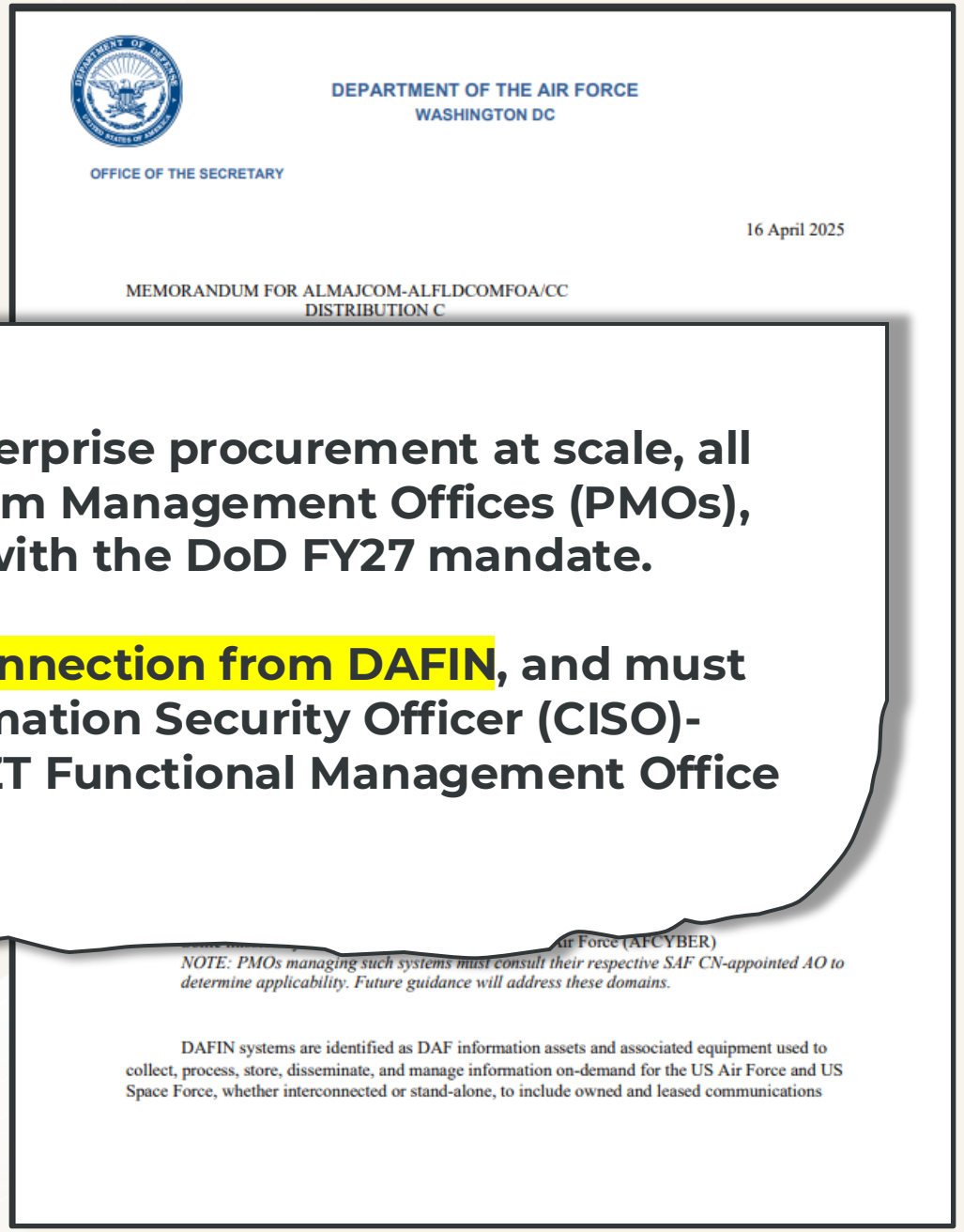
illumio

How the Air Force is meeting ZT mandates through Segmentation

Assume breach. Minimize impact. Increase resilience.

Gary Barlet, Public Sector CTO, Gary.Barlet@illumio.com

illumio



DEPARTMENT OF THE AIR FORCE
WASHINGTON DC

OFFICE OF THE SECRETARY

16 April 2025

MEMORANDUM FOR ALMAJCOM-ALFLDCOMFOA/CC
DISTRIBUTION C

ir Force (AFCYBER)
NOTE: PMOs managing such systems must consult their respective SAF CN-appointed AO to determine applicability. Future guidance will address these domains.

DAFIN systems are identified as DAF information assets and associated equipment used to collect, process, store, disseminate, and manage information on-demand for the US Air Force and US Space Force, whether interconnected or stand-alone, to include owned and leased communications

In order to realize fiscal efficiencies gained by enterprise procurement at scale, all DAF systems, including those managed by Program Management Offices (PMOs), must leverage the enterprise solution to comply with the DoD FY27 mandate.

Non-compliant systems risk quarantine and disconnection from DAFIN, and must self-identify to both the system's DAF Chief Information Security Officer (CISO)-appointed Authorizing Official (AO) and the DAF ZT Functional Management Office (FMO).

Illumio: Proven Leader in Containing Threats & Enabling Mission Resilience

PROTECTING MORE THAN

20 of the **Fortune 100**

3.5M+ workloads
For organizations of all sizes, from Fortune 100 to small business

PROVEN RESULTS WITH ILLUMIO

$3M
in tool consolidation and reduced firewall costs

$3.8M
in savings due to fewer outages and downtime

111%ROI
composite return over three years

90%
decrease in operational effort by Cybersecurity Teams

66%
reduction in impact of a breach

KEY DEPARTMENT OF DEFENSE CUSTOMERS

U.S. AIR FORCE

FEDERAL CERTIFICATIONS

FedRAMP
FedRAMP Moderate

NIAP

Common Criteria
Enterprise Security Management - Policy Management

FIPS VALIDATED 140-2

Illumio: Proven Leader in Containing Threats & Enabling Mission Resilience

Source: The Forrester Wave™: Microsegmentation Solutions, Q3 2024

KEY DEPARTMENT OF DEFENSE CUSTOMERS

U.S. AIR FORCE

FEDERAL CERTIFICATIONS

FedRAMP

FedRAMP Moderate

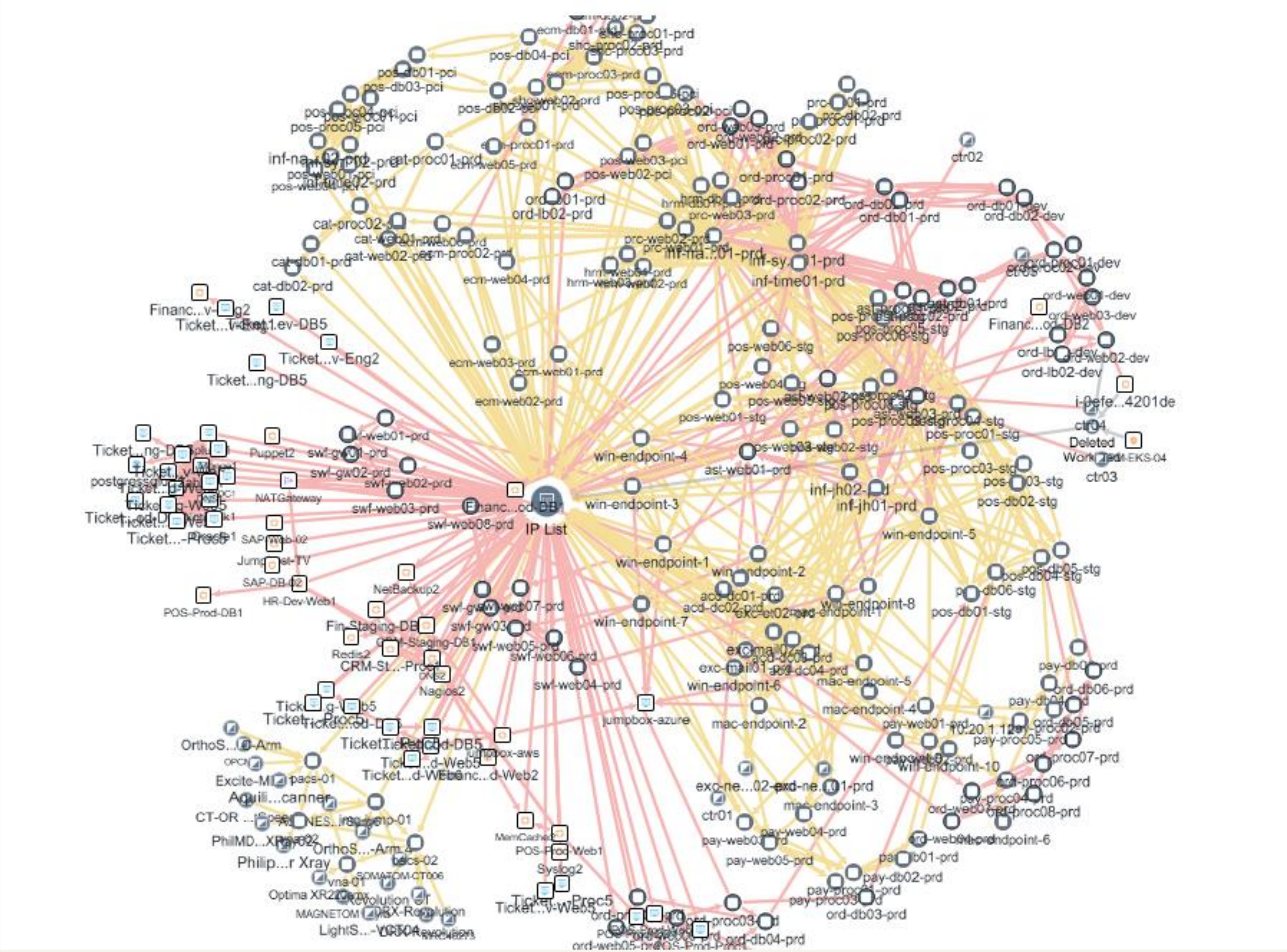
NIAP

Common Criteria

Enterprise Security Management - Policy Management

FIPS VALIDATED 140-2

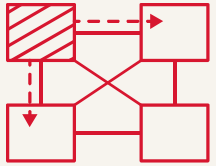
The reality of what we face...



Why are attacks successful?

Prevention and detection fails

- Undetected + unauthorized intrusion
- Attackers lurk for months – dwell time
- AI is increasing the effectiveness of attacks



Attack spreads

- Lateral movement allows attackers full network access
- Flat networks with no segmentation are defenseless

In a hyperconnected, hybrid, multi-cloud world, lateral movement is THE biggest risk

Critical assets compromised

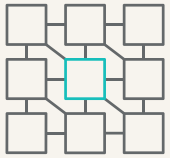
- Malware locks systems and demands ransom
- Risk of exfiltrated data and regulatory violations

Illumio ZTS Platform

The first platform for breach containment

Eliminate blind spots

Visualize all communications and traffic between workloads across on-prem and cloud environments.



Prevent lateral movement

Lower risk of adversaries accessing sensitive information by controlling east-west traffic.

Ringfence high-value assets

Proactively control communications and **isolate mission-critical applications and environments**.

Stage Policies

Implement policies **prior to mission execution** and **continue to enforce** policy based on last instructions received.

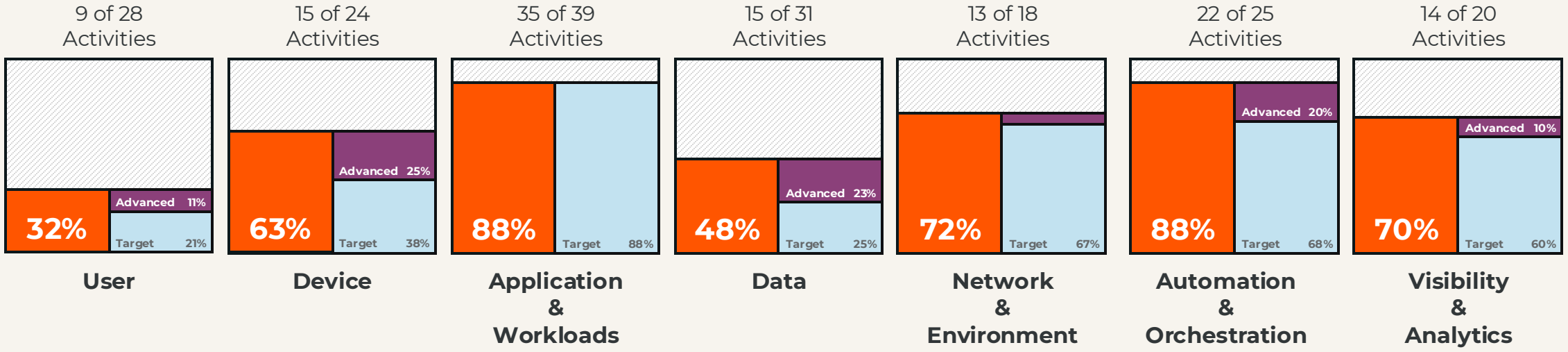
Continuous protection in DDIL

Maintain protection in **disconnected and air-gapped networks**, even if access to Illumio is lost.

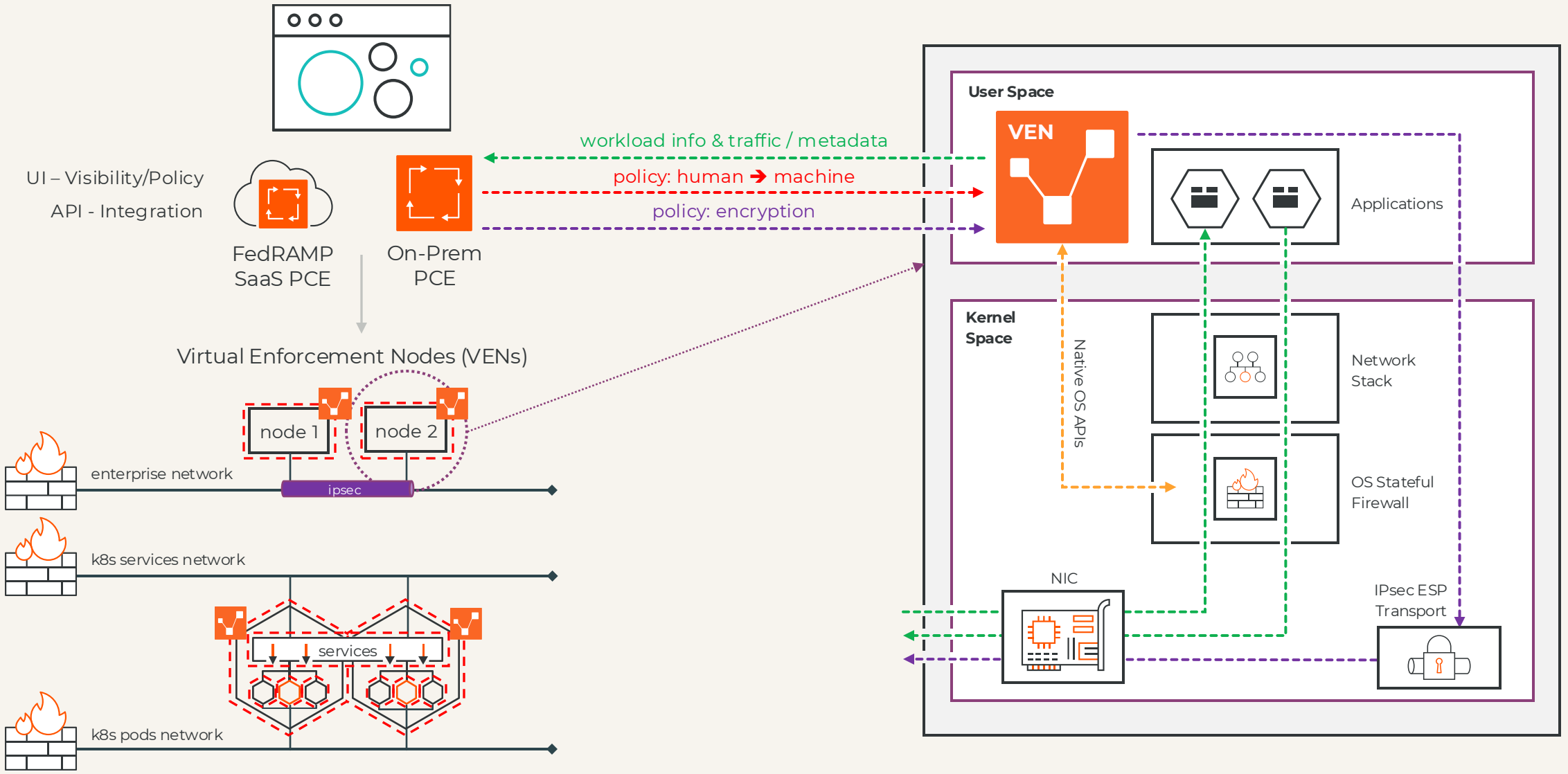
Lightweight Footprint

Minimum compute and bandwidth requirements, utilizing **non-disruptive** deployment and upgrades.

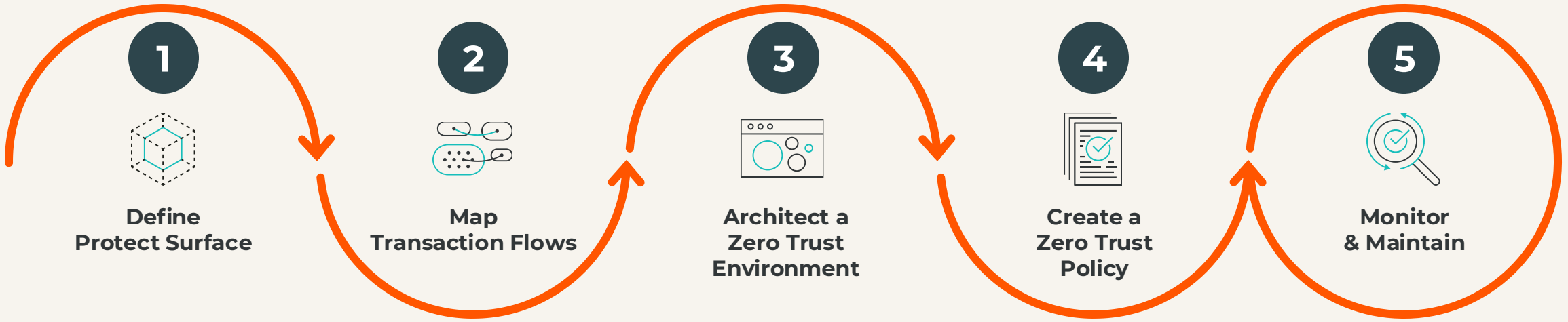
Illumio Mapping to DoD Zero Trust Reference Architecture



Illumio Architecture and Components

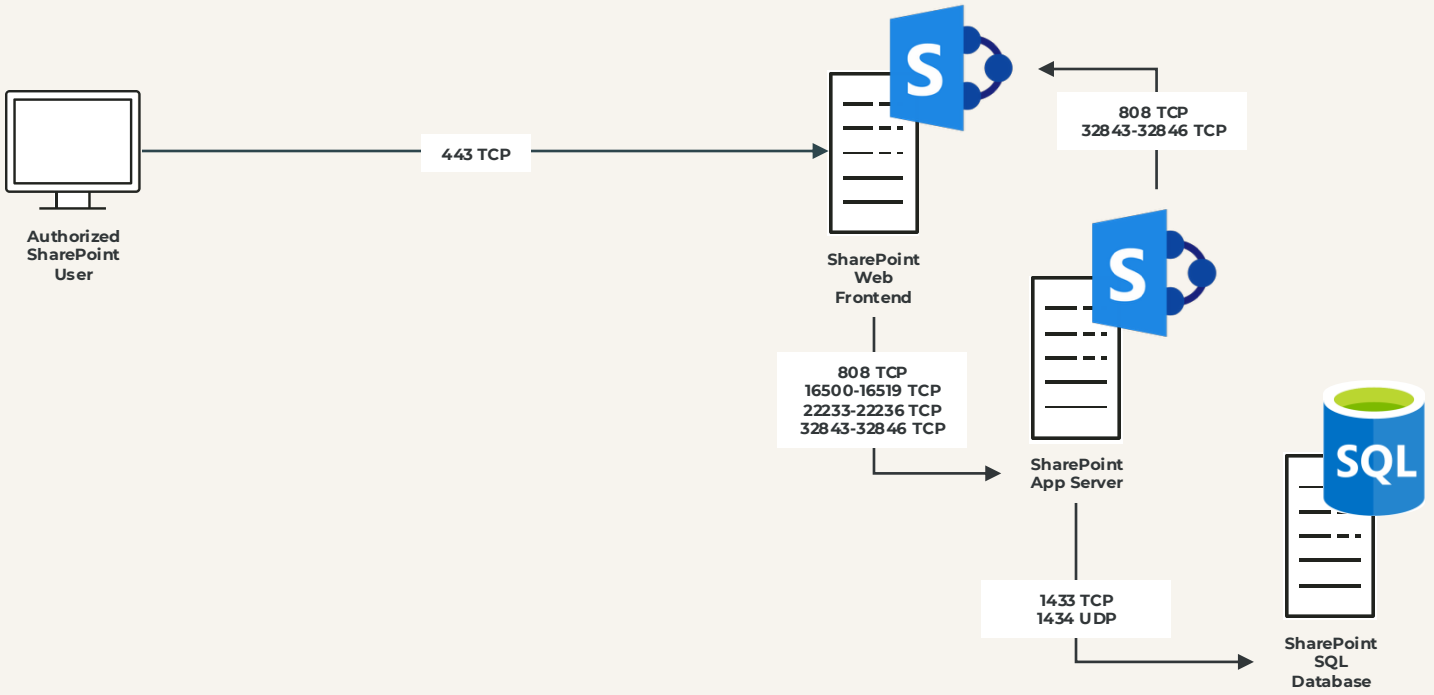


5-Step Methodology for Deploying Zero Trust



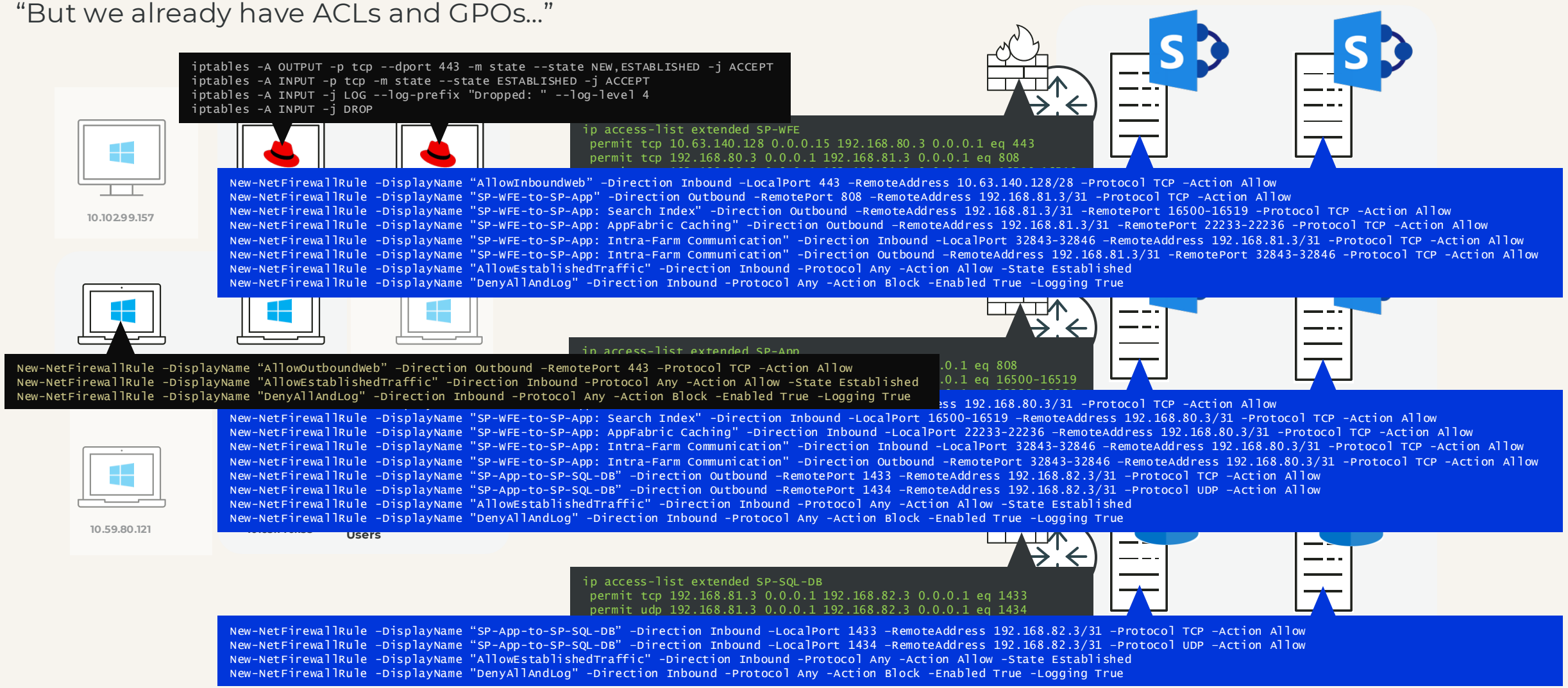
Securing a multi-tiered application

Microsoft SharePoint

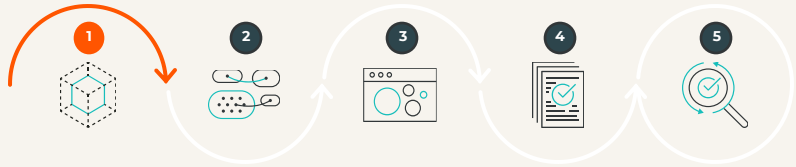


Securing a multi-tiered application

"But we already have ACLs and GPOs..."



Define the Protect Surface



L-RIC E-Prod A-SP Users R-Endpoint

10.102.99.157

10.63.140.129

SP Users

10.63.140.130

10.63.140.131

SP Users

10.63.140.132

10.209.156.111

10.59.80.121

10.63.140.133

SP Users

10.63.140.134

Illumio
Policy Compute Engine
"The Brains"

Container Workload Info

L-RIC E-Prod A-SharePoint R-Web

SharePoint WFE-1 192.168.80.3

SharePoint WFE-2 192.168.80.4

L-RIC E-Prod A-SharePoint R-App

SharePoint App-1 192.168.81.3

SharePoint App-2 192.168.81.4

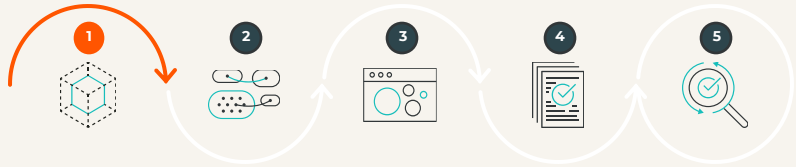
L-RIC E-Prod A-SharePoint R-DB

SQL-1 192.168.82.3

SQL-2 192.168.82.4

Virtual Enforcement Node
Lightweight Agent

Define the Protect Surface



L-RIC E-Prod A-SP Users R-Endpoint

10.102.99.157

10.63.140.129

SP Users

10.63.140.130

10.63.140.131

SP Users

10.63.140.132

10.209.156.111

10.59.80.121

10.63.140.133

SP Users

Heartbeat & Telemetry

10.63.140.134

Illumio
Policy Compute Engine
"The Brains"

Container Workload Info

L-RIC E-Prod A-SharePoint R-Web

SharePoint Web-1 192.168.80.3

SharePoint Web-2 192.168.80.4

L-RIC E-Prod A-SharePoint R-App

SharePoint App-1 192.168.81.3

SharePoint App-2 192.168.81.4

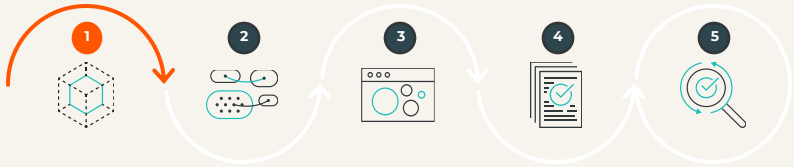
L-RIC E-Prod A-SharePoint R-DB

SQL-1 192.168.82.3

SQL-2 192.168.82.4

Virtual Enforcement Node
Lightweight Agent

Define the Protect Surface



L-RIC E-Prod A-SP Users R-Endpoint

10.102.99.157

10.63.140.129

SP Users

10.63.140.130

10.63.140.131

SP Users

10.63.140.132

10.209.156.111

10.59.80.121

10.63.140.133

SP Users

10.63.140.134

Illumio
Policy Compute Engine
"The Brains"

Heartbeat & Telemetry

Illumination Map

L-RIC E-Prod A-SharePoint R-Web

SharePoint WFE-1 192.168.80.3

SharePoint WFE-2 192.168.80.4

L-RIC E-Prod A-SharePoint R-App

SharePoint App-1 192.168.81.3

SharePoint App-2 192.168.81.4

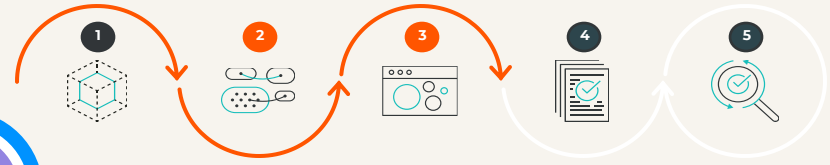
L-RIC E-Prod A-SharePoint R-DB

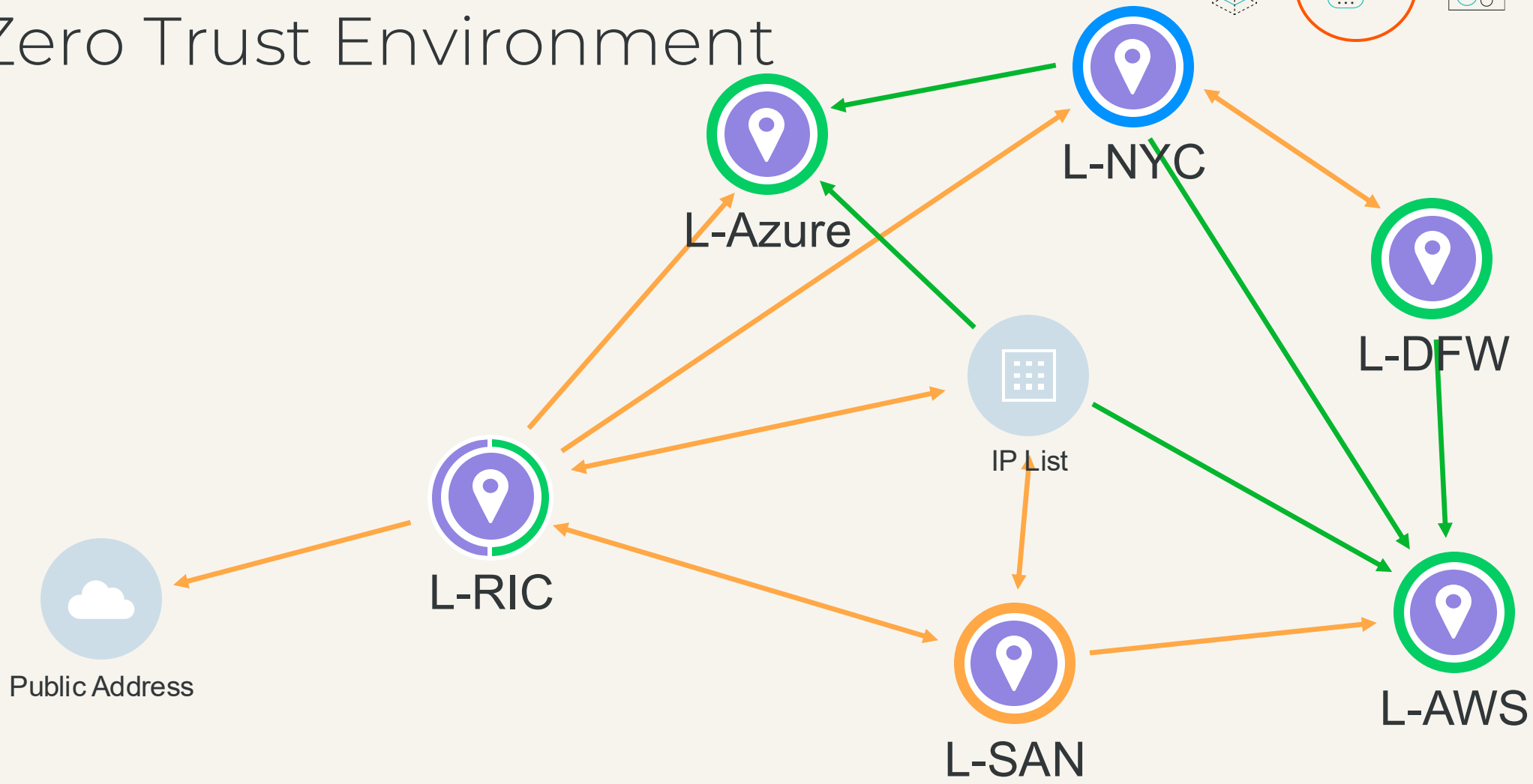
SQL-1 192.168.82.3

SQL-2 192.168.82.4

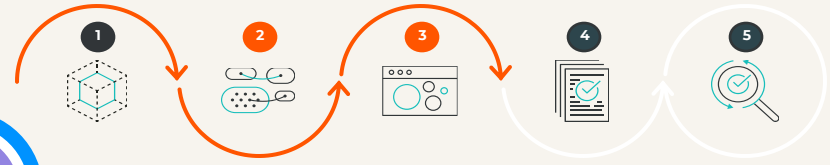
Virtual Enforcement Node
Lightweight Agent

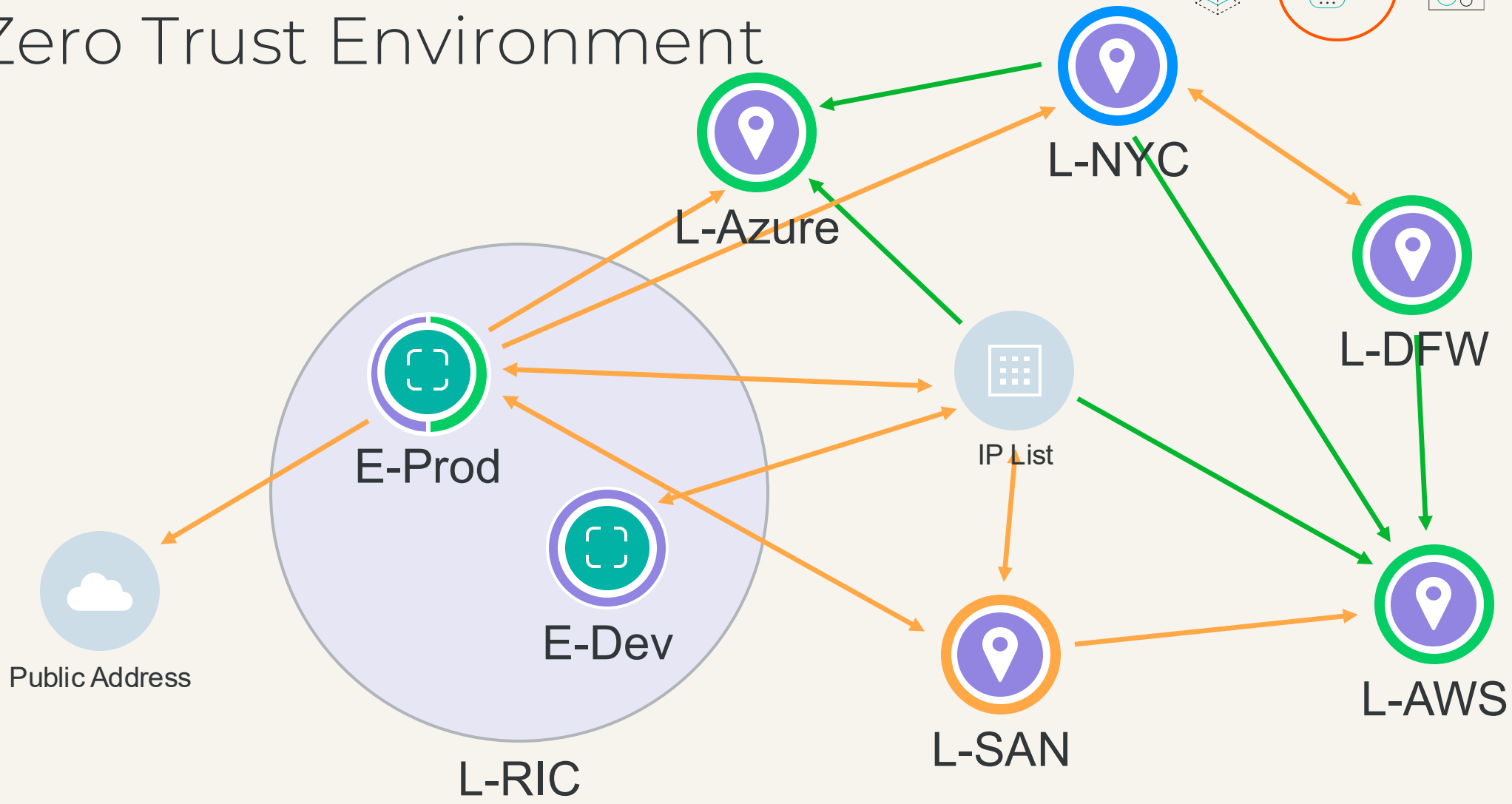
Map Transaction Flows & Architect Zero Trust Environment



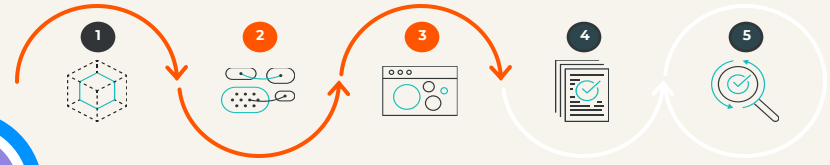


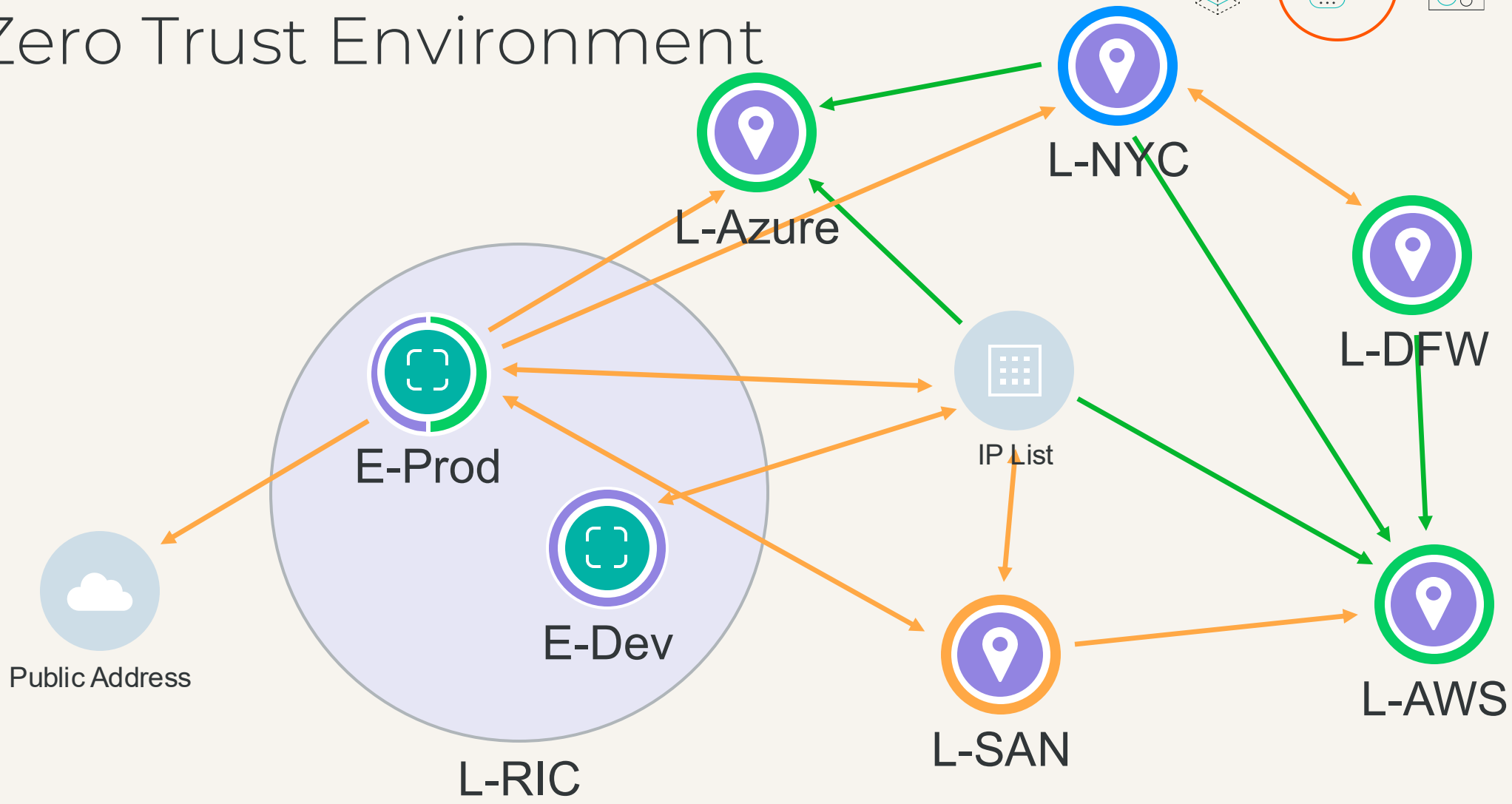
Map Transaction Flows & Architect Zero Trust Environment



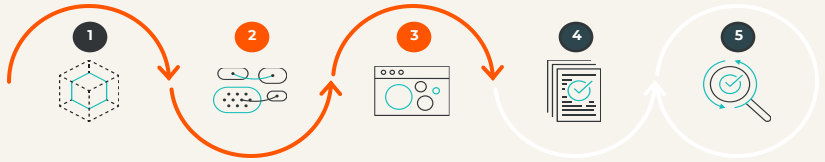


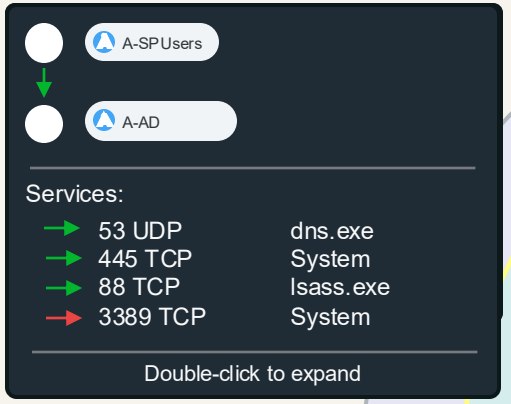
Map Transaction Flows & Architect Zero Trust Environment

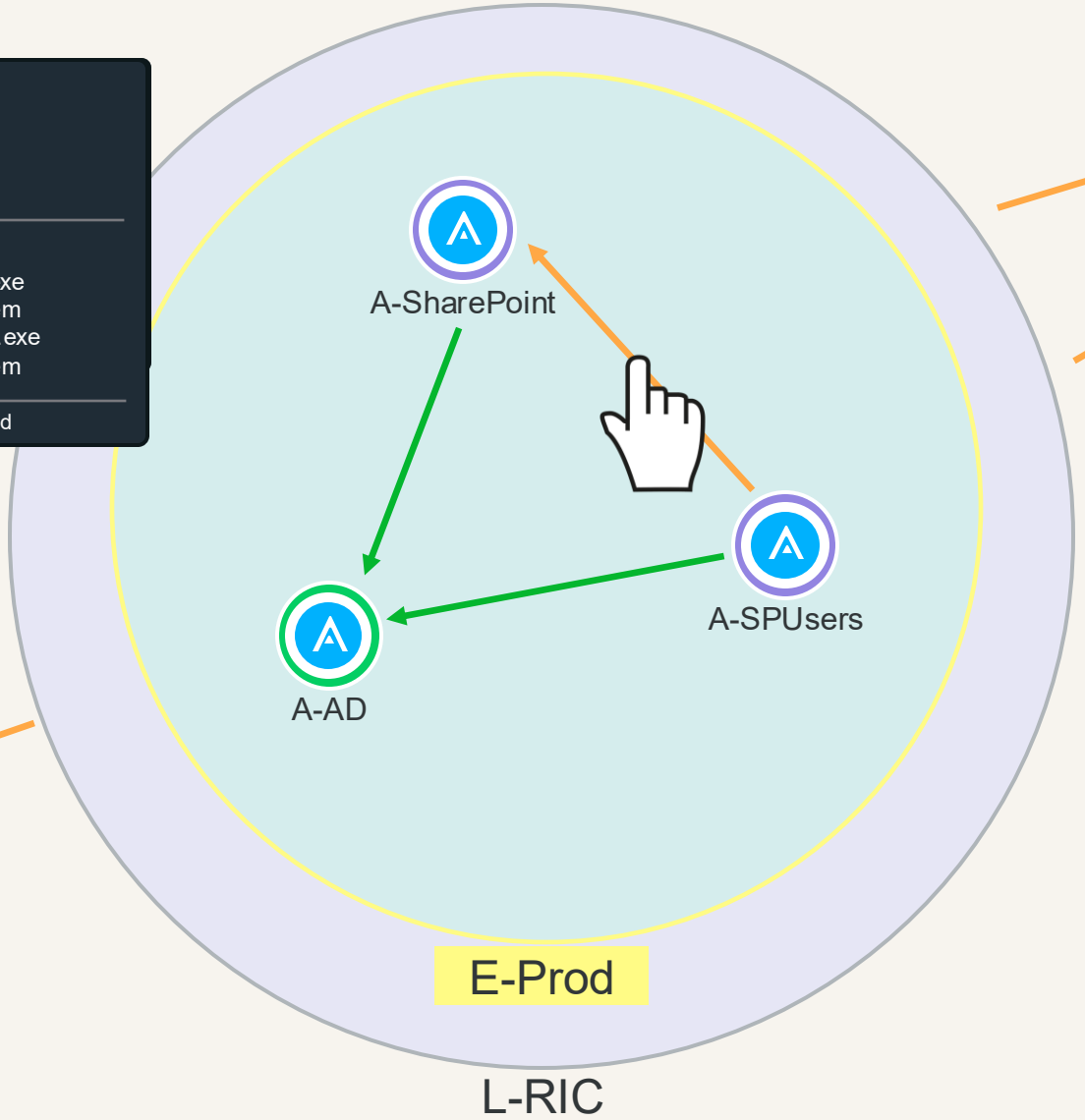


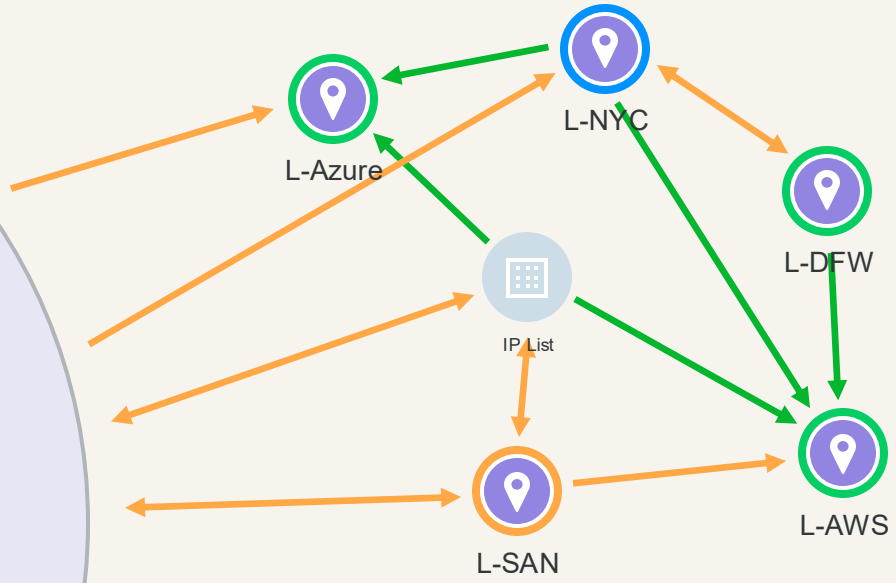


Map Transaction Flows & Architect Zero Trust Environment

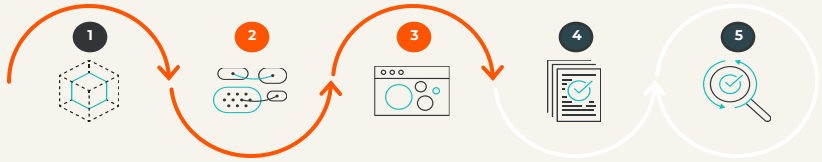


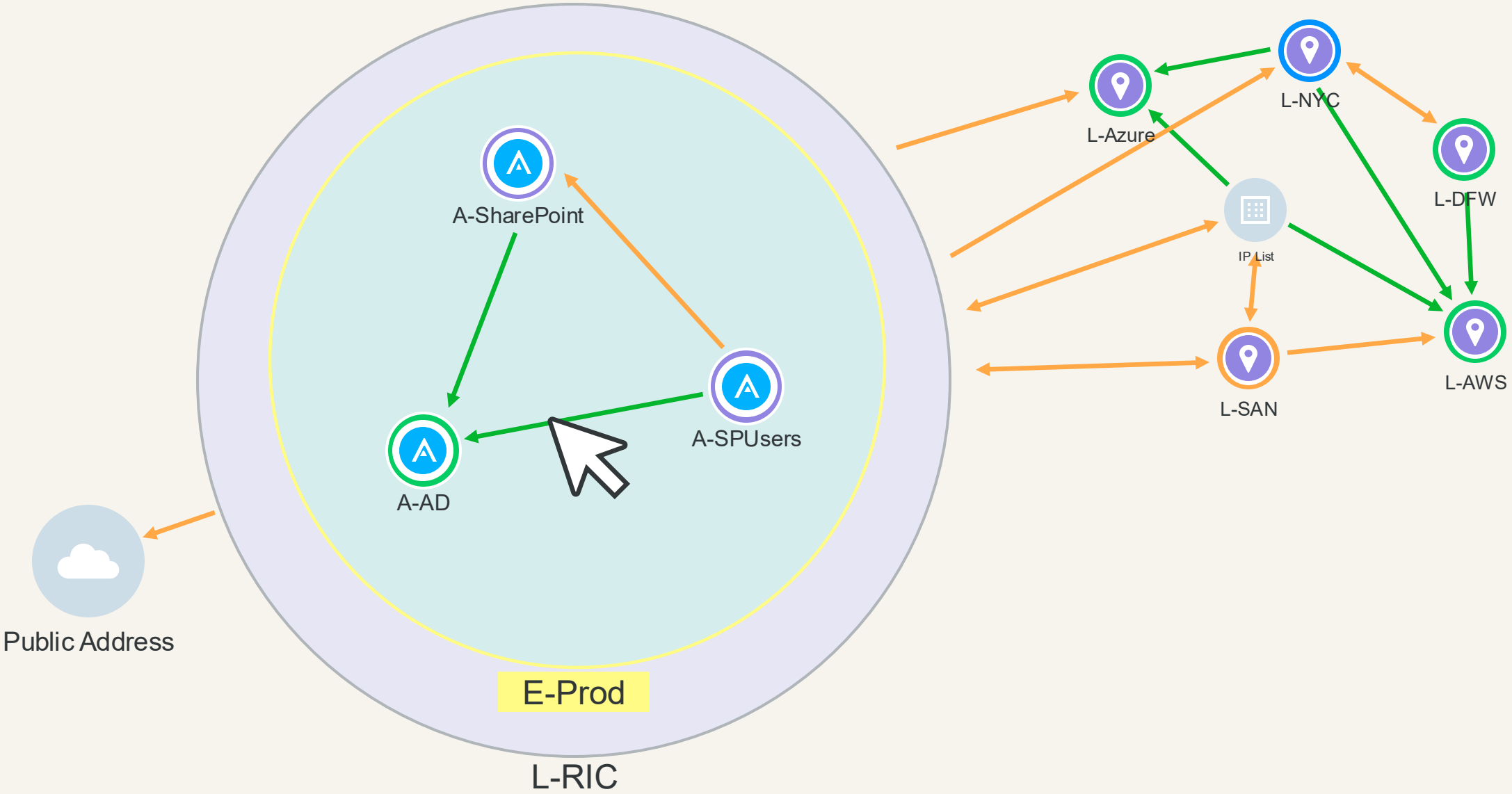




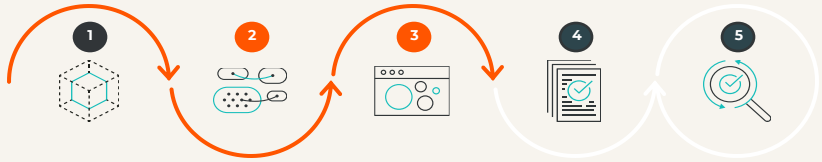


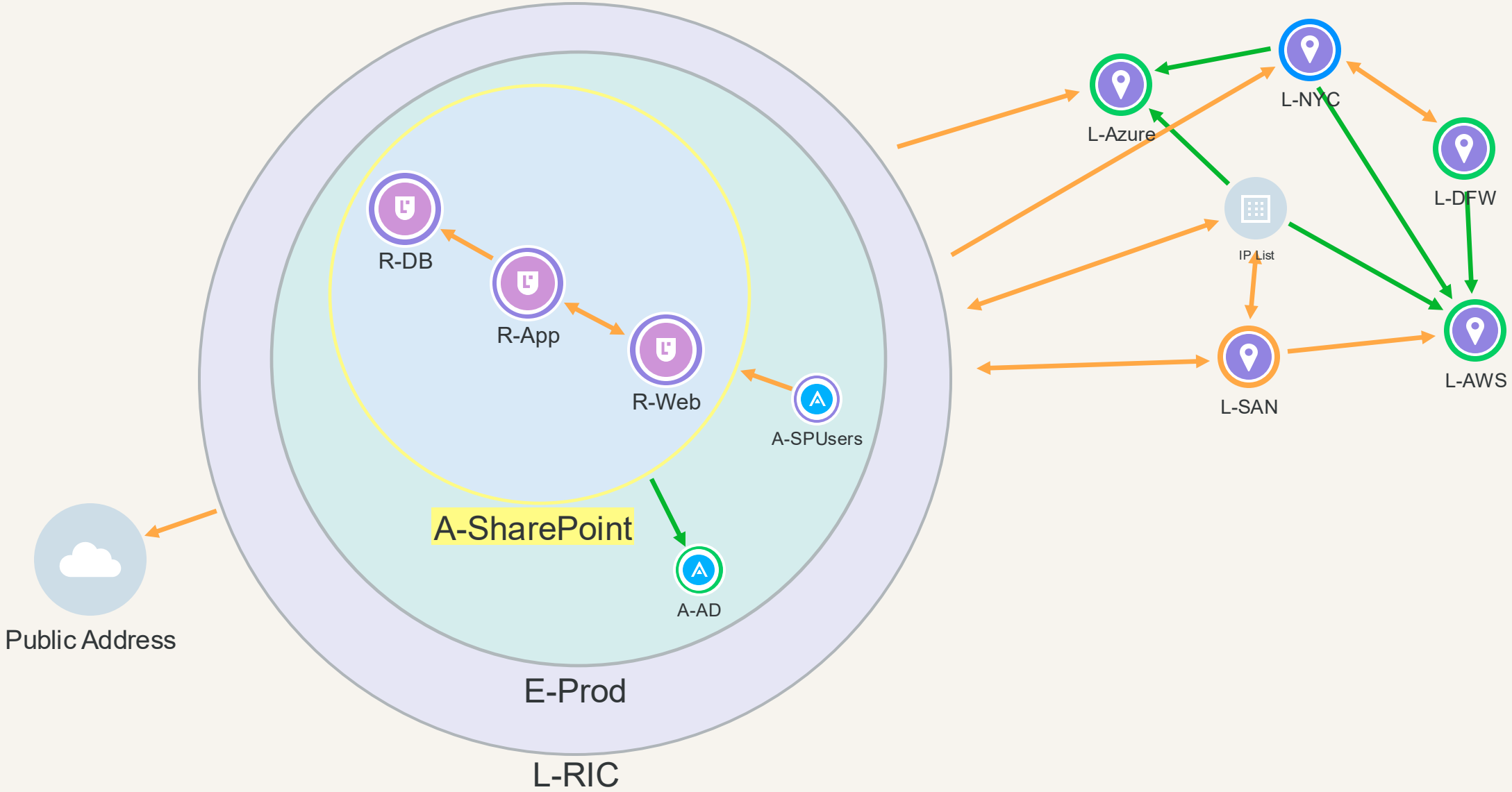
Map Transaction Flows & Architect Zero Trust Environment



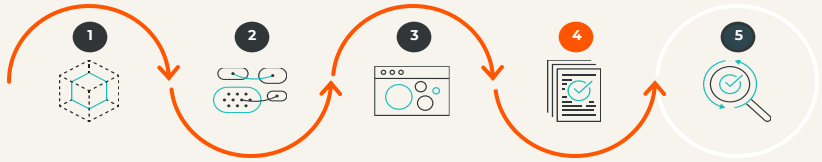


Map Transaction Flows & Architect Zero Trust Environment

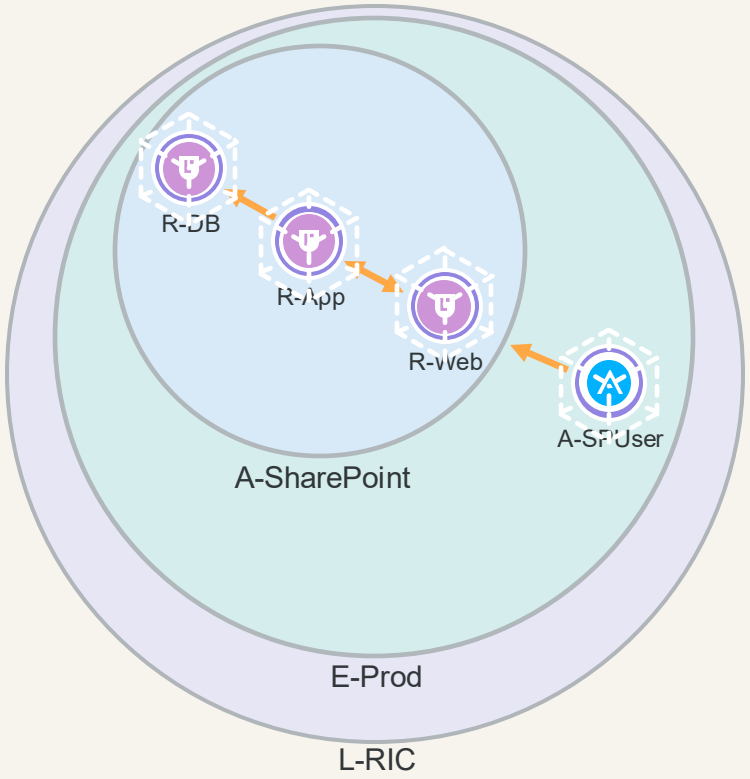




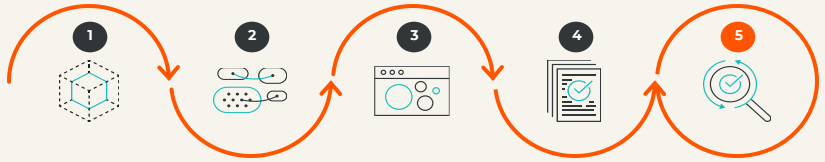
Create a Zero Trust Policy

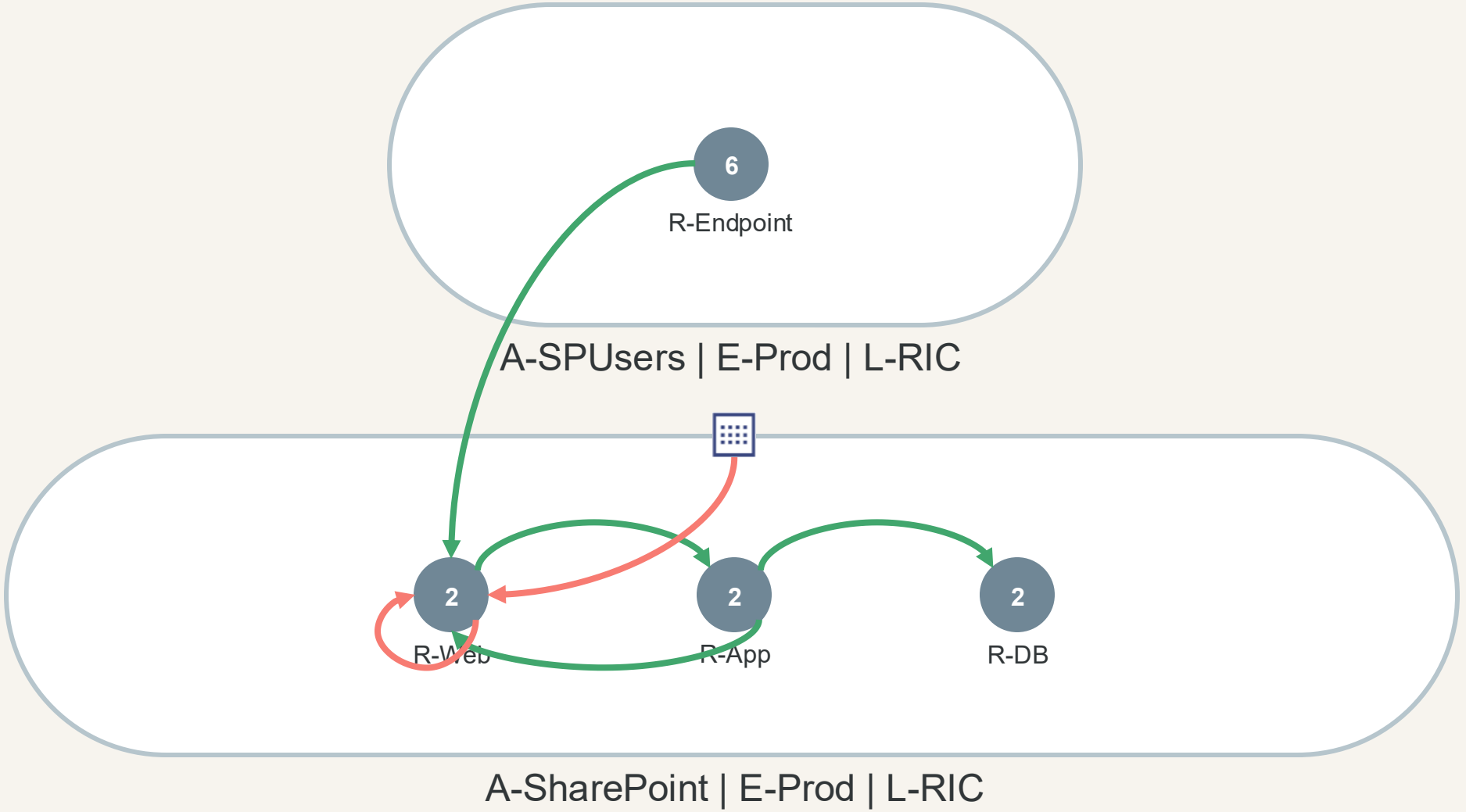


Natural Language	Illumio Label-Driven Policy Model
Define the **Protect Surface**	**Scope:** L-RIC, E-Prod, A-SharePoint
Web can talk to **App** using **SharePoint** services **App** can talk to **Web**, & **App** can talk to **App** using **SharePoint** services **App** can talk to **DB**, & **DB** can talk to **DB** using **SQL** services	**Intra-Scope Rulesets:** Sources: R-Web → Destinations: R-App → Destination Services: S-SP Intra-Farm Svcs Sources: R-App → Destinations: R-Web, R-App → Destination Services: S-SP Intra-Farm Svcs Sources: R-App, R-DB → Destinations: R-DB → Destination Services: S-SQL
SharePoint Users can access **Web** using **Secure HTTP**	**Extra-Scope Rulesets:** Sources: L-RIC, E-Prod, A-SPUsers → Destinations: R-Web → Destination Services: S-HTTPS

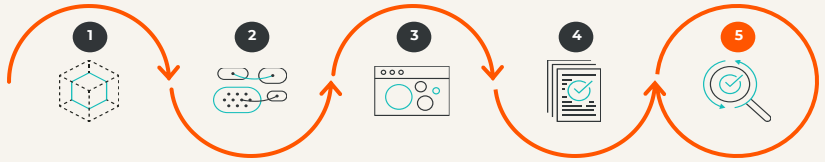


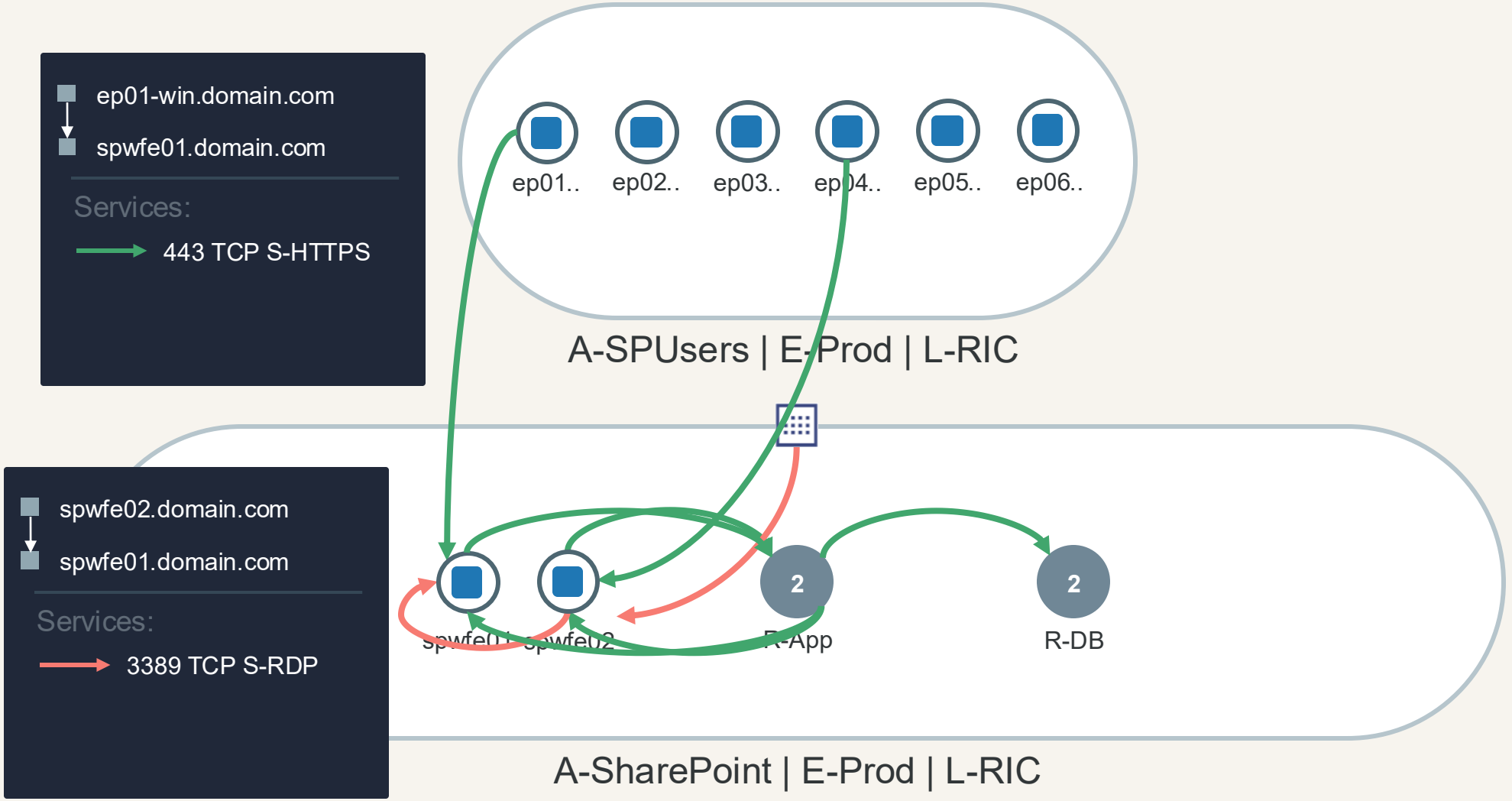
Monitor & Maintain: Never Trust, Always Verify





Monitor & Maintain: Never Trust, Always Verify





Current Air Force Highlights

By the Numbers

- ✓ **Over 13,000 Known Servers**
- ✓ **Over 8,900 Compatible Servers with VENs Installed (remaining 3,500+ are unmanaged)**
- ✓ **Over 9,300 Servers Fully Labeled**
- ✓ **Over 2,900 Applications in Micro-segmentation**
- ✓ **Over 770 Rules Written**
- ✓ **Over 180 Applications Transferred to Operations**

illumio

Thank you for your time