



Zero Trust Segmentation: The Key to Cyber Resilience

Louis Cheung
Sr. Regional Systems Engineer

Sep 2022

ILLUMIO CONFIDENTIAL



Ransomware has moved
from a cyber-security
problem to become a
business resilience issue



Challenges ...

1

Attack Surface is expanding

Cyber resilience
is now a priority
for business
leaders!

2

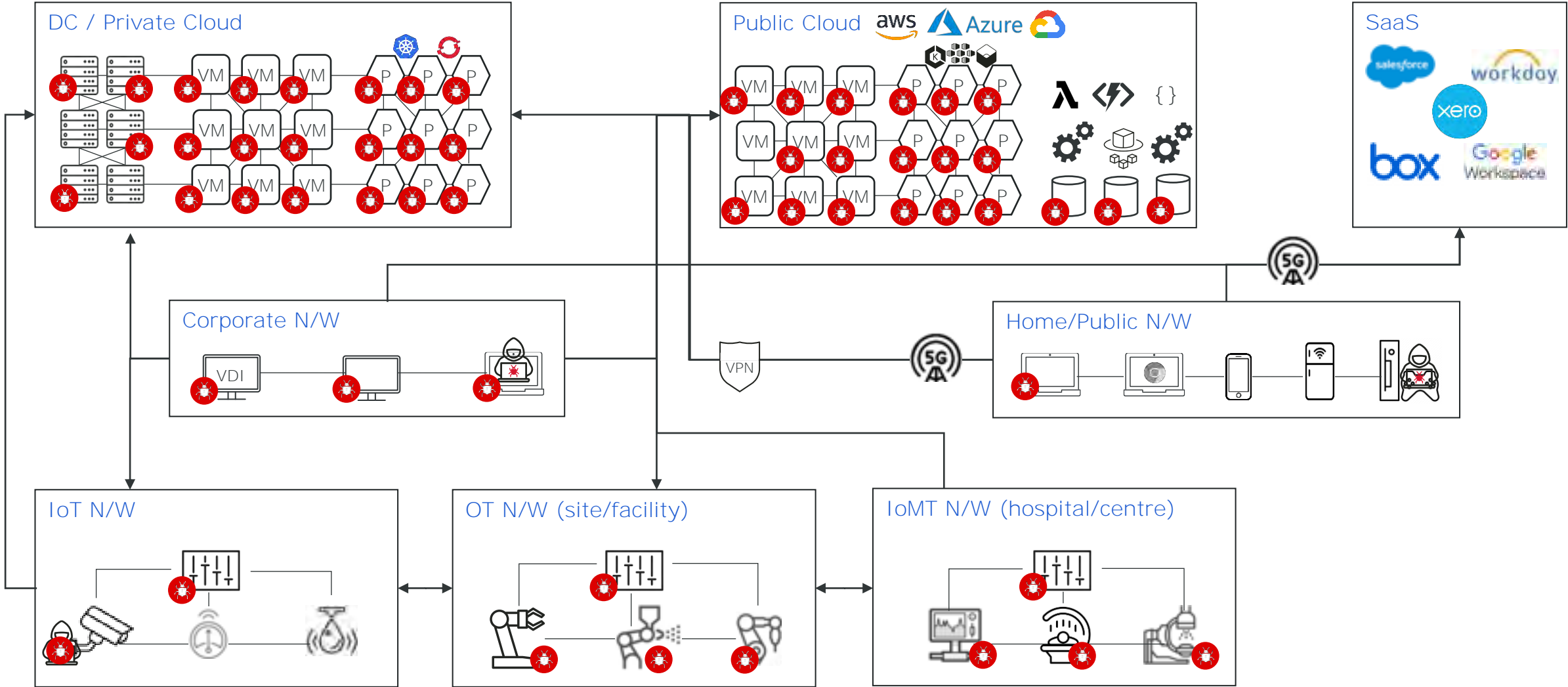
Fragmented security approach

Assume breach
mindset is
imperative!

3

Breaches are more catastrophic

Attackers use Existing Connectivity to Catastrophic Effect



The 3 Steps to Cyber Resilience

**Identify
areas of
highest
risk**

**Install
immediate
protection**

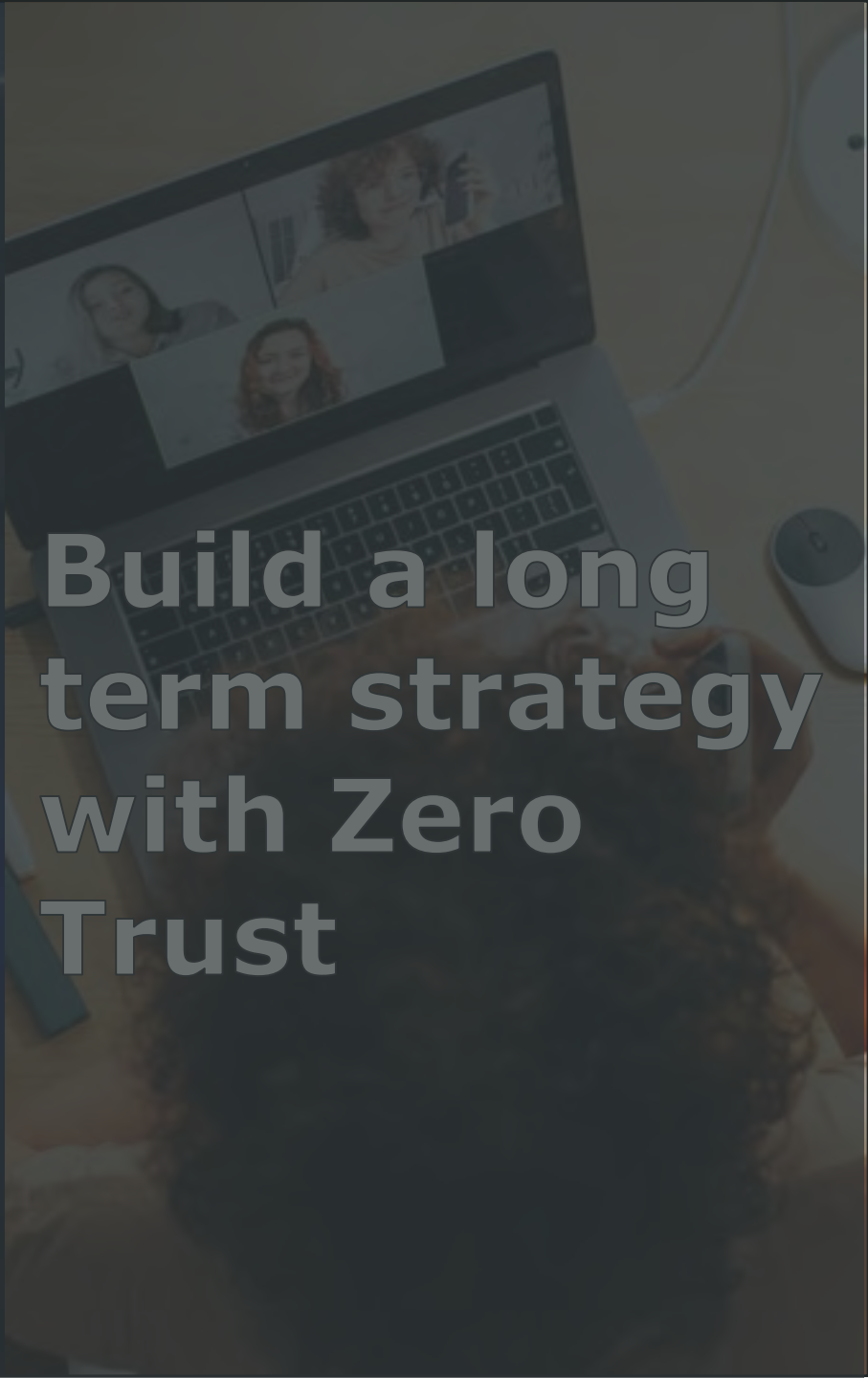
**Build a long
term strategy
with Zero
Trust**



**Identify
areas of
highest
risk**

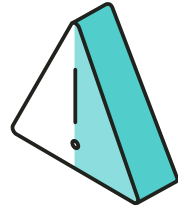


**Install
immediate
protection**



**Build a long
term strategy
with Zero
Trust**

Risk Management



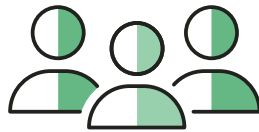
Avoid

Turn down projects or change scope



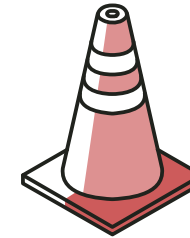
Transfer

Transfer risk to insurance



Mitigate

Put measures in place to combat threat



Accept

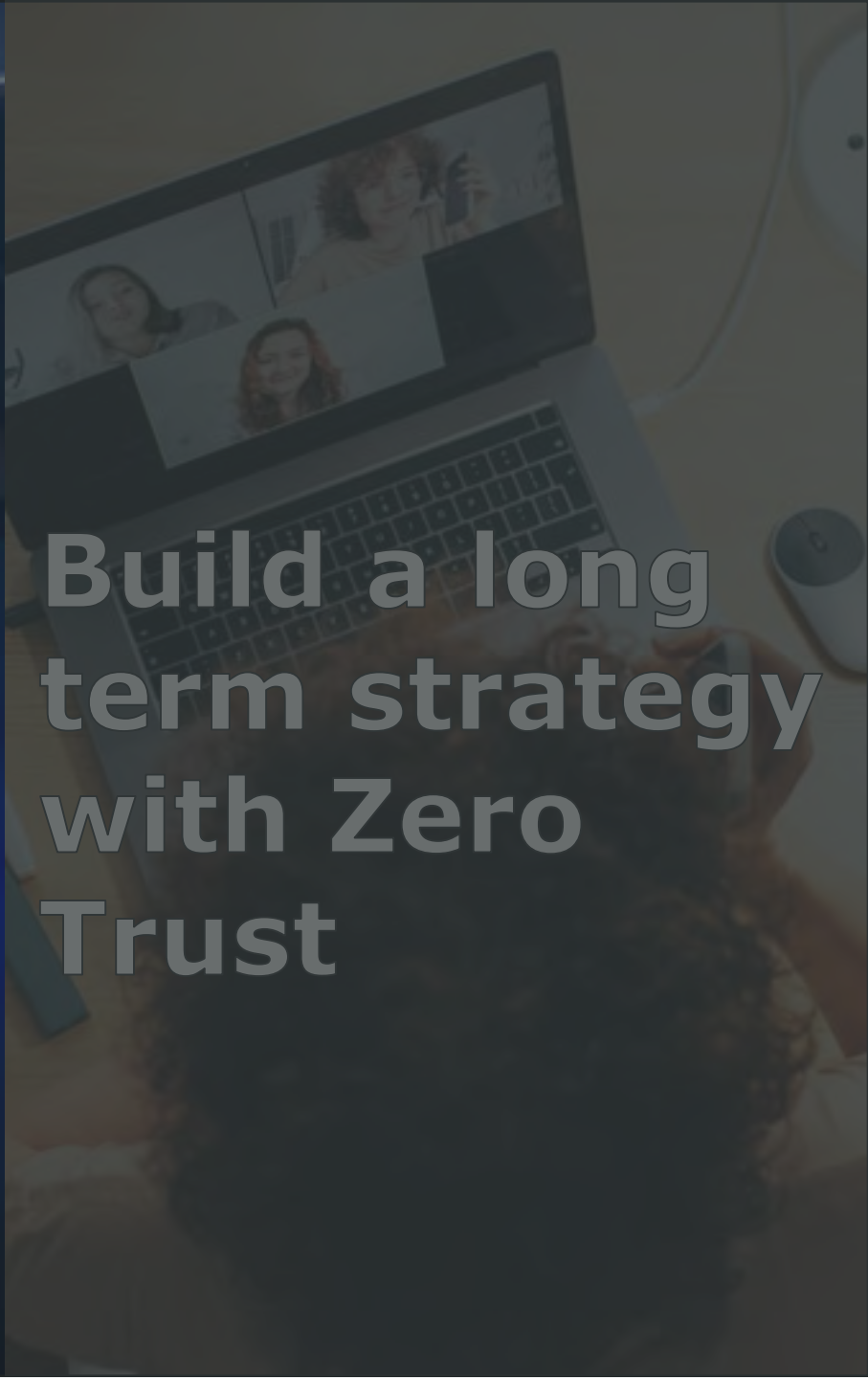
Create a contingency plan or work around



**Identify
areas of
highest
risk**




**Install
immediate
protection**



**Build a long
term strategy
with Zero
Trust**

How Ransomware Moves

- Ransomware can only move using existing transport systems
- It stows away on legitimate communication used in legal activities
- These transport systems are not used everywhere by every system
- Blocking these pathways leads to immediate protection from common ransomware families



RDP =
Ransomware
Distribution
Protocol



**Identify
areas of
highest
risk**



**Install
immediate
protection**



**Build a long
term strategy
with Zero
Trust**

Security Strategy shift

From trying to:

identify what is bad and stopping it

to ...

identifying what is good and
allowing it



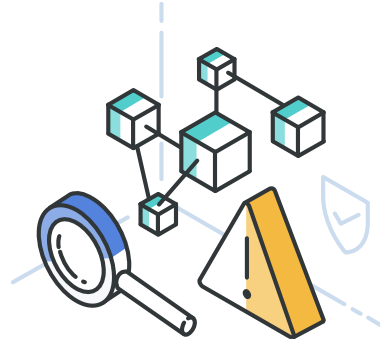
Zero Trust Taxonomy

Zero Trust Network Access



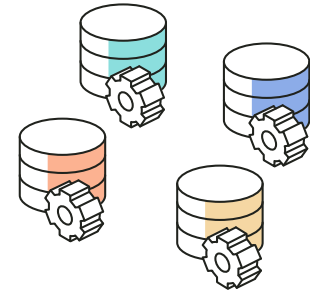
Next generation perimeter,
restricting access to
verified users

Zero Trust Segmentation



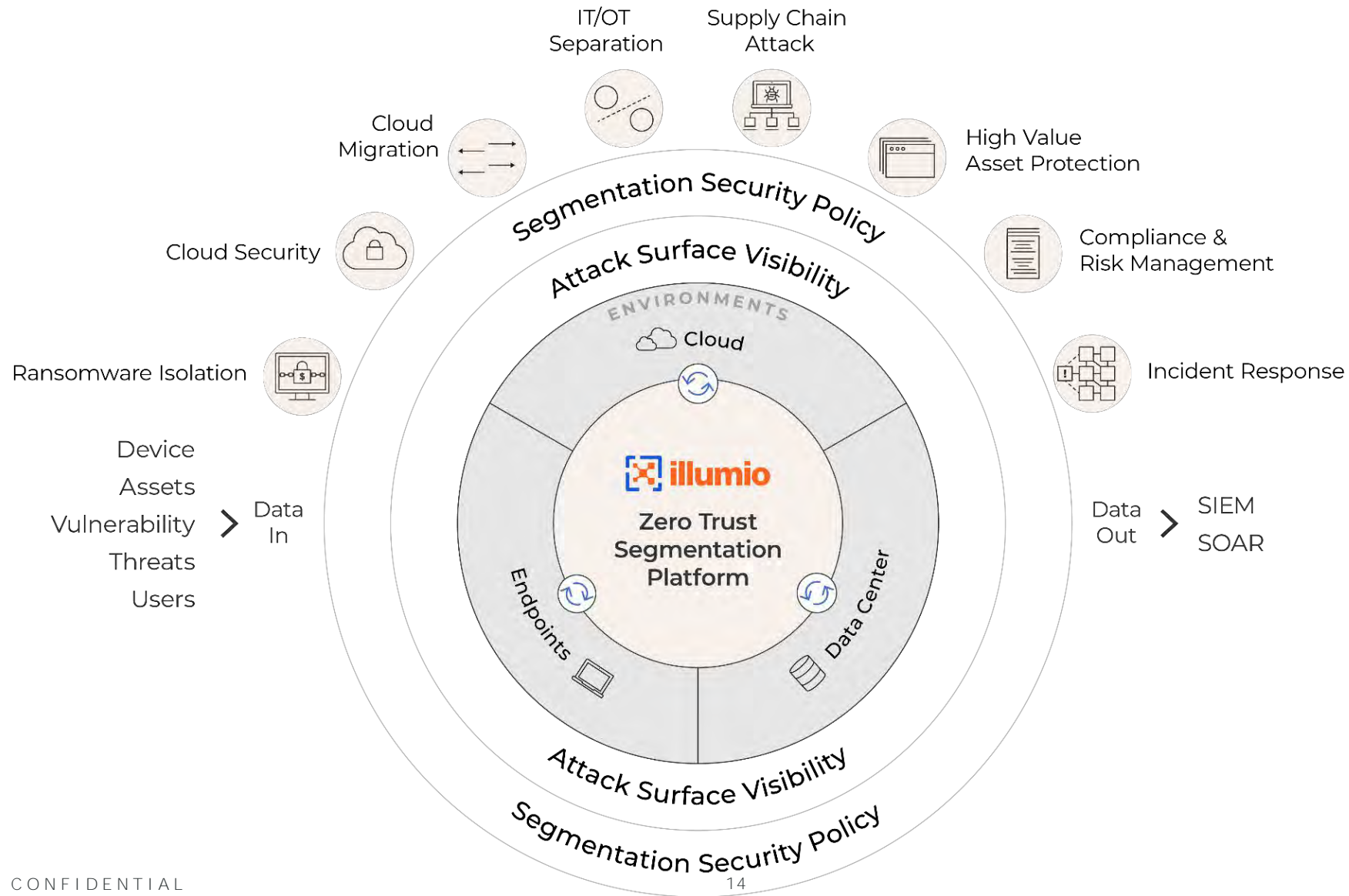
Control communication
between verified systems
and assets

Zero Trust Data Security



Provide reliable restoration
of data

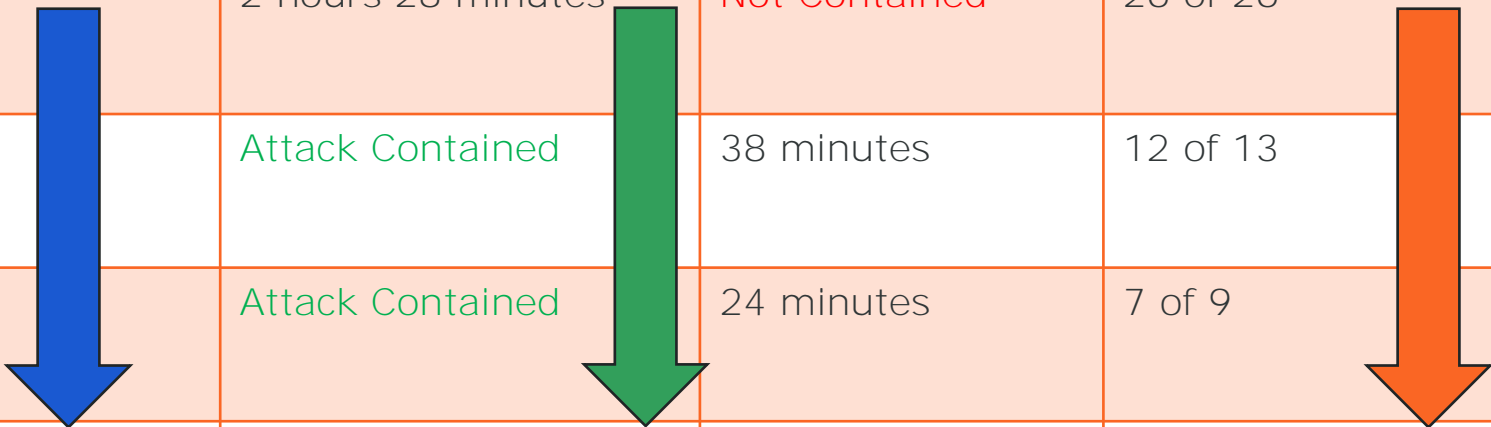
Illumio Zero Trust Segmentation Platform



Zero Trust Segmentation – It delivers actual results

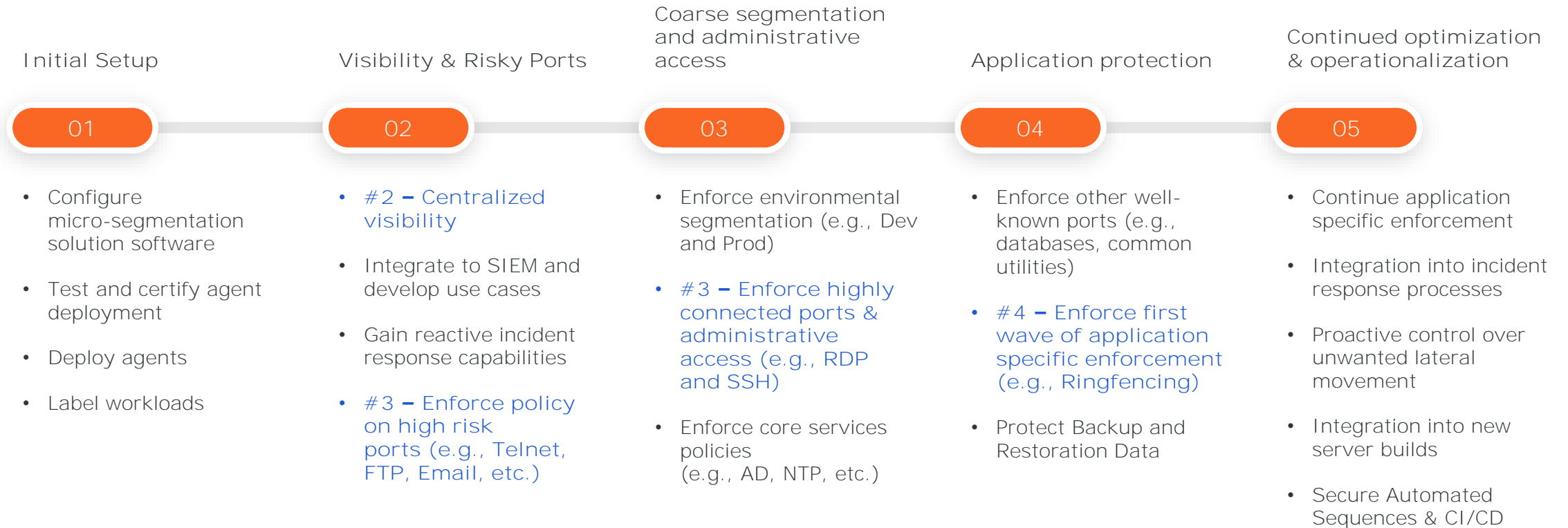
Ransomware Scenario Emulation

Scenario	Compromised Hosts	Time to Complete Attack	Time to Containment of Attack	Successful TTPs
Scenario 1: Control test – Illumio not deployed	16 of 16	2 hours 28 minutes	Not Contained	26 of 26
Scenario 2: Detection and response	2 of 16	Attack Contained	38 minutes	12 of 13
Scenario 3: Pre-configured static protection	2 of 16	Attack Contained	24 minutes	7 of 9
Scenario 4: Full application ring fencing	1 of 16	Attack Contained	10 minutes	6 of 8



- **Time to Complete:** The time it took for the **attacker to meet their goal of compromising all the test environment** OR the time it took for the **defender to completely stop the attack**.
- **Successful TTPs:** The number of TTPs that were successfully executed (not blocked by security solutions) out of the total number of TTPs that the attacker tried to run before the attack was blocked, or the attacker goals were achieved.

Mapping the scenarios to the ZTS customer journey



\$20M/year in app
downtime savings

5 cyber disasters
averted per year

14 digital/cloud
projects accelerated per
year

68% faster MTTR

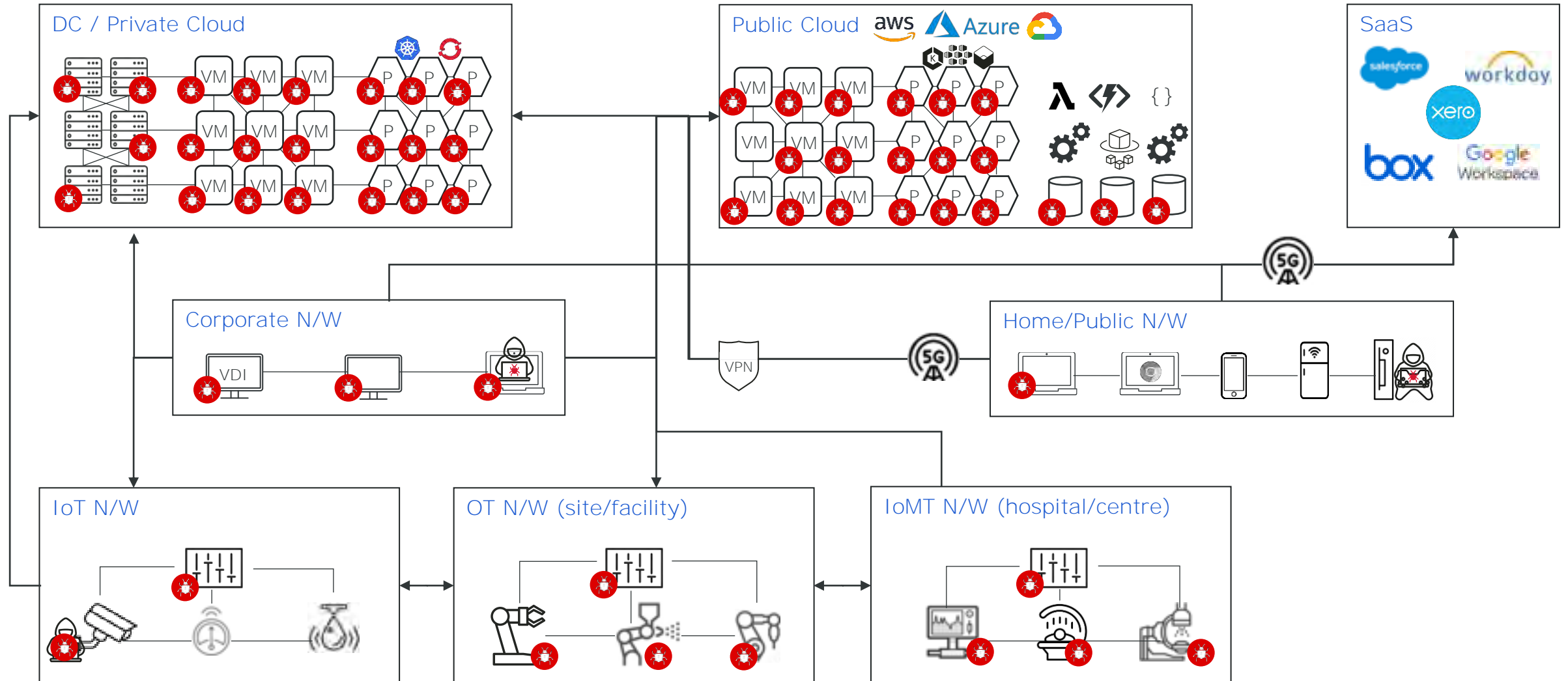


© 2022 Illumio

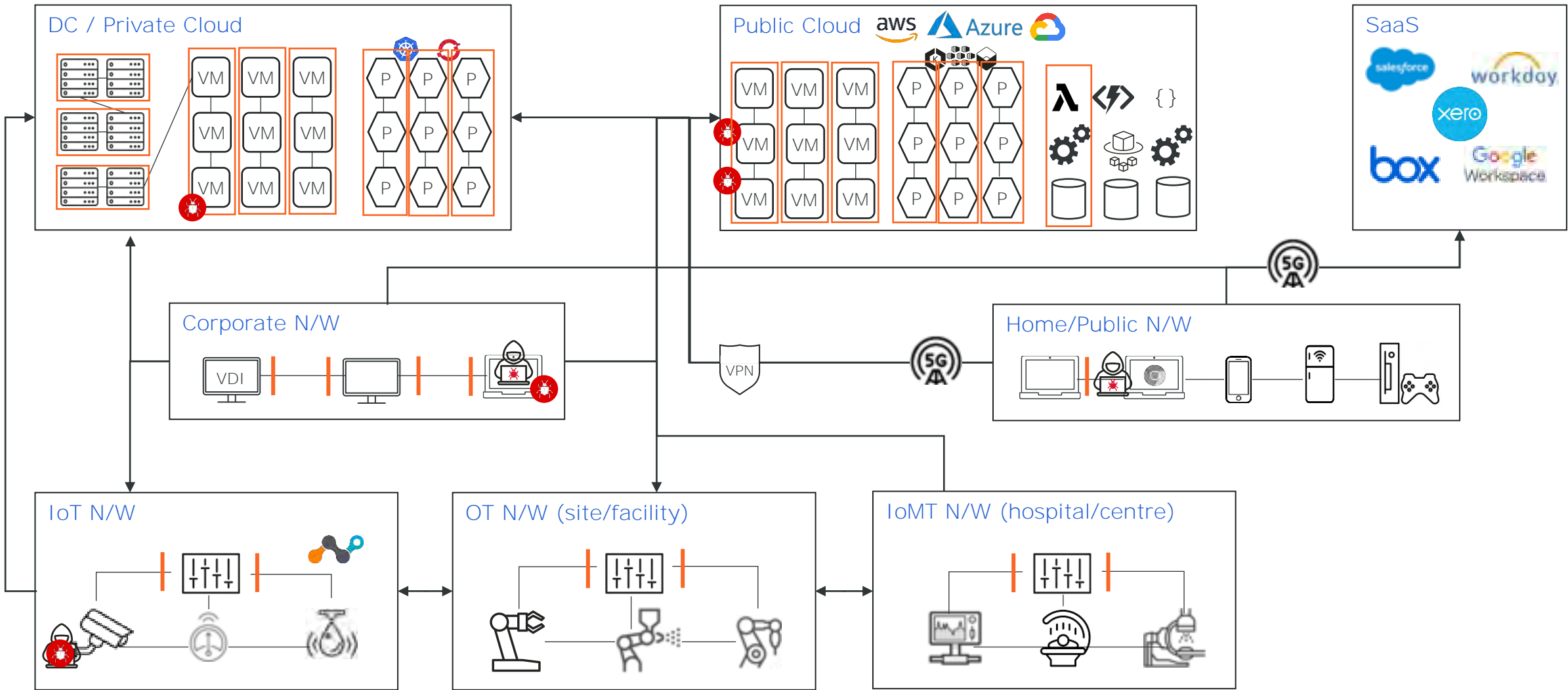


© 2022 TechTarget, Inc. All Rights Reserved.

Helping you go from this



To this



We're at Exhibitor Booth 09

Email:

Louis.Cheung@illumio.com

Register our 90 mins

Online Workshop -

Ransomware Containment





Thank you