

Reducing Risk of Ransomware: Tightening security posture with micro-segmentation



Prof. Avishai Wool
CTO and Co-Founder



MOTIVATING EXAMPLE: LATERAL MOVEMENT / RANSOMWARE ATTACKS

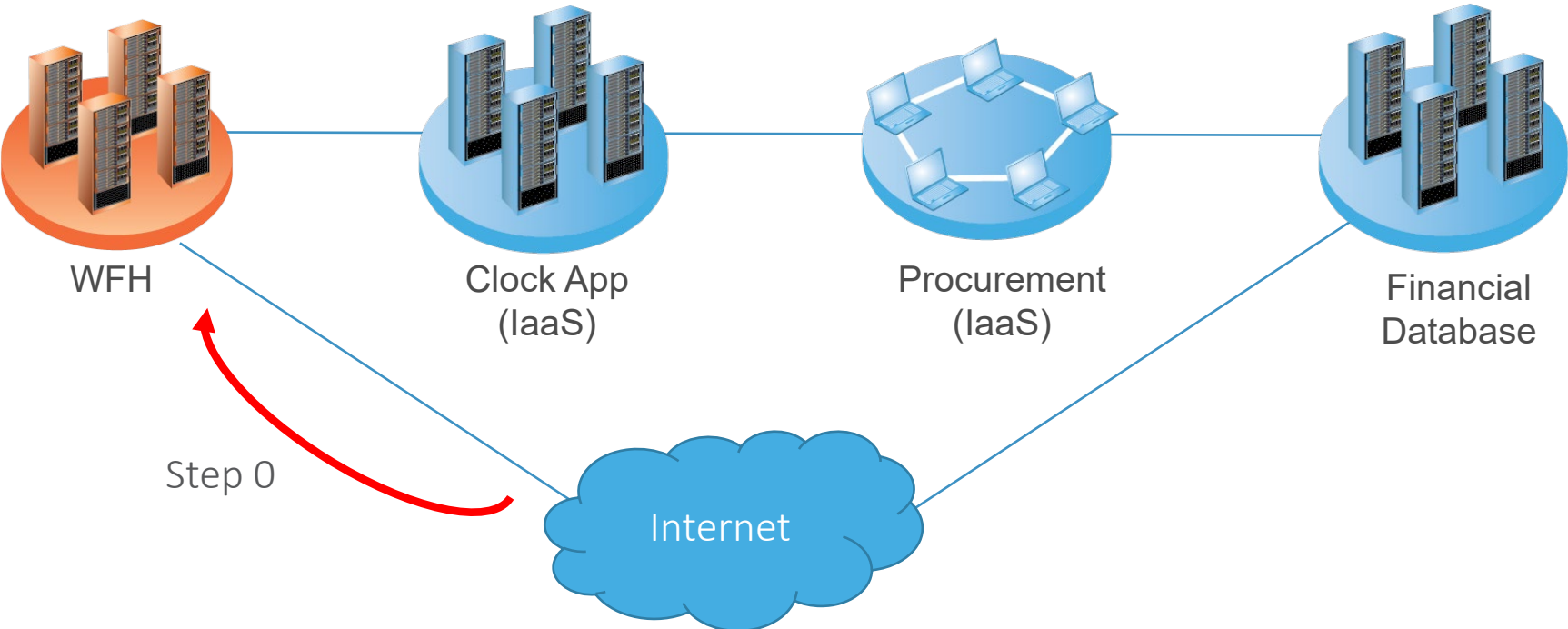
HOW?

1. Deliver exploits to 1st victim computer
2. Repeat per victim computer:
 - Encrypt file system
 - Encrypt accessible networked file shares
 - Move laterally: explore the network
 - Deliver exploits to next victim via network
3. Wait for victim to call
4. Collect ransom
5. Supply decryption key

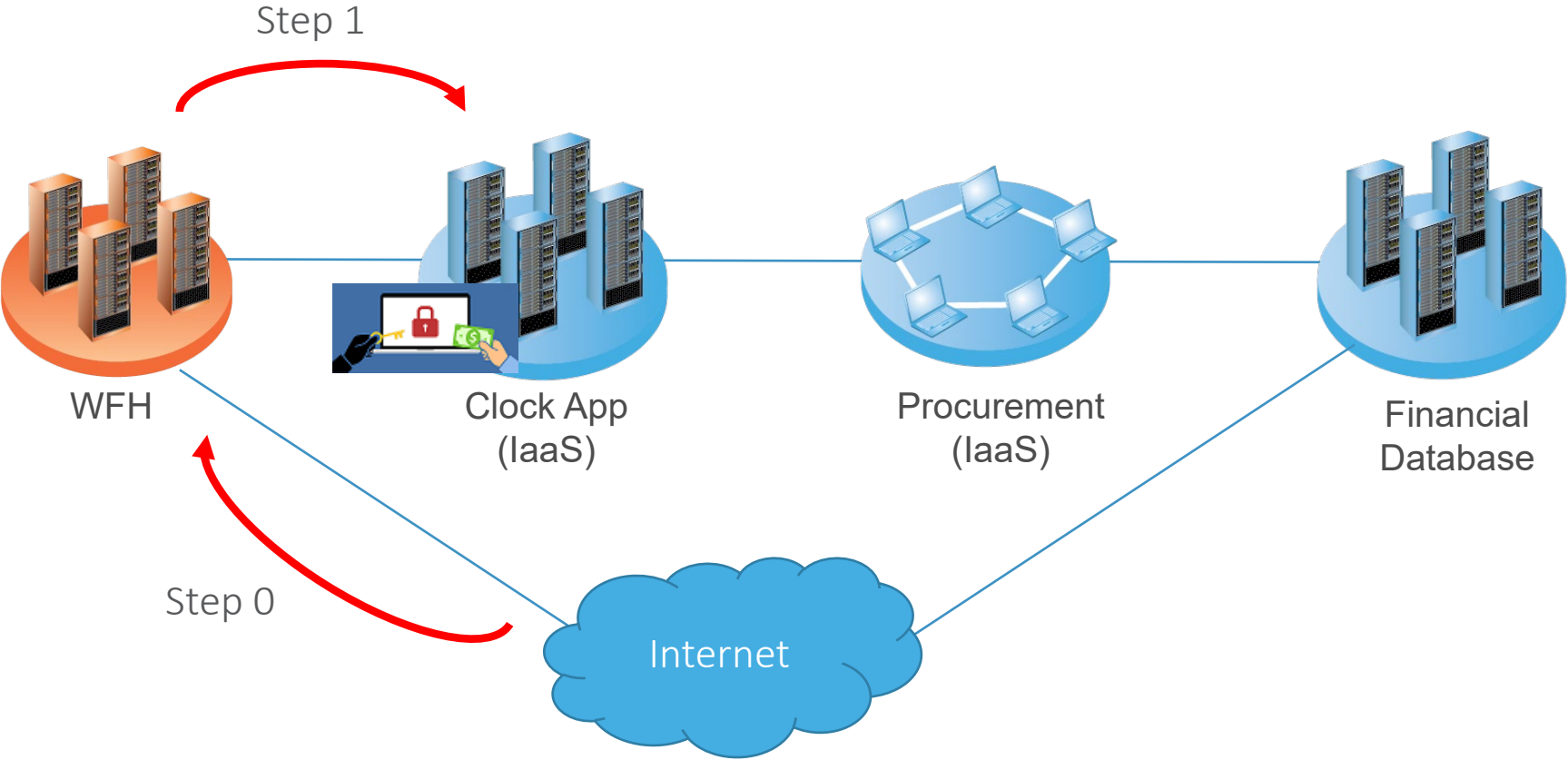


“Advanced Persistent Threat”, Wikipedia

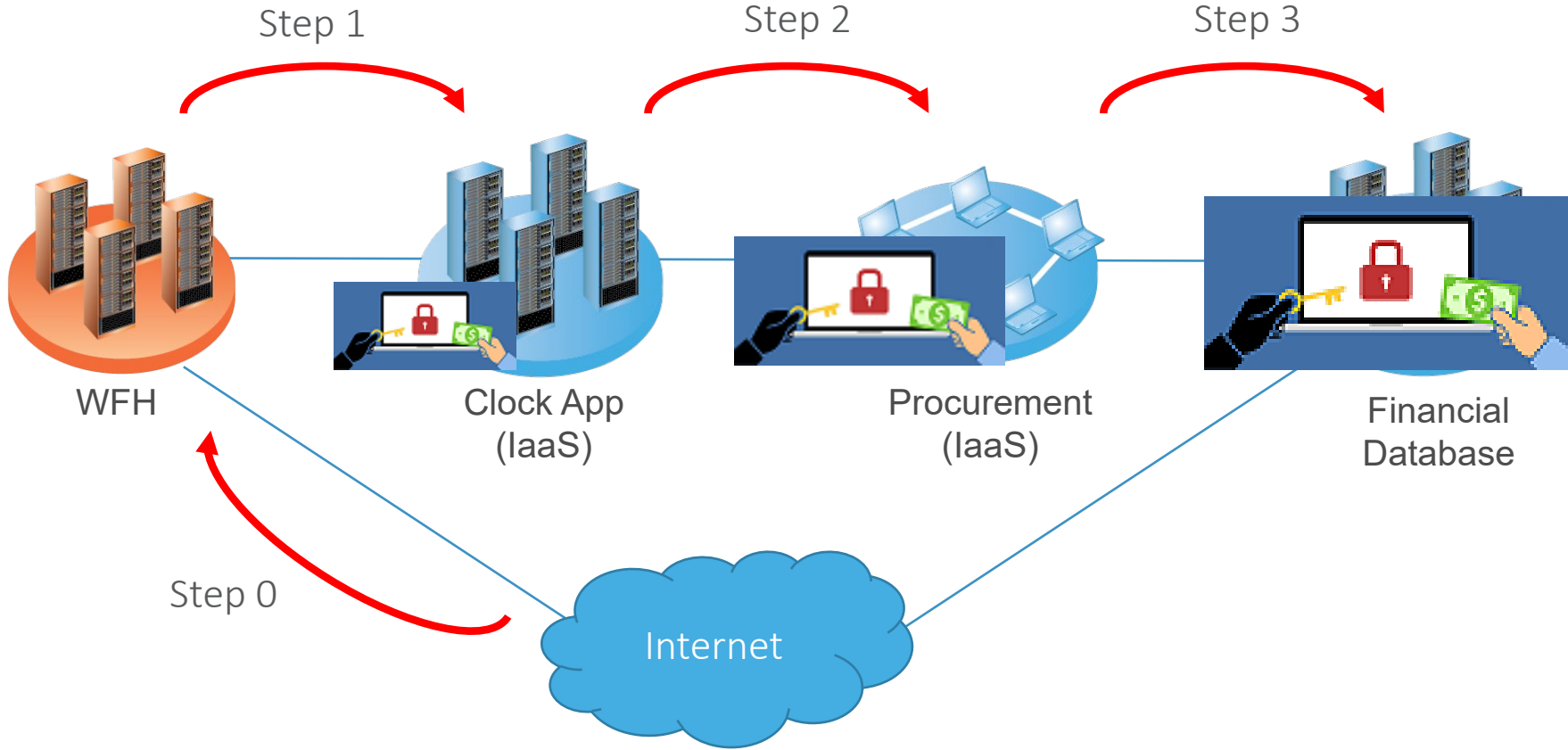
STEPPINGSTONES



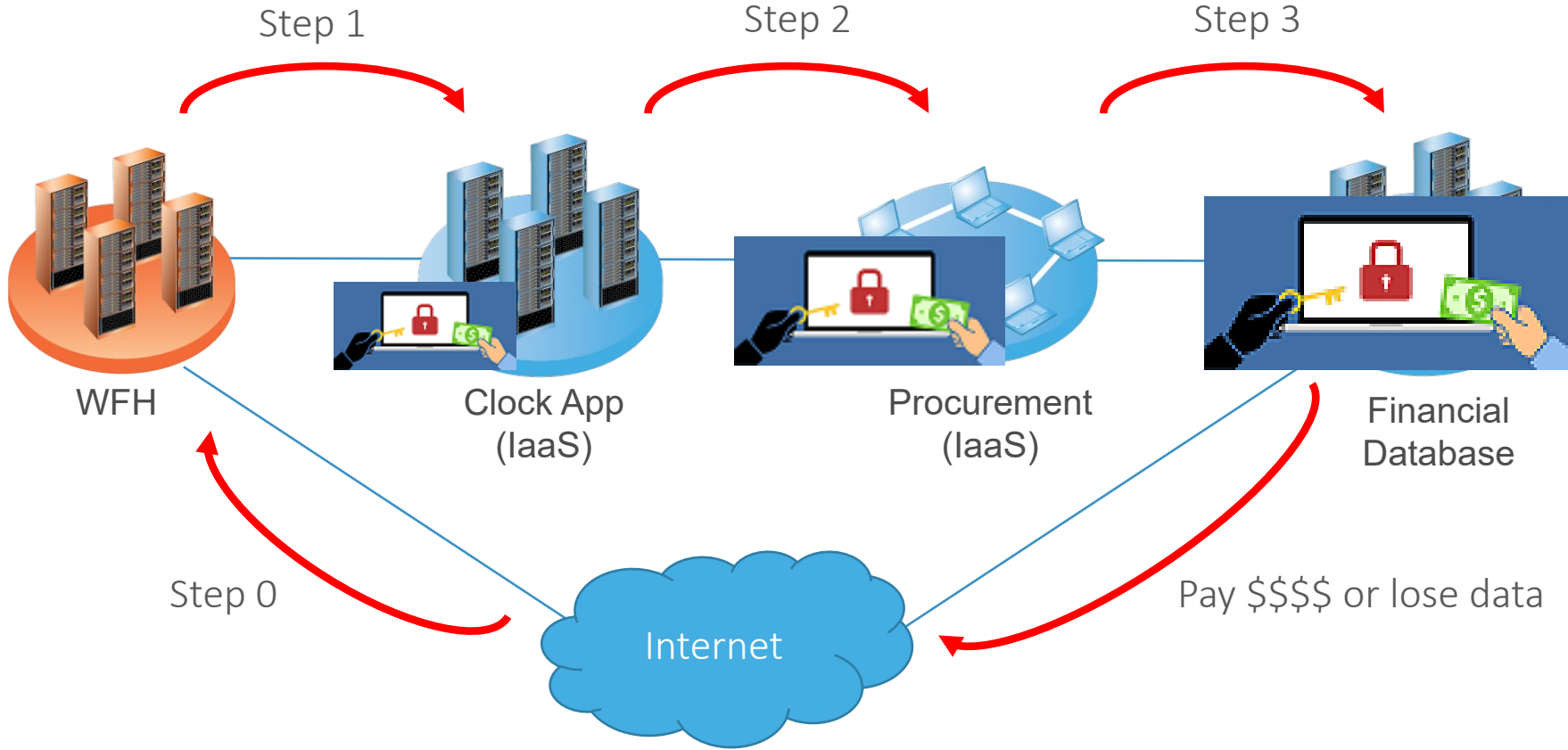
STEPPINGSTONES



STEPPINGSTONES



STEPPINGSTONES





MICRO-SEGMENTATION: REDUCING THE ATTACK SURFACE

“ZERO TRUST” == MICRO-SEGMENTATION?

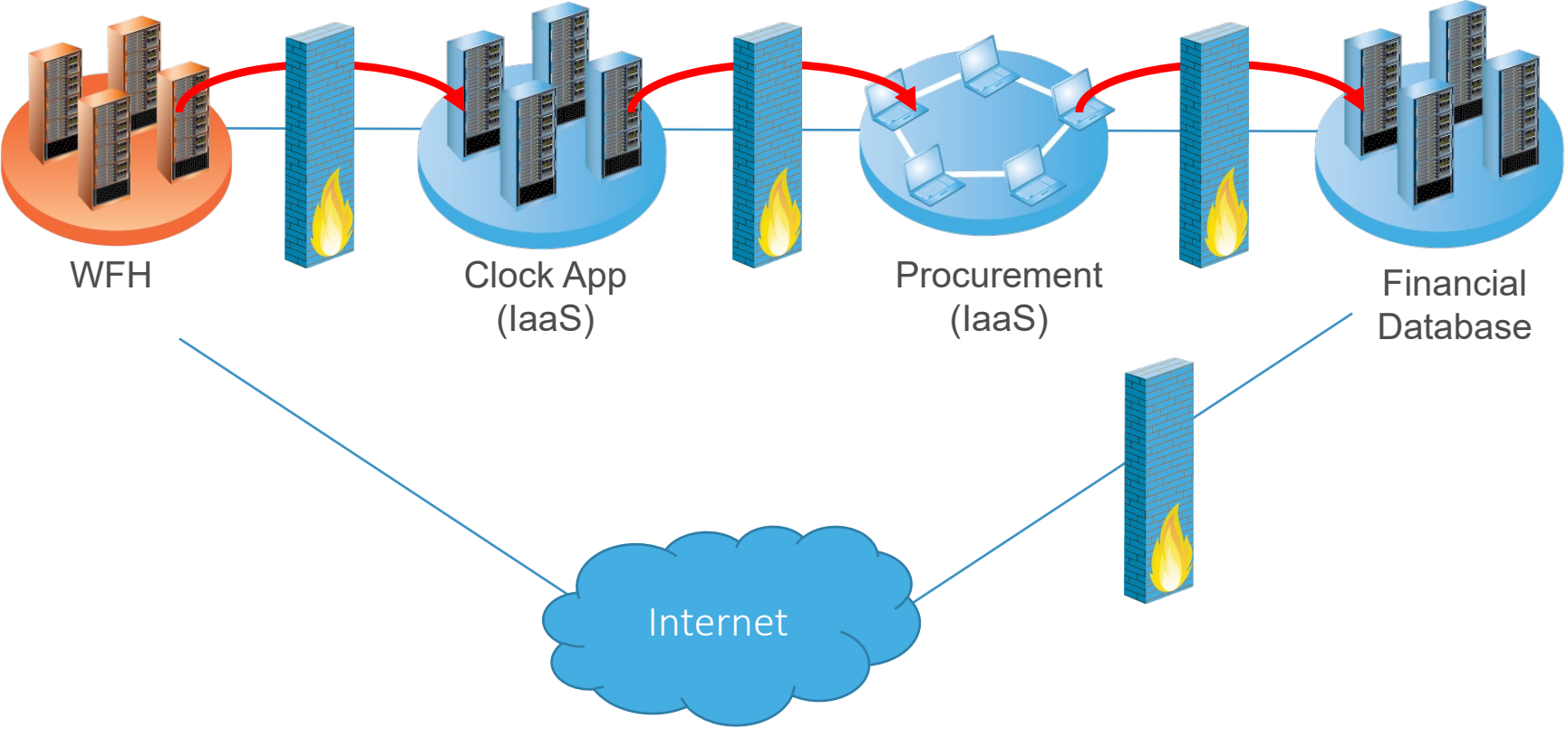
- “Zero Trust” is really a philosophy, not a technology
 - No traffic and communications should be trusted, from both outside and inside the data center
- Micro-segmentation is a “zero trust” implementation strategy at the network layer
 - The modern equivalent of “default deny”

MICRO-SEGMENTATION: A BLUEPRINT

- Define network segments to control east-west traffic
- Activate traffic filters crossing segments
 - Traffic fully inside a segment can flow freely
- Write restrictive policies for traffic crossing segment borders

CONTROL EAST-WEST TRAFFIC

Easy, right?



TRADITIONAL EXCUSES IN A TRADITIONAL DATA CENTER

Use standard or virtualized firewalls

Requires:

- Reassigning IP addresses
- Making routing changes
- Defining new VLANs
- Possibly connecting new cables

Hard Work!

SOFTWARE-DEFINED DATA CENTERS

- Comes with filtering capabilities inside the networking fabric
 - Reassigning IP addresses
 - Making routing changes
 - Defining new VLANs
 - Possibly connecting new cables

Old excuses are gone!

- On-premise virtualized data center:

- Cisco ACI
- VMware NSX



- Public cloud:

- Amazon AWS
- Microsoft Azure
- Google Cloud



Technology is just the 1st step.
You still need to configure it!

NEXT CHALLENGES

- What filtering policy should you write ?
 - So all legitimate business traffic is allowed!
- To do this – you just need to know (the intent of) all the legitimate traffic in the data center, so you can write policy allowing it.

Naturally, you have perfectly accurate records of all the application flows running through the data center, so it's easy. right?



FOR EVERYONE ELSE: APPLICATION DISCOVERY

- Need to:
 - Detect all the network flows
 - Annotate them with application name (“intent”)
 - Aggregate & optimize “thin” flows into “fat” flows
 - Place in the filtering policy
- How:
 - Netflow → AlgoSec AutoDiscovery
or Cisco Secure Workload (formerly Tetration) → AutoDiscovery)
 - Import into AlgoSec AppViz
- Results:
 - Micro-segmentation knowhow
 - Application name annotates current + future rules that support it

USE CASE 1: DISCOVERY OF INTENT

Discovery

Discover business applications and import them into AppViz

AutoDiscovery

Automatically discover your business applications using AlgoSec AutoDiscovery

Cisco Tetration

Automatically discover your business applications using Cisco Tetration

Import Flows from File

Import flows using a CSV file

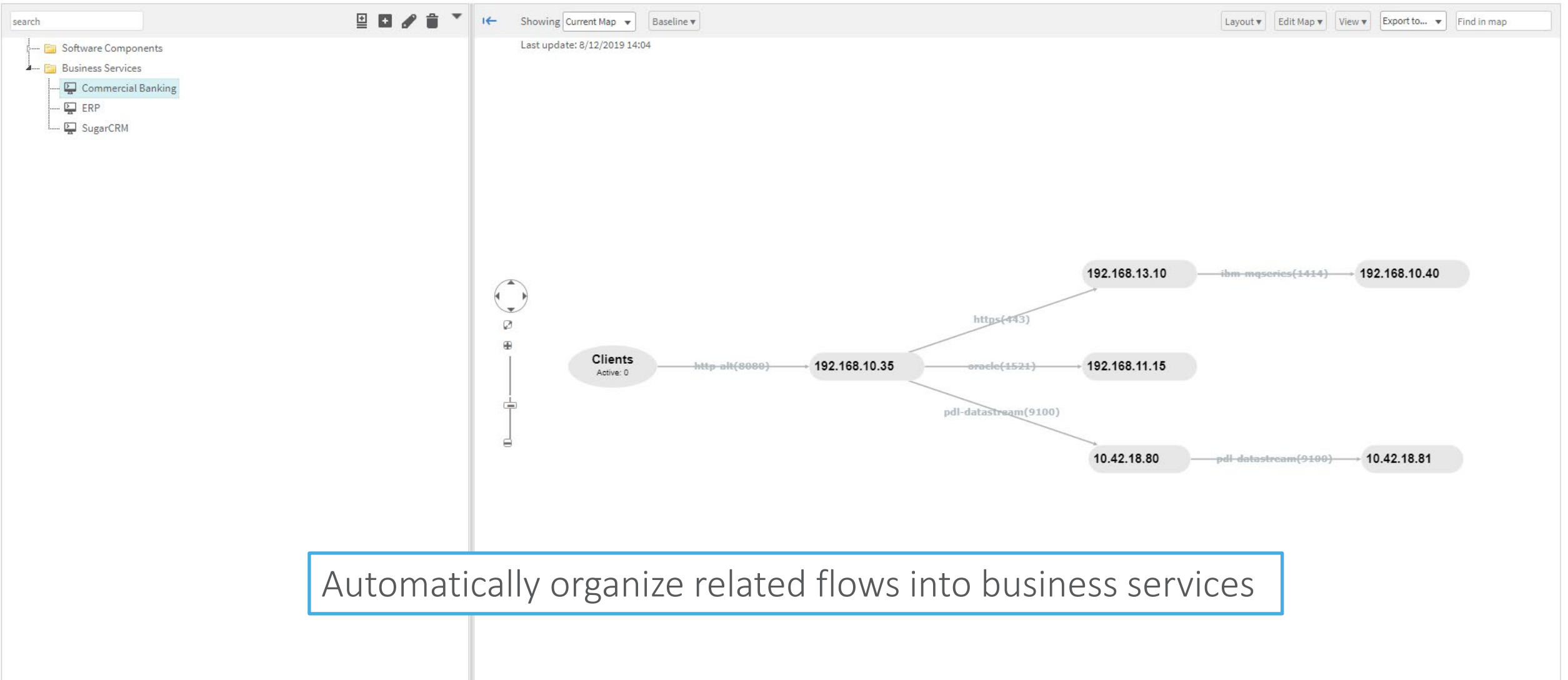
New business services

Discover Selected Discover by Server/Port Multiple entry points- Create/Add Hide entry points Show all Search

Name	URL	Server	Port	Virtual	Clients	Last Seen	Freq.	Match
10.200.12.118:8080	http://10.200.12.118:8080	10.200.12.118	8080 (http-alt)	false	10	174 days ago	High	105
ERP	http://erp	192.168.11.25	443 (https)	false	6	174 days ago	High	101
10.200.15.125:80	http://10.200.15.125	10.200.15.125	80 (http)	false	4	174 days ago	High	99
Trading	http://trading	10.200.12.11	443 (https)	false	3	174 days ago	High	98
ATM	http://atm	192.168.11.11	443 (https)	false	2	174 days ago	High	97
Pension Management	http://pensionmgmt	192.168.10.55	443 (https)	false	2	174 days ago	Medium	90
192.168.10.30:443	https://192.168.10.30	192.168.10.30	443 (https)	false	1	174 days ago	Medium	89
192.168.13.11:443	https://192.168.13.11	192.168.13.11	443 (https)	false	1	174 days ago	Medium	89
Asset Management	http://assetmgmt	192.168.11.10	80 (http)	false	10	174 days ago	High	75
10.200.12.24:9443	9443 (illumini)	10.200.12.24	9443 (illumini)	false	1	174 days ago	High	66
10.200.12.153:5555	5555 (personal-agent)	10.200.12.153	5555 (personal-agent)	false	1	174 days ago	Medium	59
192.168.9.62:1372	1372 (fc-ser)	192.168.9.62	1372 (fc-ser)	false	1	174 days ago	Medium	59
192.168.9.12:1623	1623 (jaleosnd)	192.168.9.12	1623 (jaleosnd)	false	1	174 days ago	Medium	59
192.168.10.45:7500	7500 (silhouette)	192.168.10.45	7500 (silhouette)	false	1	174 days ago	Medium	59
192.168.12.30:2049	2049 (nfs)	192.168.12.30	2049 (nfs)	false	1	174 days ago	Medium	59
192.168.12.46:50000	50000	192.168.12.46	50000	false	1	174 days ago	Medium	59
192.168.10.41:9100	9100 (pdl-datastream)	192.168.10.41	9100 (pdl-datastream)	false	1	174 days ago	Medium	59
10.200.15.135:1521	1521 (oracle)	10.200.15.135	1521 (oracle)	false	10	174 days ago	High	55
192.168.9.105:1355	1355 (intuitive-edge)	192.168.9.105	1355 (intuitive-edge)	false	1	174 days ago	Low	52
192.168.9.119:1228	1228 (florence)	192.168.9.119	1228 (florence)	false	1	174 days ago	Low	52
192.168.9.125:1771	1771 (vaultbase)	192.168.9.125	1771 (vaultbase)	false	1	174 days ago	Low	52
192.168.9.178:1106	1106 (isoipsigport-1)	192.168.9.178	1106 (isoipsigport-1)	false	1	174 days ago	Low	52
192.168.13.10:443	https://192.168.13.10	192.168.13.10	443 (https)	false	7	174 days ago	High	52
10.200.15.112:1433	1433 (ms-sql-s)	10.200.15.112	1433 (ms-sql-s)	false	4	174 days ago	High	49
192.168.12.22:1433	1433 (ms-sql-s)	192.168.12.22	1433 (ms-sql-s)	false	3	174 days ago	High	48
192.168.12.36:1521	1521 (oracle)	192.168.12.36	1521 (oracle)	false	1	174 days ago	Medium	39

Netflow (e.g., from VMware / Router / ...)

Business Services



Automatically organize related flows into business services

AutoDiscovery

Select AppViz applications and flows to be created.

<input checked="" type="checkbox"/> AppViz applications	# of optimized flows		
<input checked="" type="checkbox"/> Commercial Banking	5		
	Source	Destination	Service
<input checked="" type="checkbox"/>	192.168.10.35	192.168.13.10	https
<input checked="" type="checkbox"/>	192.168.10.35	192.168.11.15	oracle
<input checked="" type="checkbox"/>	192.168.13.10	192.168.10.40	ibm-mqseries
<input checked="" type="checkbox"/>	192.168.9.16 192.168.9.220 192.168.9.227 192.168.9.250	192.168.10.35	http-alt
<input checked="" type="checkbox"/>	192.168.10.35 10.42.18.80	10.42.18.80 10.42.18.81	pdl-datastream
<input checked="" type="checkbox"/> SugarCRM	1		

Aggregate into fat flows

2 new AppViz applications will be added or updated

Back

Close Import

Applications

Search...

Advanced Search

Recent (out of 23)

- Commercial Banking
- Billing
- infrastructure
- production_accounting
- GameStop
- WebAccess - DCN1 Zone
- SugarCRM
- Help Desk_2
- Email
- Peppers Project

+ New Application

Commercial Banking

DASHBOARD | FLOWS | DIAGRAM | CHANGE REQUESTS | VULNERABILITY | RISKS | ACTIVITY LOG

Revision 3

Revision Status: Active

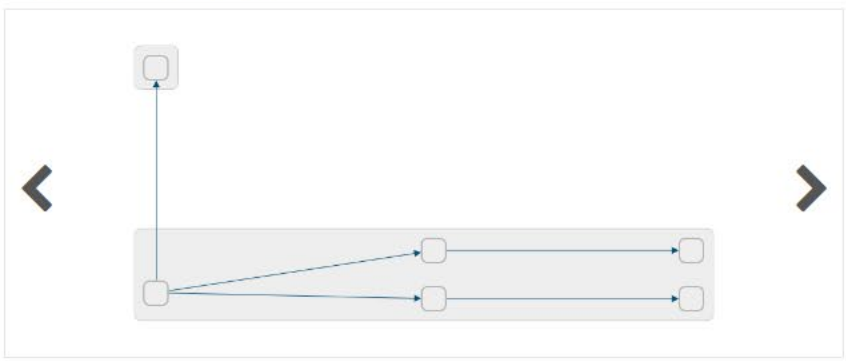
Revision Creation Date: 14/02/2020, 20:21

Number of flows: 5

Risk Score: 100%

Decommission | Export | Clone | Refresh Connectivity

Application Diagram



General Information

Created on: 12/02/2020, 08:44

Application Lifecycle: Testing

Labels

PCI

Contacts

Primary Technical Contact

Harry Jones

harry@company.com

Result:

- Discovered legitimate traffic
- Annotated the intent

USE CASE 2: ONGOING MAINTENANCE

POLICY CHANGE AUTOMATION

Billing

EXPIRES IN **24** DAYS

DASHBOARD

FLOWS

DIAGRAM

CHANGE REQUESTS

VULNERABILITY

RISKS

ACTIVITY LOG

Revision 4

Revision Status: Active

Revision Creation Date: 15/01/2018, 12:55

Number of flows: 2

Risk Score: 100%



Decommission



Export

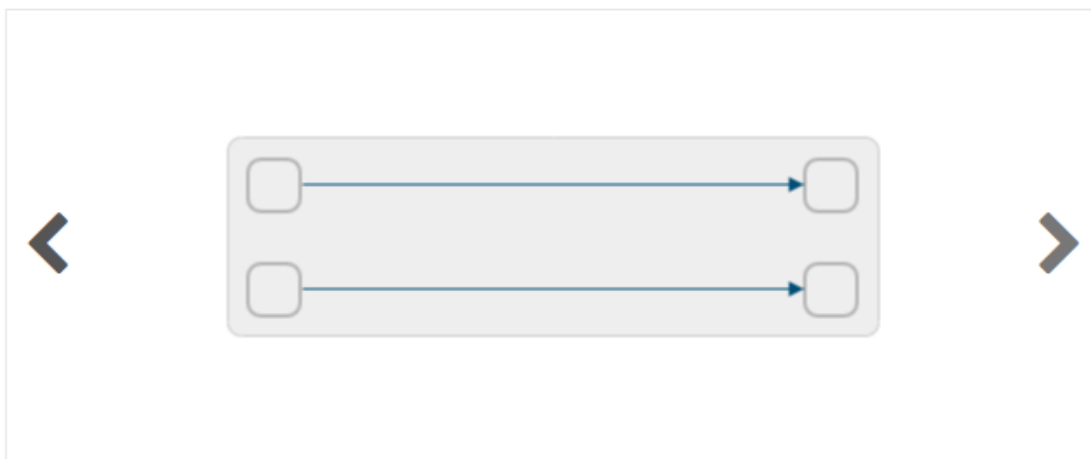


Clone



Refresh Connectivity

Application Diagram



General Information

[Edit](#)

Created on: 31/07/2017, 03:44

Expiration Date: 17/04/2020

Application Lifecycle: Testing

Business Unit: eCommerce

Labels

[Edit](#)

Finance

Third-Party

Contacts

[Edit](#)

Business Owner

Albert AppOwner
albert.appowner@company.com

Primary Technical Contact

Jane ITManager

Billing

EXPIRES IN **24** DAYS[DASHBOARD](#)**[FLOWS](#)**[DIAGRAM](#)[CHANGE REQUESTS](#)[VULNERABILITY](#)[RISKS](#)[ACTIVITY LOG](#)[Export to CSV](#)[Edit Flows](#)

Application Flows

Name	Source	User	Destination	Network Application	Service	Com
1	FP_ext	Any	FP_int	Any	http HTTP	
2	Azure_source	Any	Azure_destination	Any	ssh SSH	

Billing

EXPIRES IN **24** DAYS

DASHBOARD **FLOWS** DIAGRAM CHANGE REQUESTS VULNERABILITY RISKS ACTIVITY LOG

+ Add Flow

Subscribe to application...

Cancel

Save Changes

Application Flows ☰ Reorder application flows

Name*	Source*	User	Destination*	Network Application	Service*	Comments
	invoice-server ✕ <input type="text"/> <small>🔍 Network Object Lookup + New</small>	Any <input type="text"/> <small>🔍 User Lookup</small>	CustomerDB ✕ <input type="text"/> <small>🔍 Network Object Lookup + New</small>	Any <input type="text"/> <small>🔍 Network Application Lookup</small>	PostgreSQL ✕ <input type="text"/> <small>🔍 Service Lookup + New</small>	
1	FP_ext ✕ <input type="text"/> <small>🔍 Network Object Lookup + New</small>	Any <input type="text"/> <small>🔍 User Lookup</small>	FP_int ✕ <input type="text"/> <small>🔍 Network Object Lookup + New</small>	Any <input type="text"/> <small>🔍 Network Application Lookup</small>	http ✕ HTTP ✕ <input type="text"/> <small>🔍 Service Lookup + New</small>	
2	Azure_source ✕ <input type="text"/> <small>🔍 Network Object Lookup + New</small>	Any <input type="text"/> <small>🔍 User Lookup</small>	Azure_destination ✕ <input type="text"/> <small>🔍 Network Object Lookup + New</small>	Any <input type="text"/> <small>🔍 Network Application Lookup</small>	ssh ✕ SSH ✕ <input type="text"/> <small>🔍 Service Lookup + New</small>	

Apply Flows Changes: Billing



Change Request Summary * BusinessFlow Change Request for Billing

Show legend ▾

Changes in Flows

Will be included in the change request

<input checked="" type="checkbox"/>	Name	Source	User	Destination	Network Application	Service
<input checked="" type="checkbox"/>	3	invoice-server	Any	CustomerDB	Any	PostgreSQL
Changes details						

Cancel

Apply

2

Azure_source

Any

Azure_destination

Any

ssh

SSH

#6640 BusinessFlow Change Request for Billing



Plan

Approve

Implement

Validate

Match



● Details

● Traffic

● Business Application Information



Confirm Devices

[Edit Traffic](#)[Resolve as already works](#)

Results

Report date: Tue Mar 10 07:57:16 2020 | Change requests will be opened for 3 selected devices out of 4 | [Find out why](#)

Type to filter your results

▼ Devices that Require Changes | 3 selected devices out of 3



Policy/Device

Details



yadin_test Cisco



Barberton_Firepower

Member of a Service Graph

Blocked

Redirect with Lilium_prod1

▼ Individual devices



Lilium_prod1

In Path

Blocked



scr-3feb.W Rose_DR

In Path

Blocked

[+ Add More Devices](#)

▶ Devices that Already Work | 0 selected devices out of 1

Partially allowed

Dec 28, 2020 | 08:05:04

Export

[Resolve](#)

Requested Traffic

SOURCE	USER	DESTINATION	APPLICATION	SERVICE
10.0.0.0/24	Any	10.1.0.0/24	Any	tcp/8080

Devices in Path (5)

VIEW BY: Status

BLOCKING (1)

- Lilium_prod1

ALLOWING (4)

- Marketing_SG/Marketing_ACL
- ubuntu4michael-nag
- NSG_ssh
- Windows/VM-nag/DanaSecurityGroup

[Expected a different path?](#)

MAP | DETAILS

The diagram illustrates the network path for the requested traffic. It starts at the source (10.0.0.0/24) and passes through several Azure resources: CustomersQAResourceGroup-vnet_internetGateway, CustomersQAResourceGroup-vnet_internetGateway_Backplane, mgp/AzureBG-end.rainbowfireResourceGroup-vnet, mgp/AzureBG-end.rainbowfireResourceGroup-vnet_internetGateway_Backplane, and mgp/AzureBG-end.rainbowfireResourceGroup-vnet_internetGateway. From there, it branches into two paths: one through C007-DefaultRoute and another through virtualNetwork_internetGateway, virtualNetwork_internetGateway_Backplane, and centralus/virtualNetwork, both leading to the destination (10.1.0.0/24) via subnets. A legend on the left lists blocking and allowing rules, and a toolbar on the right provides navigation options.

#6640 BusinessFlow Change Request for Billing



Plan

Approve

Implement

Validate

Match



● Details

● Traffic

● Business Application Information



Approve

Reject

Risk Check Result

Recalculate

Risk profile: Perimeter.xml
Based on device: Barberton_Firepower
Risk Check Result is from: Tue Mar 24 16:12:18 2020.


No risks were found.


Risk profile: PCI.xml
Based on device: Rose_DR
Risk Check Result is from: Tue Mar 24 16:12:18 2020.


No risks were found.

Risk profile: Standard
Based on device: Lilium_prod1
Risk Check Result is from: Tue Mar 24 16:12:18 2020.

No risks were found.

>  Lilium_prod1 #6641
Status: approve | Owner: ned

>  Rose_DR #6642
Status: approve | Owner: ned

>  yadin_testCisco #6643 View Policy

 Lilium_prod1 #6641
Status: implement | Owner: ned

Risk Check results

Validation results



Implement On All Devices

Mark all as Implemented

Work Order Recommendations [Find out why](#)

Recalculate


 Edit

Last Updated: Tue Mar 24 2020 4:13:38 PM


After implementing this work order, you must configure the newly-created EPG(s) in the APIC to allow the required traffic

 Create Objects:

Type	Name	Value
EPG	AP-CPG-N1/ip-192.168.6.254	192.168.6.254
Filter	tcp-5432	tcp/5432

1.  Add Contract:

Device	Lilium_prod1
Contract Name	6641-1

	Consumer EPGs	Provider EPGs	Filters	Action	Description
New Contract Values	AP-CPG-N1/ip-192.168.6.254	AP-CPG-N1/CPG-non-member1 	tcp-5432	Allow	FireFlow #6640
Change Request Details	192.168.6.254/32	10.77.7.1/32	tcp/5432	Allow	

Implementation Notes

(no value)

[Edit](#)

SUMMARY

- Micro-Segmentation is KEY to tight network security
- SDN enables micro-segmentation – but it does not mean all your challenges are gone
- Discovery of intent, segment definition, and initial policy definition
- Ongoing maintenance: east-west + north-south





THANK YOU!

