Secure Your Data Center And Cloud With a Micro-Segmentation Strategy

Todd Truitt – Illumio's Director of Systems Engineering for APAC

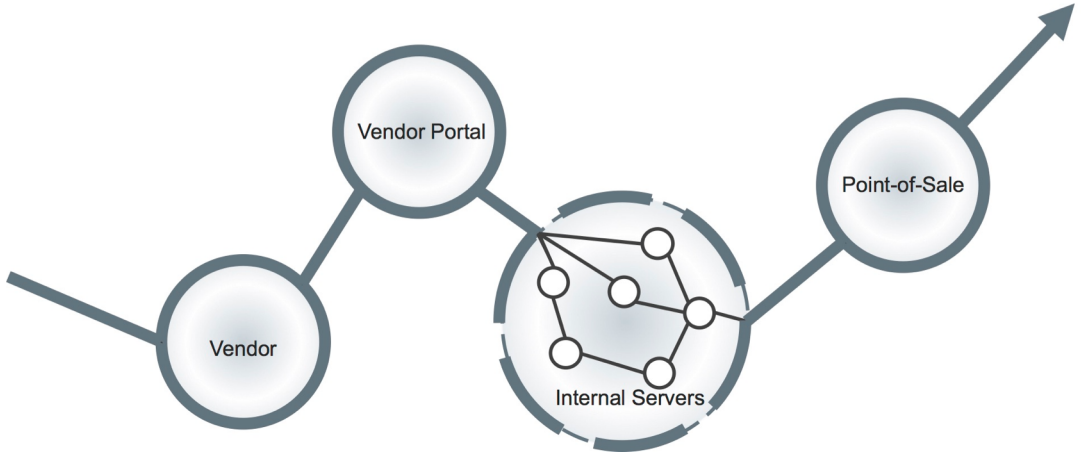
AusCERT 2018

What We Will Discuss

- Why micro-segmentation?
- Considerations when doing micro-segmentation
- How to implement a strategy in 5 steps

Why Micro-Segmentation?

Without Micro-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 2016 alone:

2,260

Avg. dwell time:

3-6

months

Singapore

NUS, NTU networks hit by 'sophisticated' cyber attacks

Australia's biggest data breach sees 1.3m records leaked

By Allie Coyne
Oct 28 2016
12:00PM

SECURITY IS POWERED BY SC MAGAZINE

11 Comments

Medical data exposed.

More than one million personal and medical records of Australian citizens donating blood to the Red Cross Blood Service have been exposed online in the country's biggest and most damaging data breach to date.

A 1.74 GB file containing 1.28 million donor records going back to 2010, published to a publicly-facing website, was

#TECHNOLOGY NEWS DECEMBER 12, 2017 / 8:28 PM / UPDATED 9 HOURS AGO

Taiwan's Far Eastern International fined T$8 million over SWIFT hacking incident

3 MIN READ

Reuters Staff

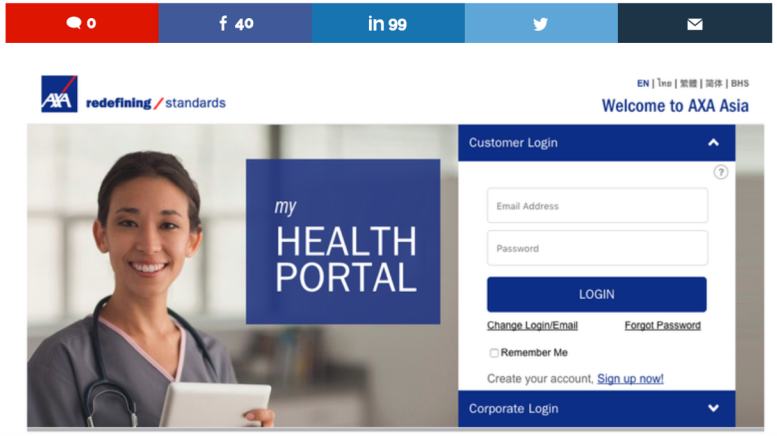
...'s financial regulator said on Tuesday it had fined
...ion ($266,524) due to deficiencies
...ident.

...ed that hackers sought to steal some
...d all but $500,000 had been recovered

AXA Insurance data breach hits customers in Singapore

Customers' e-mail address, mobile number, and date of birth are compromised in targeted the insurance company's health portal.

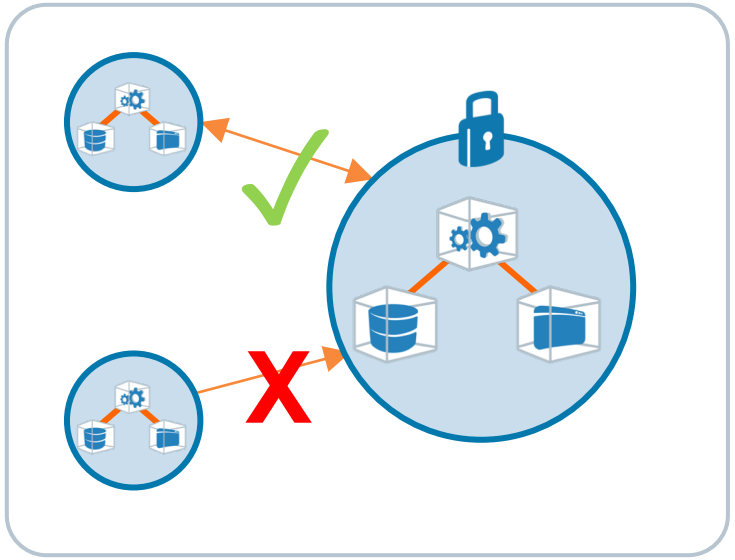
By Eileen Yu for By The Way | September 7, 2017 -- 14:15 GMT (00:15 AEST) | Topic: Security



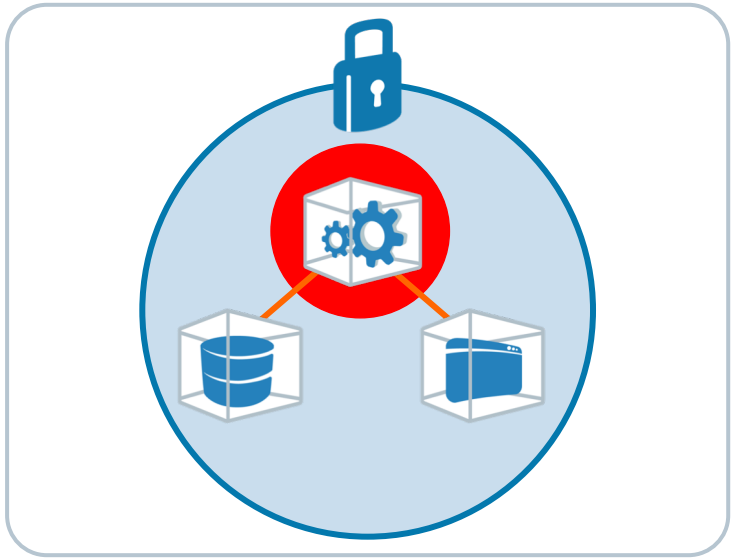
Industry Moving to Micro-Segmentation

”Segmentation adds separation and defense in depth, which is needed to contain attacks and limit the impact of a successful exploit.” – Greg Young, Research VP, Gartner

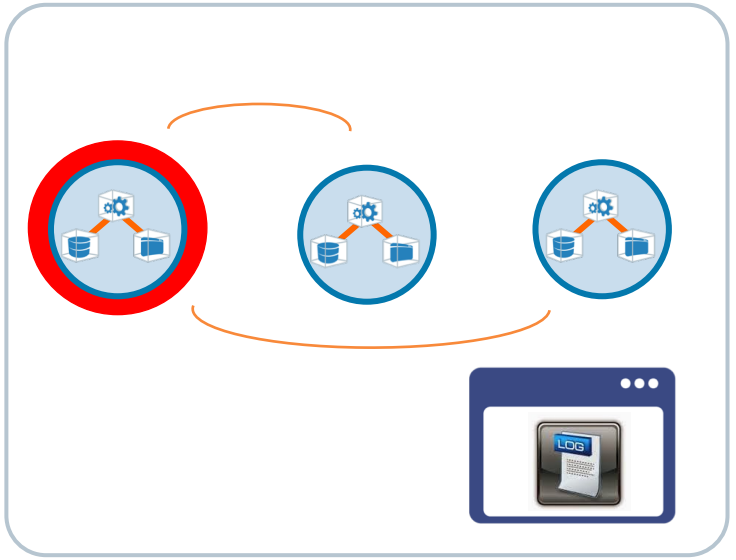
Stop the spread of unauthorised lateral movement



Control



Contain



Inform

illumio

Considerations when doing Micro-Segmentation

Segmentation the Old Way

59% have little to no visibility into traffic flows

You have to re-architect your apps and network

Up to 4 hours to create a firewall rule for new app

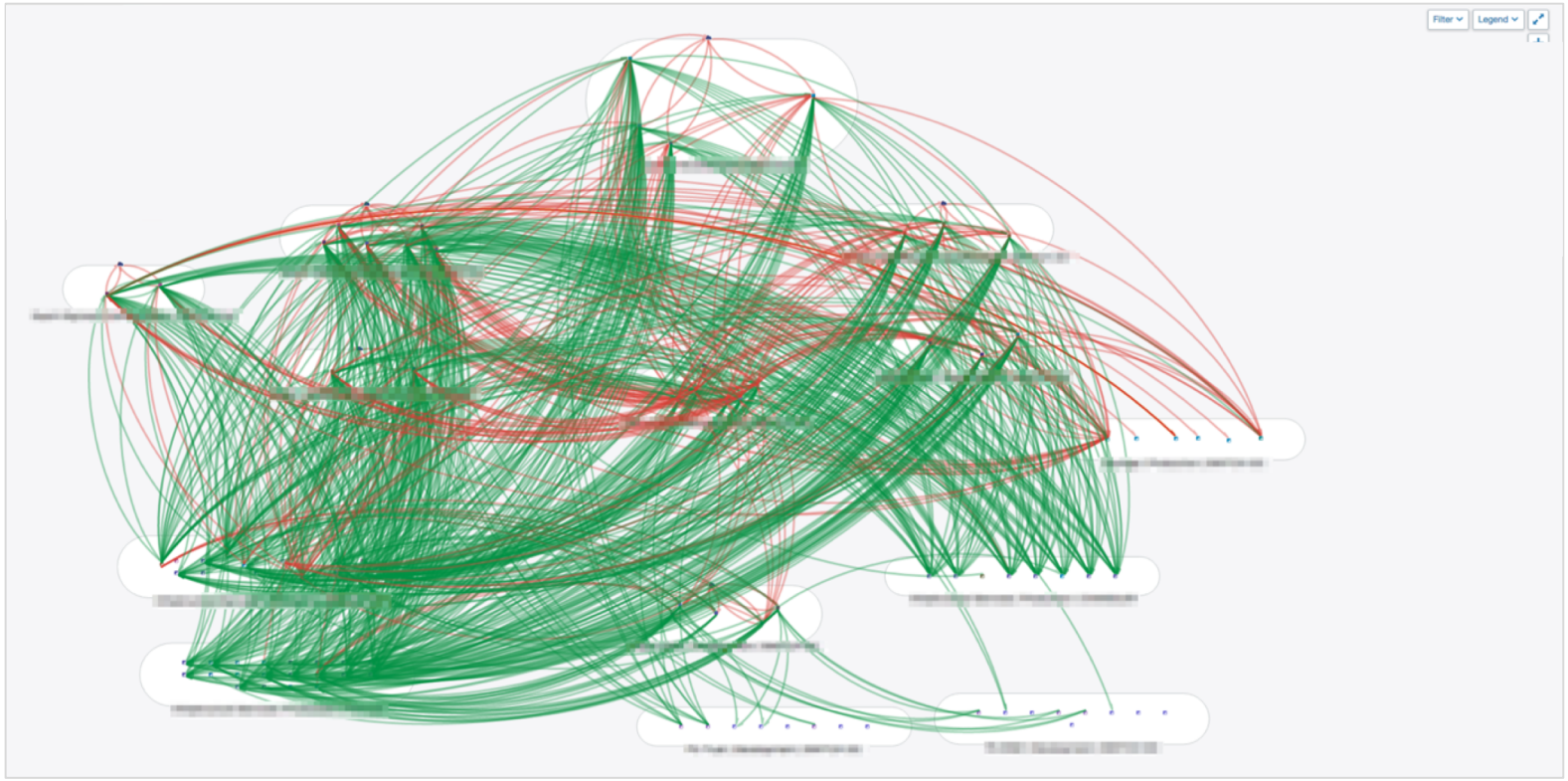
Static policies need to be updated manually

87% reported multiple outages due to configuration

Firewalls won't work in the cloud

Environments are Complex

<*100 workloads*



Dynamic

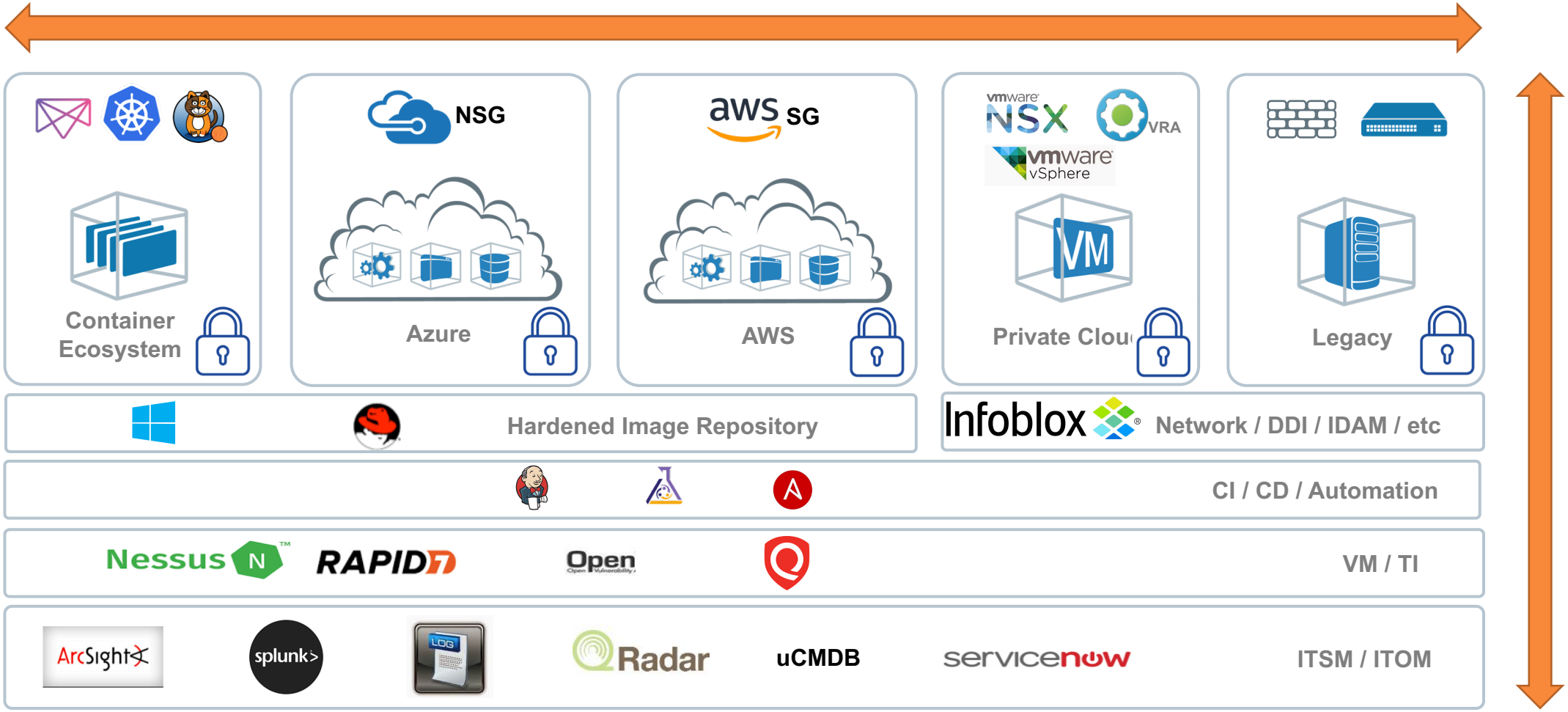
Distributed

Heterogeneous

Hybrid

Interdependent

Environments are Really Complex – Today's Modern Ecosystem



Micro-Segmentation Considerations

Supports all environments and platforms

Maps all application communication

Intuitive rule writing approach

Model and test policy before enforcement

Intuitive GUI and fully programable API

Centralized policy creation…Distributed enforcement

Customizable granularity

Protect data-in-motion between segments

How to Implement a Micro-Segmentation Strategy in 5 Steps

The 5 Steps

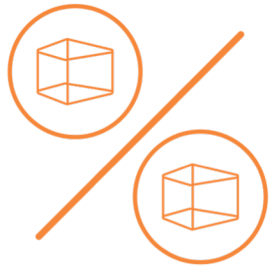
It’s as much about process as it is about technology.

Step 1: Get the right tools

Application dependency mapping

Vulnerability mapping

Policy management



Policy enforcement

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

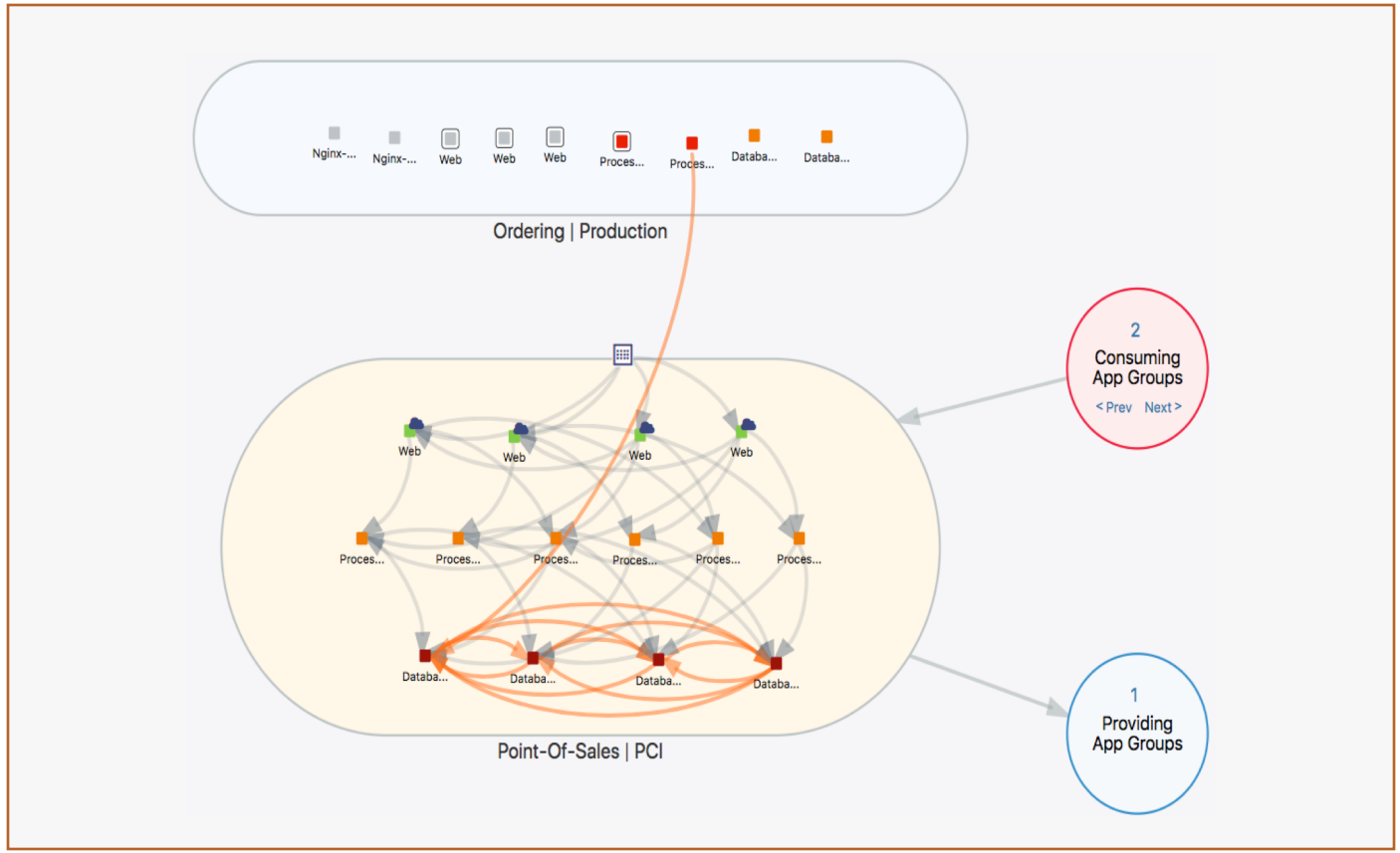
Step 2: Decide what to segment first

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

Key factors for prioritization:

- Value of data
- Compliance/audit requirements
- Vulnerability exposure
- Harm if there is an outage
- Value as a pivot point
- There’s no other way

Step 3: Map your application environment



1. Identify Core Services
2. Validate Interactions within the application group

   Engage the app teams
3. Focus connections between applications

The map should be real time and accurate

Step 4: Test *then* 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
- Combine Macro and Micro-Segmentation
- 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 and control activity into and out of a critical application

Vulnerability-Based Segmentation – limit the exposure of vulnerabilities
Tune policy to constrain or block the exposure of a vulnerability

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

Core Service 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 policies before enforcing
3. Build partnerships between security, infrastructure, and application teams
4. Segment in phases
5. Work with an internal champion who can drive the project

Ready to get started?

Visit the Illumio booth for more information