Micro-Segmentation Security Service

Stop lateral movement. Contain breaches. Protect critical systems.

Australian organisations face rising cyber threats that bypass traditional defences. Once inside, attackers move laterally to compromise sensitive systems. Our micro-segmentation service creates internal security zones that block unauthorised movement, contain breaches, and protect critical assets—without disrupting operations or requiring infrastructure overhaul.

Why Micro-Segmentation Security Service

✓ **Enhance Threat Containment**
Limit the blast radius of any breach. Prevent malware or attackers from spreading beyond the initial point of compromise.

✓ **Protect Critical Assets**
Isolate sensitive systems—finance, healthcare, industrial controls—so only authorised paths can reach them.

✓ **Simplify Compliance**
Meet regulatory requirements (PCI-DSS, Essential Eight, SOCI) with precise network segmentation and audit-ready reporting.

How it works

01 **Discover**: Automatically map internal traffic flows and identify legitimate communications using machine learning.

02 **Segment**: Create granular access policies based on identity, role, and context—enforced via built-in OS firewalls.

03 **Verify**: Trigger multi-factor authentication for sensitive lateral movements, adding identity checks deep inside the network.

Getting started with Ericom

1. Assess current network risks and segmentation gaps.
2. Deploy policy controllers and connectors—no agents required.
3. Begin with a learning phase, then enforce policies with full visibility and support.

ERICOM
SYDNEY · MELBOURNE · BRISBANE · CANBERRA

1300 360 369 | 02 8394 5500 | 03 9927 6100 engage@ericom.com.au | www.ericom.com.au

Technology features

Automated Policy Discovery Learns normal traffic patterns and recommends segmentation rules—reducing manual effort and improving accuracy.

Integrated MFA for Lateral Movement Adds identity verification when sensitive internal access is attempted—enhancing protection against unauthorised movement.

Cloud Dashboard with Traffic Maps Visualises internal communications, blocked attempts, and policy status—providing clear oversight and actionable insights.

Identity-Based Policies Segment access by user, device, application, or time—centrally managed for consistency and control.

SIEM Integration Feeds logs to Splunk, Sentinel, and other tools—enabling unified visibility and streamlined incident response.

Policy Rollback and Versioning Revert to previous segmentation policies or review changes—supporting safe experimentation and audit readiness.

CONTAINTHREATS

Our service isolates systems so ransomware and other threats can't jump between devices. Secure zones around critical assets—like backups and servers—block lateral movement and contain breaches early. This limits impact, reduces downtime, and strengthens resilience.

ABOUTUS

Ericom is an Australian-based security provider delivering advanced segmentation services tailored to local organisations. Our managed service combines cutting-edge technology with expert support—helping you achieve Zero Trust outcomes without complexity.

SIMPLIFYCOMPLIANCE

We simplify segmentation for PCI-DSS, APRA, and SOCI by automating policy creation and enforcing identity-based controls. This reduces audit scope, improves hygiene, and ensures sensitive systems are only accessed by authorised users—helping meet obligations without added complexity.

NEXTSTEPS

Request a demo or free segmentation assessment today. In just one hour, we'll show you how to lock down your network, contain threats, and protect your most critical systems. Our experts will walk you through real-world use cases and help you identify quick wins for your environment.

Network Micro Segmentation Security Service can be integrated across diverse domains, including:

- Healthcare networks
- Retail store and payment systems
- Industrial control systems
- Financial services environments
- Government and council IT
- Education and research networks
- Cloud and hybrid infrastructure
- Remote workforce segmentation
- Critical infrastructure protection

Let us show you how.

ERICOM