WHITE PAPER

The Imperative of Microsegmentation

A Strategic Shift toward Granular Network Security for the Modern Enterprise

Executive Summary

As hybrid IT environments become the norm, with enterprises operating across on-prem data centers, private clouds, and multiple public cloud providers, cyberattackers are rapidly evolving. Techniques like ransomware, insider threats, and lateral movement now target gaps in visibility and control across multi-cloud architectures. To address this growing risk, network microsegmentation has emerged as a critical solution for enforcing zero-trust security, reducing attack surfaces, and containing breaches before they spread.

Microsegmentation enables fine-grained, workload-level segmentation by applying precise security policies to virtual machines, containers, and cloud infrastructure. It provides real-time visibility, enforces least-privilege access, and helps stop lateral movement at the source. Increasingly, global regulators also recognize microsegmentation as a foundational control for securing sensitive data and critical infrastructure.

By adopting microsegmentation within a centralized, policy-driven architecture, organizations can strengthen zero-trust initiatives, meet compliance mandates, and improve cybersecurity resilience across hybrid and multi-cloud environments.

As part of their zero-trust strategic and architecture initiatives, security and risk management leaders have started seeking microsegmentation technologies in order to:

- Achieve fine-grained zoning
- Enable policies at the workload level
- Gain visibility of east-west network traffic and manage workload policies at scale

— Gartner, *Market Guide for Network Security Micro-segmentation*[1]

The Shifting Cybersecurity Landscape

Today's threat landscape is defined by the rapid expansion of hybrid IT. Enterprises now operate across a mix of environments—on-premises, private cloud, and multi-cloud—creating complex networks and vast attack surfaces. Traditional perimeter defenses are no longer enough. As east-west traffic grows and attackers become more sophisticated, modern security demands granular, application-aware segmentation.

Key trends driving adoption of microsegmentation technologies include:

- **Lateral movement and ransomware:** Once inside the network, attackers exploit flat architectures to move laterally, escalate privileges, and access critical systems. In 2024, it took an average of 258 days to detect and contain a data breach, with an average cost of $4.88 million per incident.[2] This extended exposure underscores the need for deeper segmentation and faster containment.
- **Zero-trust security models:** Microsegmentation is essential to zero trust, which assumes no implicit trust—inside or outside the network perimeter. Adoption is rising sharply: The number of organizations using multiple microsegmentation strategies is projected to increase from <5% in 2023 to 25% by 2027 (Gartner), driven by the need to isolate workloads and prevent lateral movement.[3]
- **Hybrid IT and east-west traffic:** With 78% of organizations using more than one cloud provider,[4] internal workload-to-workload communication is more difficult to monitor—and more vulnerable. East-west traffic often bypasses traditional security controls, making granular policy enforcement at the workload level essential.
- **Regulatory and compliance pressures:** Microsegmentation is becoming a baseline requirement for compliance. Global standards like NIS2 (EU), NIST/CISA (US), and PCI DSS now emphasize network zoning and segmentation as architectural imperatives—not optional safeguards. According to an IDC report, "...enterprises can no longer afford to treat data privacy and cybersecurity regulations as legal afterthoughts. These mandates are now architectural imperatives."[4]

As enterprise networks become more dynamic, microsegmentation provides the control, visibility, and policy enforcement needed to adapt. It enables organizations to secure every workload, container, and user interaction—regardless of where they operate.

From Big Zones to Smart Zones: Rethinking Segmentation

Historically, network segmentation has relied on macrosegmentation, dividing the network into large, broad zones (such as Demilitarized Zone, internal network, operational technology network) using traditional tools like VLANs, firewalls, routers, and access control lists (ACLs). While effective for initial separation, macrosegmentation only offers coarse-grained control. A breach in one segment can still allow lateral movement across a wide range of assets within that segment.

Microsegmentation, in contrast, is a zero-trust network segmentation approach that places security policies between any two workloads, effectively isolating them. This fine-grained control applies security policies directly to individual application environments, containers, virtual machines (VMs), and Infrastructure-as-a-Service (IaaS) instances. This significantly reduces the attack surface and improves the containment of breaches or malware by stopping lateral movement at its source.

	Feature	Macrosegmentation	Microsegmentation
Scope and Granularity	Granularity	Coarse-grained (large zones)	Fine-grained (individual workloads and applications)
	Focus	Network zones (e.g., DMZ, internet, OT)	Application-level or workload-level control
	Example	Separating IT from OT networks	Restricting App A to only talk to Database A
Implementation	Enforcement Tools	VLANs, firewalls, routers, ACLs	Host-based agents, SDN, workload firewalls
	Control	Network infrastructure	Endpoint/workload level
	Policy Scope	Broad (e.g., allow internal→DMZ)	Specific (e.g., App A TCP 443 → DB A only)
Security and Compliance	Risk Isolation	Limits attack spread between zones	Limits lateral movement within zones
	Compliance Support	PCI, HIPAA zone isolation	Enhances auditability and granular controls
Agility and Scalability	Visibility Needed	Moderate	Deep insight into application dependencies
	Change Management	Infrequent changes, more static	Dynamic, adapts to cloud and container workloads
	Cloud/Hybrid Support	Partial	High—ideal for cloud, virtualized, containerized apps

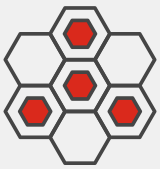
Built for Compliance. Designed for Control

Network segmentation is no longer simply a best practice. It is rapidly becoming a global regulatory norm, especially for protecting critical infrastructure and sensitive data. Here are a few examples:

- **EU – NIS2 Directive** implies segmentation as part of risk management obligations and applies to critical sectors, including energy, health, transportation, and government.
- **US – NIST/CISA/EO 14028** recommends segmentation to support zero-trust principles, facilitate IT/OT separation, and prevent lateral movement.
- **China – MLPS** enforces segmentation based on data classification levels.
- **Japan – CI Cybersecurity Guidelines** mandate network zoning across OT and IT environments.
- **Industry standards** such as PCI DSS require segmentation of cardholder data environments, while ISO/IEC 27001 recommends segregation for business and security purposes.

The global average time to identify a data breach in 2024 was 194 days, while the average time to contain a breach was 64 days—meaning the average lifecycle of a data breach is approximately 258 days, with an average remediation cost of $4.88 million per incident.

—IBM Security and the Ponemon Institute. *Cost of a Data Breach Report 2024.*[5]



Microsegmentation "isolates different parts of the network—applications, databases, or workloads—and applies security policies to control traffic between these areas. This reduces the overall impact of a breach, even if one segment is compromised." This approach specifically addresses the threat of lateral movement.

— The Forrester Wave™: *Microsegmentation Solutions, Q3 2024*[6]

Beyond compliance, microsegmentation is driven by strategic imperatives, including:

- **Fine-grained zoning:** Creating highly specific security zones down to the individual workload
- **Workload-level policy enforcement:** Applying security policies directly where applications reside
- **Real-time visibility:** Gaining deep insight into east-west traffic patterns to detect anomalies and enforce policies effectively
- **Need for least-privilege access:** Granting only the minimum access necessary for a workload or user to perform its function

The Power of Microsegmentation

Microsegmentation offers powerful capabilities for a wide range of use cases:

- **Workload-level control** applies security policies directly to individual application environments in containers, VMs, and IaaS to reduce the attack surface and contain breaches.
- **Policy recommendation engines** automate the creation of granular rules based on observed behavior, thereby simplifying setup and reducing manual effort.
- **Enforcement via identity, tags, and OS attributes** leverages identity, tags, and operating system attributes to provide precise policy control, enhancing accuracy and minimizing misconfigurations.
- **Application-mesh visibility** provides deep insight into application communication patterns to improve security policy enforcement and anomaly detection.
- **Context-based rules** enforce security based on workload attributes instead of static IP addresses, enabling more adaptive and resilient policy enforcement across dynamic environments.

A comprehensive microsegmentation solution can extend your zero-trust architecture across hybrid environments, including multi-cloud (AWS, Azure, GCP), data centers, OT networks (SCADA, PLCs), and campus/branch offices (finance, HR, IoT devices). They also often integrate with AI-powered services for centralized management, real-time analytics, and automated orchestration, providing a single pane of glass for enhanced visibility and operational efficiency.

Conclusion

The shift from traditional network segmentation to microsegmentation is not merely a technological upgrade but a fundamental change in how organizations approach cybersecurity. Driven by the escalating threat landscape, the demands of hybrid IT, and increasingly stringent regulatory requirements, microsegmentation offers unparalleled control and visibility over network traffic.

By implementing fine-grained, workload-level policies and leveraging the advanced analytics provided by microsegmentation, organizations can significantly reduce their attack surface, halt lateral movement, simplify compliance, and build a more resilient and secure digital infrastructure for the future. Gartner's prediction[7] that a quarter of enterprises will be using multiple segmentation models by 2027 underscores the critical importance of embracing this strategic security approach.

[1] Hils, Adam, Rajpreet Kaur, and Charanpal Bhogal. *Market Guide for Network Security Micro-segmentation*. Gartner, May 2025. Update to June 2023 research note.

[2] IBM Security and the Ponemon Institute. *Cost of a Data Breach Report 2024*. IBM, July/Aug. 2024.

[3] Gartner. *Market Guide for Network Security Micro-segmentation*. Hils, Adam, Rajpreet Kaur, and Charanpal Bhogal, May 2025. Update to June 2023 research note.

[4] IDC. *Regulatory Turning Point: How Data Privacy, Cybersecurity, and AI Laws Are Reshaping Enterprise Strategy in Asia/Pacific*. IDC, May 2025.

[5] IBM Security and the Ponemon Institute. *Cost of a Data Breach Report 2024*. IBM, July/Aug. 2024.

[6] Blankenship, Joseph, et al. *The Forrester Wave™: Microsegmentation Solutions, Q3 2024*. Forrester Research, 28 Aug. 2024.

[7] Gartner. *Market Guide for Network Security Micro-segmentation*. Hils, Adam, Rajpreet Kaur, and Charanpal Bhogal, May 2025. Update to June 2023 research note.

August 4, 2025 11:39 AM / MKTG-1669-0-0-EN