Kyndryl Micro-Segmentation Implementation Services

Redefining trust in a perimeterless world

Organizations are under constant pressure to innovate, modernize infrastructure, and support hybrid and cloud-first operations. But this growing digital footprint has a downside—escalating cyber threats and a rapidly expanding attack surface.

Micro-segmentation offers a foundational pillar for modern security architectures—helping security policies follow workloads wherever they go. It embodies zero trust principles by eliminating implicit trust within the network and enabling granular control over east-west traffic.

> ***"At Kyndryl, we do more than design solutions—we build more secured, trusted ecosystems where every interaction is monitored and resilient."***
>
> ***– Jimmy Nilsson, Vice President, Global Zero Trust Domain Leader, Kyndryl***

Highlights

- Reduce breach impact by limiting lateral movement within networks
- Gain full visibility into east-west traffic to uncover hidden threats and enforce granular controls
- Improve operational efficiency by automating security policies and reducing misconfiguration
- Achieve measurable cost savings through faster containment and response
- Accelerate zero trust adoption with scalable micro-segmentation across hybrid and multicloud environments

Trends accelerating micro-segmentation adoption

Trend	Insight
Cyberattack frequency	Global attacks rose 30% in 2024. Organizations must contain breaches quickly.[1]
Zero trust prioritization	More than 86% of organizations have already started their zero trust journey.[2]
Staggering data breach cost	By 2031, ransomware will cost victims $265 billion annually, attacking a business, consumer or device every 2 seconds.[3]

Why it matters now

From cloud adoption to remote work, new operational realities expose organizations to advanced persistent threats, ransomware, and insider risks. Micro-segmentation enables organizations to isolate critical workloads, reduce lateral movement, and improve response and recovery times.

Modern cybersecurity challenges demand granular control

Traditional perimeter security is no longer enough to protect complex IT environments. With remote work, cloud adoption, and rising threats like ransomware and insider attacks, organizations need deeper visibility and control. Micro-segmentation addresses these gaps by enforcing granular security at the workload level, reducing lateral movement and limiting the impact of breaches.

1 **Technological complexity**

- Connected devices: Every connected device increases the attack surface.
- Legacy systems: Many enterprises still rely on outdated technologies without modern protections.
- Cloud security: 77% of organizations name security as a top cloud challenge.[4]

2 **Operational risks**

- Remote work: 62% of organizations witnessed more incidents due to remote working employees.[5]
- Supply chain: 62% of breaches originate from third parties.[6]
- Insider threats: Roughly 60% of all data breaches involve insider threats.[7]

3 **Security gaps**

- Undetected Advanced Persistent Threats: Persistent threats can remain hidden for months.[8]
- Ransomware: Global costs projected to reach $265B by 2031.[9]
- Compliance Pressure: Fines for non-compliance can reach 4% of annual revenue.[10]

4 **Human and resource constraints**

- Phishing and Error: Human error causes 82% of breaches.[11]
- Skill Shortages: 3.4 million cybersecurity jobs unfilled globally.[12]

5 **Financial constraints**

- SME Budget Gaps: Companies under 1,000 employees spent up to 15% of their IT budget on security.[13]
- Breach Costs: Ransomware will cost victims $265 billion annually by 2031.[14]

How micro-segmentation addresses these risks

Benefit	Impact
Reduced lateral movement	Significantly limits breach impact.
Enhanced visibility	Provides full insight into east-west traffic.
Lower misconfiguration risk	Dramatically reduces configuration errors.
Operational efficiency	Decreases manual security tasks.
Cost savings	Protects revenue and reputation.

Implementation approach and use cases

What is micro-segmentation?

Micro-segmentation is a modern security approach that simplifies network segmentation using logical labels (e.g., app, user role), enabling flexible, workload-level control across hybrid environments.

Traditional segmentation limits:

- Focused only on perimeter controls
- No control over internal movement within segments
- Limited visibility of intra-segment communication

Micro-segmentation advantages:

- Dynamic, adaptive policies follow workloads
- Fine-grained visibility and control
- Minimizes risk of lateral movement
- Integrates with existing security tools and workflows

Kyndryl's proven implementation methodology

Kyndryl offers Micro-Segmentation Implementation as a stand-alone service or as part of a comprehensive zero trust journey. Our approach includes:

- **Strategy Development**
  Define goals, prioritize high-value assets, and align with zero trust strategy.
  Tip: Start with compliance-mandated workloads for quick wins.
- **Discovery & Mapping**
  Identify traffic flows, dependencies, and risks.
  Tip: Ensure visibility into east-west communication.
- **Policy Design**
  Use logical labels, keep policies simple and scalable.
  Tip: Avoid overly granular policies that impede manageability.
- **Pilot & Scale**
  Validate policies in a test group, refine, and expand.
  Tip: Use data from pilot to demonstrate ROI.
- **Automation & Integration**
  Enable dynamic policy adaptation and SIEM/ITSM integration.
  Tip: Automation reduces workload and human error.
- **Continuous Monitoring**
  Real-time analytics, forensic insights, and iterative optimization.
  Tip: Use alerts and baselines to spot anomalies and prevent policy drift.

Use Case	Benefits
Zero-day exploit defense	Contain threats and maintain operations.
Securing remote work	Protect endpoints and secure access.
M&A integration	Integrate new networks securely.
Insider threat prevention	Restrict access and detect anomalies.
Faster incident response	Isolate threats and speed recovery.

Why Kyndryl and Illumio?

With decades of experience, global reach, and industry-leading technology, Kyndryl and Illumio together deliver the expertise, tools, and strategies to secure your zero trust journey.

Expertise and Experience

- Kyndryl's deep infrastructure and security knowledge is paired with Illumio's market-leading micro-segmentation platform.
- Continuous support from planning through full adoption.
- Proven methodologies backed by rich intellectual capital.

Comprehensive, Scalable Solutions

- Seamless integration of Illumio micro-segmentation into on-prem, hybrid, or multi-cloud environments.
- Reduced implementation risk with tested, repeatable frameworks.
- Solutions tailored to compliance, operational, and business needs.

Business-Aligned Outcomes

- Strategic workshops, asset discovery, and actionable recommendations.
- SIEM/ITSM integration for alerts and workflows.
- Documented schema and full knowledge transfer for ongoing success.

Micro-segmentation partner: Illumio

Illumio is the world leader in breach containment, helping organizations around the globe protect their critical applications, workloads, and assets. Trusted by organizations of all sizes, the Illumio platform protects more than 20 of the Fortune 100 and secures more than 40 million workloads globally. For more information visit: illumio.com.

Get started with Kyndryl

Micro-segmentation is no longer optional—it's a strategic imperative for security, compliance, and operational resilience. Let Kyndryl help you take control of your security posture with a proven, scalable approach.

Book a Meeting with Kyndryl today to schedule a discovery workshop and take the next step on your zero trust journey.

> ***"Kyndryl's micro-segmentation services are designed not just to secure—but to empower your infrastructure."***
>
> ***– Jimmy Nilsson, Vice President, Global Zero Trust Domain Leader, Kyndryl***

Sources:

[1] Check Point. (2025). *The State of Cyber Security 2025.*

[2] Cisco. (2023) *Security Outcomes for Zero Trust*.

[3, 9, 14] Cybersecurity Ventures (2025). *Ransomware Will Strike Every 2 Seconds by 2031.*

[4] Flexera. (2025). *State of the Cloud Report.*

[5] Fortinet. (2023). *2023 Work-from-Anywhere Global Study Report.*

[6, 7, 11] Verizon. (2025). *Verizon 2025 Data Breach Investigations Report.*

[8] Mandiant. (2025). *M-Trends 2025 Report*.

[10] Exabeam. *The Main GDPR Requirements in Plain English.*

[12] ISC². (2023). *ISC2 Cybersecurity Workforce Study: Looking Deeper into the Workforce Gap*.

[13] Cymulate. (2025). *How Cybersecurity Leaders are Optimizing their Budgets in 2025.*