Micro-Segmentation 101

Adam Brady – Systems Engineer
What We’ll Cover

- What is micro-segmentation?
- Why micro-segmentation?
- The principles of micro-segmentation
- How to implement a strategy in 5 steps
What is Micro-Segmentation?
What is Micro-Segmentation?
What is Micro-Segmentation?

Stop the spread of unauthorized lateral movement.

Control & Contain
Why Does Micro-Segmentation Matter?
Vendor Portal

Vendor

Internal Servers

POS system
Without Segmentation…

Common breach methodology

Step 1: **Breach** low value workload
Step 2: **Map** paths and connections
Step 3: **Move** to high value assets

# of breaches in 2017 alone: **1,579**

Avg. dwell time: **200+ days**
Micro-Segmentation Addresses Key Concerns

- Map Application Dependencies

- Meet Compliance Requirements

- Secure Critical Applications

- Securely Move To Cloud
Why is Micro-Segmentation Growing Now?

Risk reduction, audit, and compliance
What’s Stopping Us?

~100 workloads
~200k “flows”
Environments are Complex

Distributed

Dynamic

Heterogeneous

Hybrid/Multi-Cloud
Segmentation the Old Way

- 59% have little to no visibility into traffic flows
- Up to 4 hours to create a firewall rule for new app
- 87% reported multiple outages due to configuration
- You have to re-architect your apps and network
- Static policies need to be updated manually
- Firewalls won’t work in the cloud
Different Micro-Segmentation Approaches

Segment on the Network

Using firewalls or ACLs

**Challenge:** No application visibility, doesn’t work in cloud.

Segment in the Hypervisor

Adding a firewall to hypervisors

**Challenge:** Vendor specific, no bare-metal, limited cloud support.

Segment at the Workload

Leveraging the native firewall in the OS

**Challenge:** Managing agents.
What Are the Principles of Micro-Segmentation?
What You Need for Micro-Segmentation

- Support for all environments and platforms
- Application-centric visibility
- Centralized policy creation and management
- Adaptive and automated
- Customizable granularity
How to Implement a Micro-Segmentation Strategy in 5 Steps
The 5 Steps

1. Get the right tools
2. Map your application environment
3. Decide what to segment first
4. Test and enforce policy
5. Decide what to segment next

It’s as much about process as it is about technology.
Step 1: Get the right tools

The right tools should:

- Work with multiple environments, platforms, and infrastructure.
- Allow for easy testing, validation, and updating of policies.
- Be designed with automation and scale in mind.
Step 2: Map your application environment

The map should be real time and accurate.
Step 3: Decide what to segment first

You can’t segment everything at once. Start where you get the greatest return.

Key factors for prioritization:

- Value of data
- Compliance/audit requirements
- Harm if there is an outage
- Application owner relationship

- Value as a pivot point
- Related active projects
- There’s no other way
Step 3: Decide what to segment first

Different segmentation granularity might be appropriate in different places.
Step 4: Test and enforce policy

Segmentation alters the communications of your applications.

Test policy before you enforce it.

The right solution should:
- Enable policy modeling.
- Provide visual feedback.
- Adapt policy to changes in the environment.
Step 5: Decide what to segment next

- Identify the next application priority.
- Many organizations never micro-segment everything.
- Some environments may never go into enforcement everywhere.

The right solution should:
- Support phased deployment.
- Support a mix of modeling and enforcement.
Real-World Examples

**Environmental Segmentation** – separate development and production  
- Maintain flexibility and contain exposure to high-value targets

**Application Segmentation** – segment an ordering application  
- Control activity into and out of a critical application

**Tier Segmentation** – separate web, database, and application servers  
- Reduce the ability of attackers to move freely through an application

**Process Segmentation** – protect Active Directory  
- Control communications down to the process level and automatically adjust policy
Closing Advice for Success

1. Start with visibility.
2. Test policy before enforcing.
3. Segment in phases.
4. Build partnerships between security, infrastructure, and application teams.
5. Work with an internal champion who can drive the project.
More questions?

Contact me:

adam.brady@illumio.com