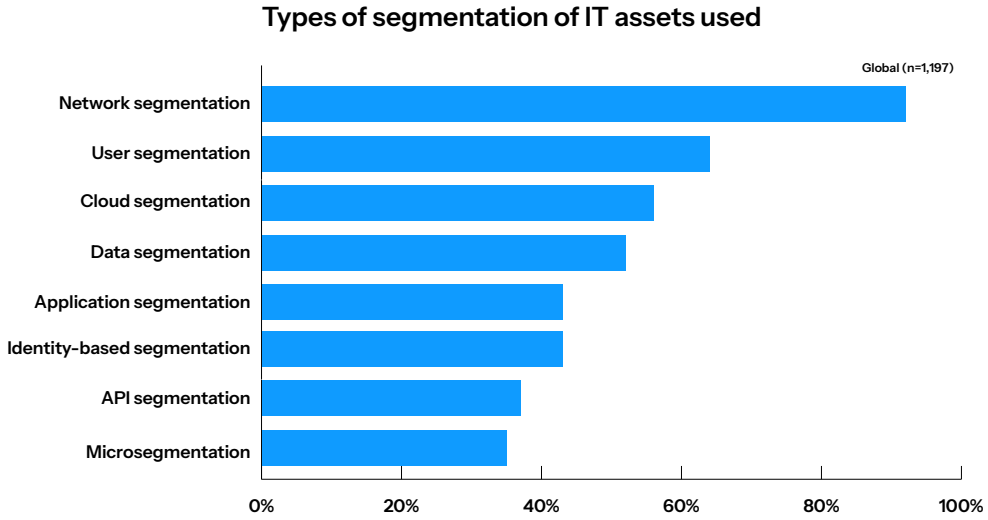

Fig. 2: While most organizations have started their segmentation journey, few have achieved sufficient depth to meaningfully reduce risk.

Global microsegmentation adoption rate league table:

1. APJ	**38%**	3. North America	**34%**
2. EMEA	**36%**	4. LATAM	**31%**
Global average	**35%**		

Section 3.

Internal adoption barriers: Complexity, cost, and cultural resistance

While awareness of microsegmentation is rising, many organizations remain stalled in the early stages of adoption. The journey from intent to execution is slowed not by lack of conviction, but by a host of internal barriers.

Network complexity stands out as the single greatest inhibitor. As enterprises modernize their infrastructure, they inherit a more fragmented landscape. Legacy systems are layered alongside public cloud workloads, SaaS platforms, and edge applications. Each layer introduces unique connectivity patterns, toolsets, and governance requirements. As a result, even experienced security teams struggle to design, deploy, and maintain consistent segmentation policies.

In highly distributed environments, identifying what to segment and how to define the right policy boundaries becomes a major challenge. Visibility gaps compound this issue. Without a clear understanding of interdependencies between workloads, missteps can cause unexpected issues. As a result, most organizations are understandably risk averse.

Main barriers to microsegmentation adoption

- **Network complexity** is the most cited challenge, with 44% of respondents naming it a top-three barrier.
- **Visibility gaps** slow policy design, with only 39% claiming strong visibility across segmented assets.
- **Operational resistance** persists, with at least 32% citing concerns about performance or business disruption.
- **Cultural inertia** emerges when ownership is unclear and segmentation lacks direct accountability.
- **Limited expertise** is particularly evident in LATAM, where 36% rank it as a particular challenge.
- **Regional disparities** reflect uneven maturity, with APAC leading in adoption and LATAM and EMEA trailing.
- **Fragmented systems** make enforcement difficult across legacy, cloud, and SaaS layers.
- **Fear of disruption** continues to deter deeper segmentation, especially where uptime is critical.
- **Partial implementation** remains common, with just 44% of organizations segmenting public-facing apps.

Operational resistance is another recurring theme. Segmentation is often viewed as intrusive or burdensome by teams outside of security. Business units worry about degraded performance or application downtime. Network and infrastructure teams may be reluctant to relinquish control or invest time in policy maintenance. These concerns create a cultural drag on progress, where implementation slows not because of technical issues, but due to organizational inertia.

In many cases, segmentation remains a project with no clear home. Security wants it. Infrastructure supports it. Compliance requires it. But no single function feels fully accountable for delivering it. This misalignment delays decision-making, limits resourcing, and undermines long-term governance.

Internal expertise also plays a critical role. Organizations with mature security operations, often those with dedicated Security Operations Centers (SOCs), tend to report higher segmentation maturity. In contrast, enterprises without sufficient in-house cloud security or workload protection expertise face steeper learning curves. This challenge is particularly evident in regions where demand for these skills outpaces supply.

For example, in Latin America, more respondents cited limited internal expertise as a top-three barrier compared to global averages. This should not be interpreted as a shortcoming.

Instead, it reflects different regional trajectories in cloud migration and cybersecurity investment, which naturally influence the pace of segmentation maturity.

These barriers have tangible consequences. Many organizations attempt segmentation but fail to fully operationalize it. Policies are inconsistently applied. Coverage gaps persist. Some systems remain entirely unsegmented due to risk aversion or architectural incompatibility.

As a result, the illusion of segmentation maturity may mask critical vulnerabilities.

Simply put: Platform-based, cloud native segmentation models are gaining traction because they abstract much of the underlying complexity, simplify policy authoring, and reduce the risk of disruption. By embedding controls directly into the workload layer, they enable continuous enforcement without relying on brittle perimeter boundaries or legacy configurations.

Section 4.

Visibility: The rising driver behind microsegmentation adoption

As enterprise infrastructure becomes more complex, visibility is no longer a byproduct of segmentation; it becomes a primary driver. In today's fragmented environments, many security teams lack a comprehensive view of how workloads, applications, and systems communicate. **Without this visibility, it becomes almost impossible to design or enforce meaningful segmentation policies.**

Blind spots persist between legacy infrastructure, cloud workloads, and SaaS environments. Attackers routinely exploit these gaps to move laterally within networks. The demand for greater visibility is evident in our research data. Visibility is now ranked among the top three drivers of segmentation adoption by a growing share of enterprises. It reflects a deeper recognition that security controls are only as effective as the understanding behind them. Segmentation built on assumption or incomplete data risks creating a false sense of security.

Microsegmentation addresses this issue directly. Leading solutions provide workload-level observability, enabling organizations to map dependencies, monitor traffic patterns, and surface communication paths that would otherwise remain hidden. These insights help teams identify unnecessary connections, tighten access controls, and reduce lateral movement risk without disrupting business operations.

Crucially, this level of visibility is not just a benefit of microsegmentation — it is a prerequisite. Granular policy enforcement depends on knowing what exists in the environment and how it behaves. Without visibility, policies can be too broad, misaligned, or difficult to maintain. Inconsistent enforcement and unmanaged exceptions undermine the entire segmentation strategy.

Visibility is a prerequisite for control

- 85% of security leaders say visibility gaps undermine segmentation effectiveness.
- Microsegmentation delivers real-time observability at the workload level.
- Visibility not only drives control but also increases confidence in Zero Trust enforcement.
- Platforms that unify segmentation and observability accelerate maturity and reduce risk.

This is why leading enterprises now see observability and segmentation as tightly coupled disciplines. Solutions that provide both capabilities in a single platform reduce complexity and accelerate adoption. By delivering real-time, contextual insights alongside policy controls, they help organizations move from static rules to adaptive, intelligence-led security.

Industry guidance reinforces this direction. The National Institute of Standards and Technology (NIST) emphasizes the importance of deep visibility in Zero Trust models. If trust must be continuously verified, organizations need to see everything. That includes not just north–south traffic at the perimeter, but also east–west traffic within the environment where threats can propagate unnoticed.

Cutting-edge microsegmentation solutions reflect this shift. They enable continuous visibility across on-premise and cloud-based assets, aligning segmentation efforts with broader observability goals. This helps enterprises detect issues early, refine controls faster, and respond more effectively when threats emerge.

Why visibility is gaining strategic weight

Visibility may rank tenth in the top reasons to adopt segmentation, but it underpins virtually every other driver on the list. The survey shows 51% of organizations cite visibility as a reason for adopting segmentation. While it trails behind more urgent concerns like ransomware containment or incident response, it's the hidden engine behind them. Without deep visibility, it's impossible to isolate critical assets, detect lateral movement, or enforce consistent policy. In that sense, it is a prerequisite for the rest.

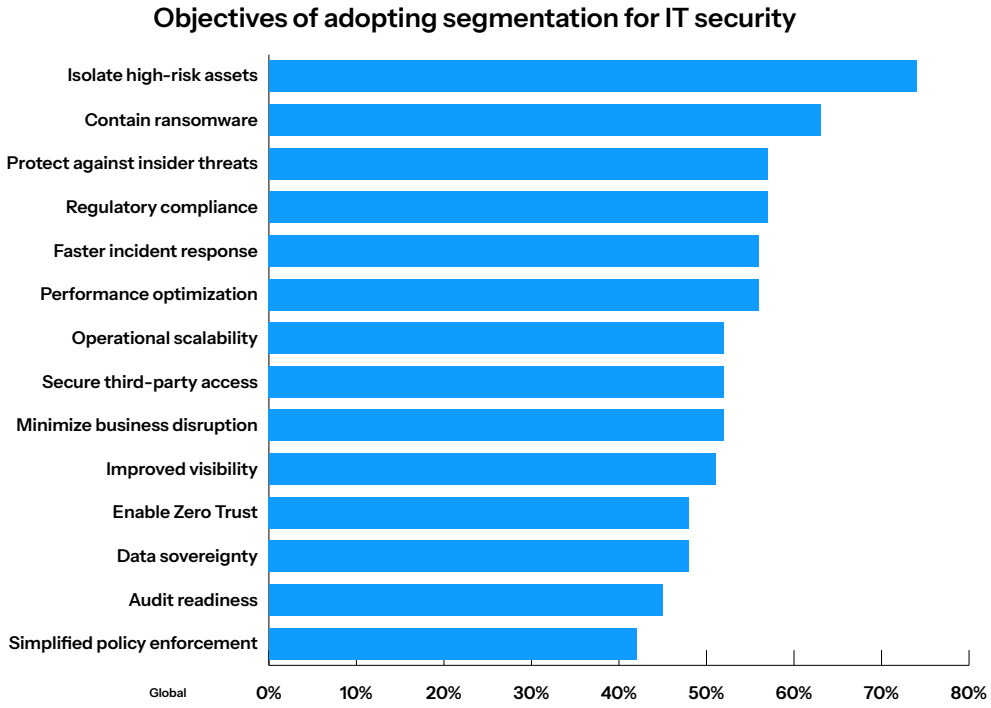

Fig. 3: Organizations across all four of the surveyed regions all identified isolating high-risk assets as their top barrier.

Section 5.

The operational payoff: Containment, resilience, and financial benefit

The value of microsegmentation is most evident during a breach. In these high-stakes moments, the ability to contain an attack quickly separates minor incidents from major crises. Organizations with effective segmentation are better equipped to isolate threats, protect critical systems, and sustain operations. This reduces both financial and reputational damage.

Our research reveals that enterprises using microsegmentation contain ransomware attacks 21.4% faster, on average. For large organizations with more than US$1 billion in revenue, that figure rises to 32.6%. In high-pressure incidents, this acceleration can be the difference between minor disruption and a full-blown crisis.

Mature adopters of microsegmentation also report higher levels of satisfaction with their containment response. They are able to limit the spread of malware or unauthorized access within the environment, effectively shrinking the blast radius and reducing the need for wide-scale remediation.

For business leaders, these outcomes have clear financial and operational implications. Faster containment means fewer systems impacted, less downtime, and lower recovery costs. This agility also strengthens business continuity during incidents, allowing critical operations to continue even as security teams work to resolve the threat. Microsegmentation advances long-term security maturity by improving visibility, simplifying compliance, and enabling Zero Trust controls.

Organizations that embed granular controls at the workload level are better positioned to meet internal and external assurance demands, from compliance audits to cyber insurance assessments. This has a growing financial impact.

As noted in Section 1, insurers are now factoring segmentation maturity into premium pricing and claims processing, rewarding those with stronger containment capabilities. While the benefits are clear, implementation can still present challenges, especially for organizations that lack in-house segmentation expertise. This is where managed services play a growing role.

The containment advantage:

Microsegmentation dramatically improves breach response. According to our 2025 global survey of 1,200 security leaders:

- Organizations using microsegmentation contain ransomware 21.4% faster.
- Enterprises with revenues of US$1 billion-plus achieve containment 32.6% faster.
- Users are also twice as likely to rate their containment performance as “effective” or “very effective.”
- Such organizations have fewer systems compromised, lower recovery costs, and stronger business continuity.

Our research shows that pairing microsegmentation platforms with managed threat hunting or segmentation-as-a-service offerings helps accelerate maturity, particularly among mid-sized enterprises. These partnerships reduce the complexity of deployment, offer guided policy design, and help operationalize segmentation faster. They also extend visibility and protection to organizations that may already have a security operations center (SOC) but lack the segmentation depth needed to isolate threats effectively.

This partnership approach is especially valuable in environments where IT and security teams are stretched. By offloading some of the design and enforcement burden, managed services free up internal resources and reduce operational friction, making segmentation more scalable and sustainable over time.

Microsegmentation significantly improves lateral control, according to security leaders.

Organizations that have implemented microsegmentation are significantly more confident in their ability to limit lateral movement during an attack. The survey shows a 10-point satisfaction gain among enterprises using microsegmentation. This uplift reinforces its value, not just as a policy control but as a critical lever for attack containment and operational resilience.

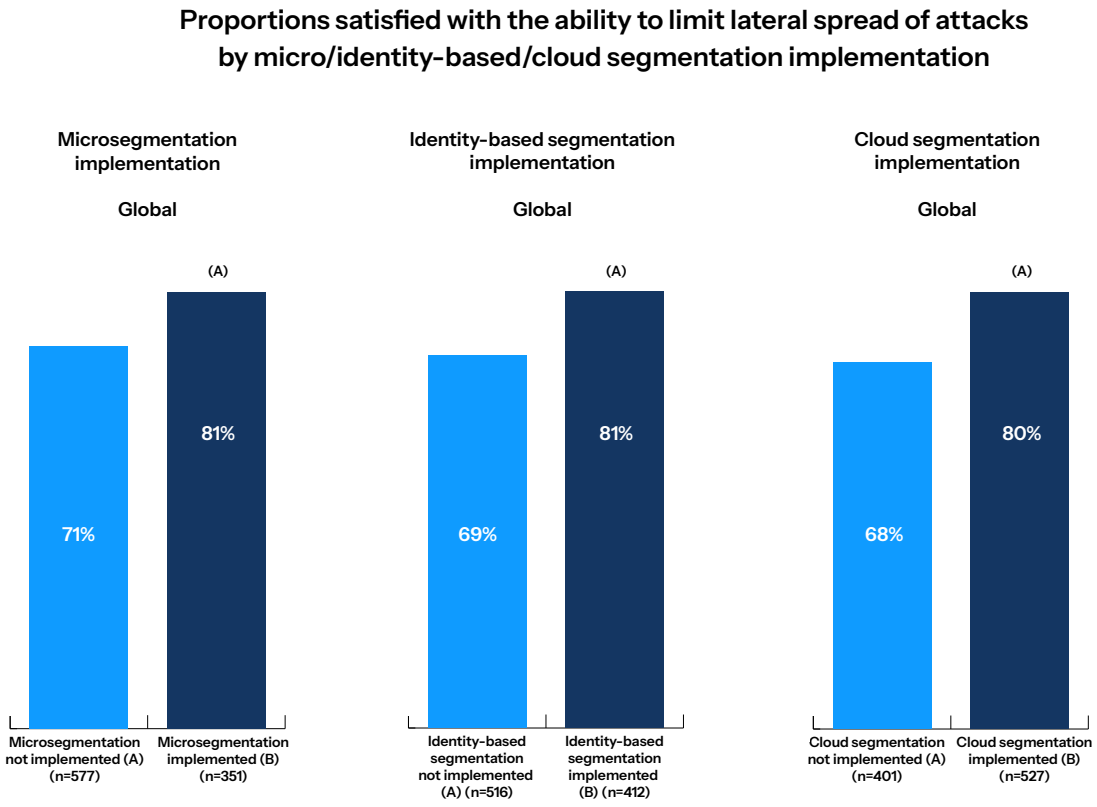

Fig. 4: Organizations that deploy microsegmentation effectively respond faster, recover sooner, and face lower downstream costs when attacks occur.

Section 6.

Managing financial risk: Segmentation as a compliance and cost advantage

Microsegmentation is no longer viewed solely as a breach prevention tool. It is now considered a lever for managing enterprise-wide financial risk. Regulators, insurers, and auditors increasingly treat segmentation maturity as a proxy for security posture, changing how organizations are assessed and insured.

According to our respondents, 75% of organizations report that insurers now assess segmentation as part of their underwriting process. For nearly one-third (30%), segmentation is already a formal requirement to obtain or renew cyber insurance. These shifts reflect growing recognition that segmentation maturity directly correlates with lower risk exposure.

This evolution has real cost implications. Sixty percent of surveyed organizations say they have received premium reductions as a direct result of improved segmentation posture. Stronger microsegmentation also improves the likelihood of claim approval. Nearly three-quarters (74%) of respondents believe it strengthens their position when filing claims. This positions microsegmentation as a strategic risk buffer reducing potential financial exposure.

Segmentation's financial edge: What the data shows

Based on responses from 1,200 global security and technology leaders:

75% say insurers now assess segmentation posture during underwriting

30% report segmentation is a formal insurance requirement

60% have received premium reductions tied to segmentation maturity

74% believe stronger segmentation **improves claim approval** likelihood

85% say segmentation simplifies audit reporting

33% report lower attestation and assurance costs as a result

LATAM organizations lead in self-reported compliance improvements

Auditors are also taking note. Eighty-five percent of organizations say segmentation simplifies audit processes, particularly when demonstrating workload-level access controls and continuous enforcement. One-third report that this has translated into lower attestation and assurance costs. These efficiencies are especially valuable for enterprises operating across multiple jurisdictions or under strict regulatory mandates.

While segmentation maturity is gaining traction globally, regional trends suggest different drivers. Organizations in LATAM lead on self-reported compliance improvements, reflecting a broader regulatory push and growing investment in modern security controls. This signals an important shift: segmentation is becoming an enabler of not only resilience but also regulatory alignment and financial agility.

For executive teams, these developments elevate segmentation to a board-level priority. As insurers tighten underwriting standards and regulators demand deeper assurance, segmentation maturity directly influences enterprise risk ratings. It affects how incidents are judged, how claims are paid, and how audit findings are resolved.

Simply put: The impact of microsegmentation extends beyond cutting-edge threat containment. It actively reduces insurance premiums, streamlines audits, and strengthens enterprise risk posture.

Section 7.

The market inflection point: Why timing matters now

Microsegmentation is no longer an emerging concept. It is a fast-accelerating security imperative. As cyberthreats grow more complex and regulators demand deeper controls, organizations across sectors are intensifying their focus on segmentation maturity. The data suggests we are now at a critical inflection point.

According to the global survey, **50% of current non-adopters plan to implement microsegmentation within the next 24 months**. This indicates a decisive shift: what was once considered optional is rapidly becoming essential. Segmentation is moving from pilot projects and proof-of-concept trials into broader strategic deployment. The momentum isn't limited to new adopters. Among organizations that already use microsegmentation, **two-thirds expect to increase their investment**, deepening coverage and expanding policy enforcement across more assets. This budgetary trend points to a broader organizational realignment. Security teams are no longer treating segmentation as a tactical fix but as a structural control central to Zero Trust and enterprise resilience. This timing matters. Early adopters are already locking in measurable advantages — faster breach containment, lower insurance costs, improved audit readiness, and stronger compliance posture. They are also reducing operational risk and accelerating response times when attacks occur. These benefits compound over time, setting a high bar for late adopters to match.

Three major cyberattacks microsegmentation could have mitigated:

1. **Capital One breach (2019)**

   Cloud misconfiguration exploited: Microsegmentation would have blocked lateral access from the compromised server to sensitive customer data stored in the cloud.

2. **Colonial Pipeline ransomware attack (2021)**

   VPN credentials compromised: Microsegmentation would have contained movement between business systems and critical infrastructure, limiting ransomware spread.

3. **United Natural Foods (2025)**

   Unauthorized internal network access: Segmentation at the workload level could have isolated business-critical systems and restricted attacker reach.

In contrast, delayed adopters face growing disadvantages. As insurers and regulators elevate expectations around containment and visibility, organizations without workload-level controls could be seen as higher risk. This could mean **higher premiums, slower claims processing, and more intensive audits**, with reputational and financial consequences.

The opportunity cost is also growing. As segmentation becomes a lever for financial optimization and operational resilience, those that delay adoption may struggle to catch up — especially in sectors where downtime or data exposure can inflict heavy losses.

Boardroom attention is rising, too. As we have seen, segmentation posture is increasingly influencing insurance underwriting, regulatory assessments, and audit scoring. Security leaders are under pressure to demonstrate progress toward segmentation maturity, not just intent.

Ultimately, the segmentation curve is steepening. Organizations that move early gain a strategic lead — operationally, financially, and competitively. Those that wait may find themselves reacting to threats and compliance demands rather than shaping their own risk trajectory.

Segmentation investment outlook for the next 24 months

Investment momentum is building fast. 68% of enterprises globally plan to boost their microsegmentation budgets, rising to 74% in both EMEA and LATAM. With non-adopters also planning uptake within two years, the adoption curve is steepening fast.

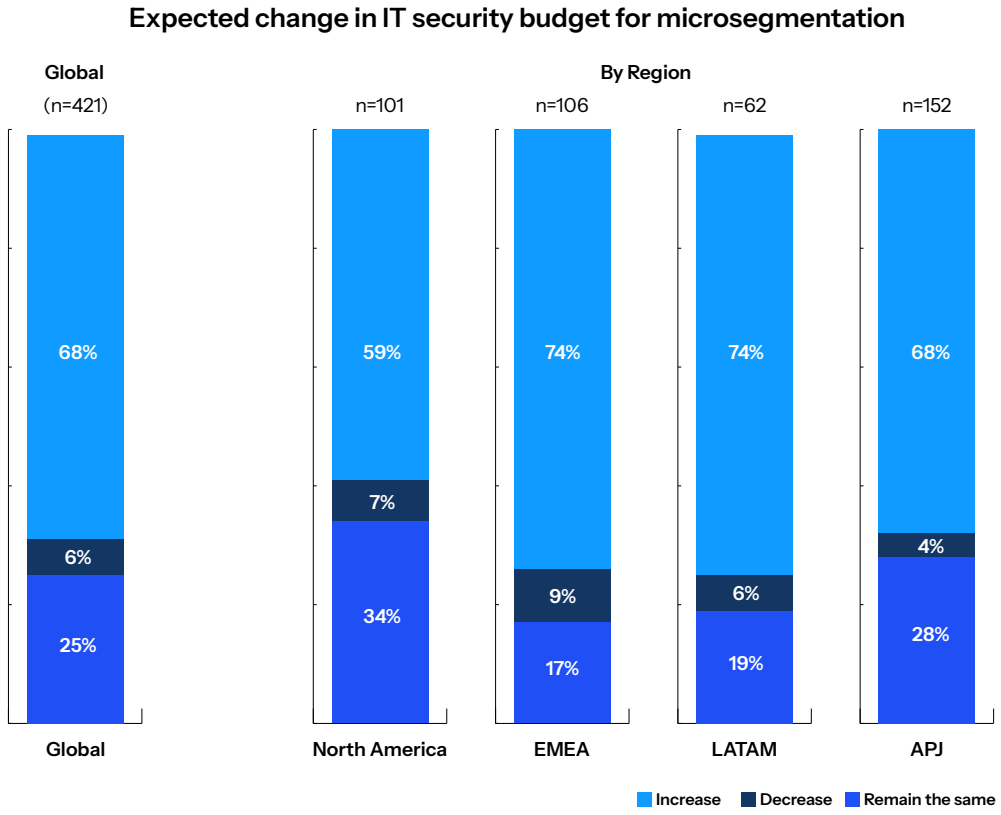

Fig. 5: Microsegmentation adoption is entering a phase of rapid acceleration. Early movers are cutting costs, streamlining audits, and leading on resilience.

Conclusion

The microsegmentation imperative for 2025 and beyond

The evidence is clear. As threats grow more advanced, lateral movement more damaging, and oversight more demanding, microsegmentation has become a foundational control for enterprise resilience. Microsegmentation delivers what legacy segmentation cannot. It provides workload-level visibility, enforces policy where it counts, and contains threats before they escalate. It reduces blast radius, supports business continuity, and simplifies compliance under pressure.

As we look to 2026 and beyond, there are several key drivers when it comes to segmentation that we recommend our global audience keep top of mind. For the APAC region, the regulatory-driven and cloud native advantage environment should prioritize segmentation. In the EMEA, we anticipate the increasingly complex compliance landscape might remain a barrier for more universal adoption of microsegmentation solutions. When it comes to the expansion of microsegmentation in LATAM, organizations will likely feel more pressure from compliance along with skill shortages.

Enterprise risk is being redefined. Insurers, auditors, regulators, and boards now treat microsegmentation maturity as a key marker of cyber readiness. Organizations without it face growing financial and reputational exposure.

Four steps toward market-leading microsegmentation

Achieve deep, continuous visibility:
Start by mapping workloads, applications, and traffic patterns in real time to surface dependencies and risks.

Design policies at the workload level:
Apply fine-grained controls that limit lateral movement and enforce Zero Trust principles across hybrid and cloud environments.

Simplify deployment with scalable architecture:
Adopt solutions that embed segmentation into existing infrastructure, minimizing disruption and operational complexity.

Strengthen governance and automation:
Align segmentation with security operations and compliance goals, using automation to sustain enforcement and accelerate maturity.

The time is now to deepen Zero Trust with microsegmentation. A technology that was previously viewed as an optional add-on has become a vital investment for any security plan. It helps prevent significant financial losses resulting from increasingly sophisticated cyberattacks, including ransomware attacks that leverage AI to find and exploit vulnerabilities.

As networks grow more complex and interconnected, microsegmentation provides precise, policy-based controls that contain threats and protect critical assets. By adopting microsegmentation technology now, security teams can build their expertise and extend protection across the enterprise before attackers can move laterally.

Why Akamai?

Akamai's microsegmentation solutions implement Zero Trust principles at the workload level for data center and cloud environments, with granular security policies governing every connection among applications, services, and users. From policy design to deployment, Akamai is the simplest, fastest way to deploy and manage precise segmentation policies that provide unparalleled visibility while preventing malicious lateral movement in your network.

Research methodology

This report is informed by proprietary research conducted by Phronesis Partners for Akamai in 2025. It captures insights from 1,200 security and technology leaders worldwide, offering a rare window into how organizations are approaching segmentation and evolving toward microsegmentation maturity. The sample spans industries, regions, and organizational sizes, providing a high-resolution view of current practices, challenges, and emerging priorities.

To learn more about how to eliminate risk in your network with industry-leading segmentation, visit Akamai.com/guardicore

Credits

Editorial and writing

Jacob Abrams
Kimberly Gomez
Clint Huffaker
Shivangi Sahu

Review and subject matter contribution

Igor Livshitz
Craig Sirois

Promotional materials

Barney Beal

Marketing and publishing

Georgina Morales Hampe

State of the Internet/Security

Read back issues and watch for upcoming releases of Akamai's acclaimed State of the Internet/Security reports. akamai.com/soti

Akamai threat research

Stay updated with the latest threat intelligence analyses, security reports, and cybersecurity research. akamai.com/security-research

Akamai security research

Read the Akamai security research blog for a rapid response perspective on today's most important research. akamai.com/blog/security-research