

Zero Trust Segmentation: The Key to Cyber Resilience

Louis Cheung Sr. Regional Systems Engineer

Sep 2022





Challenges

Attack Surface is expanding

2

Fragmented security approach

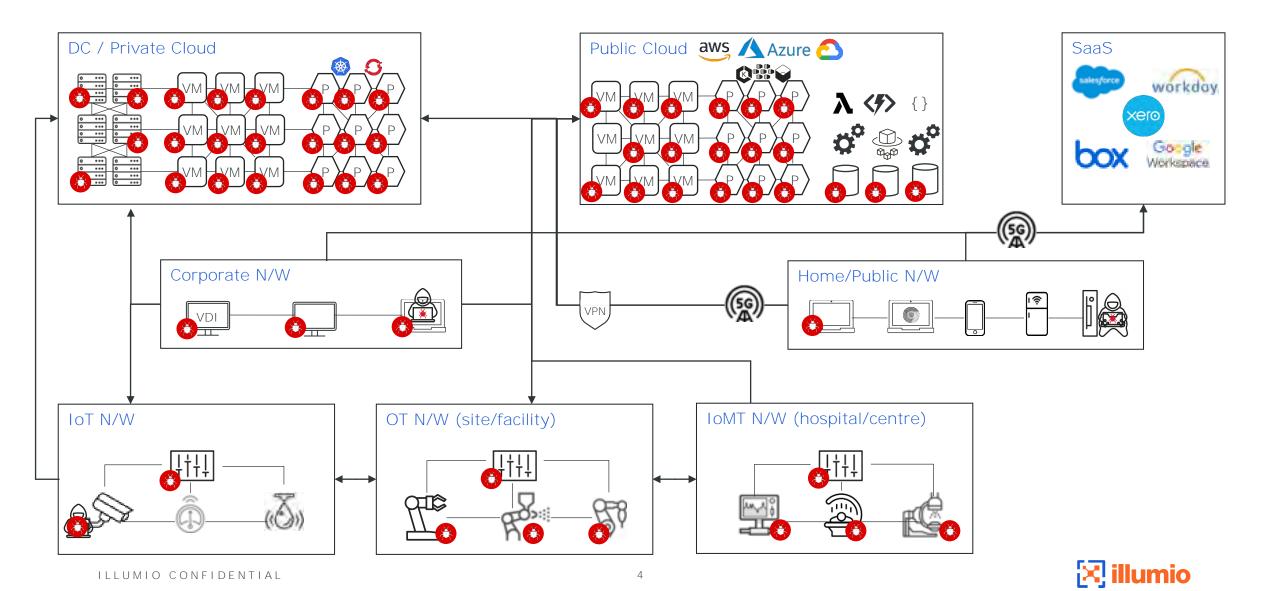
Cyber resilience is now a priority for business leaders!

Assume breach mindset is imperative

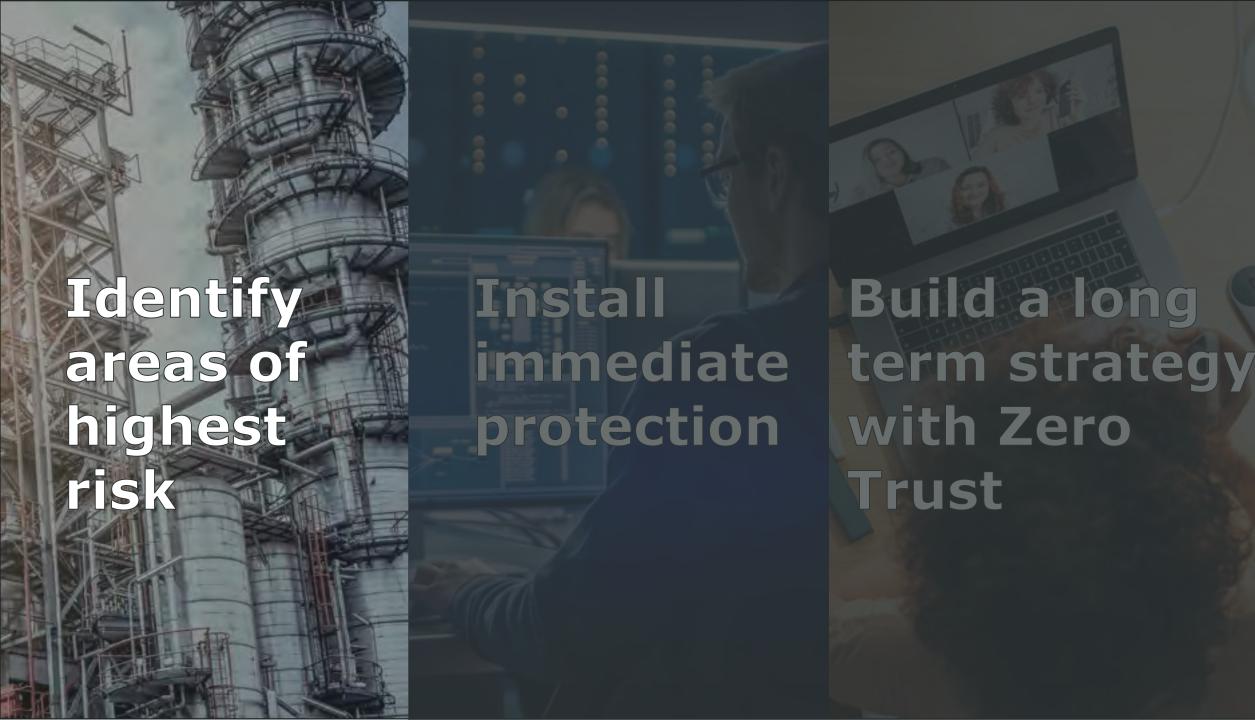
3 Breaches are more catastrophic



Attackers use Existing Connectivity to Catastrophic Effect







Risk Management



Avoid

Turn down projects or change scope



Transfer

Transfer risk to insurance



Mitigate

Put measures in place to combat threat



Accept

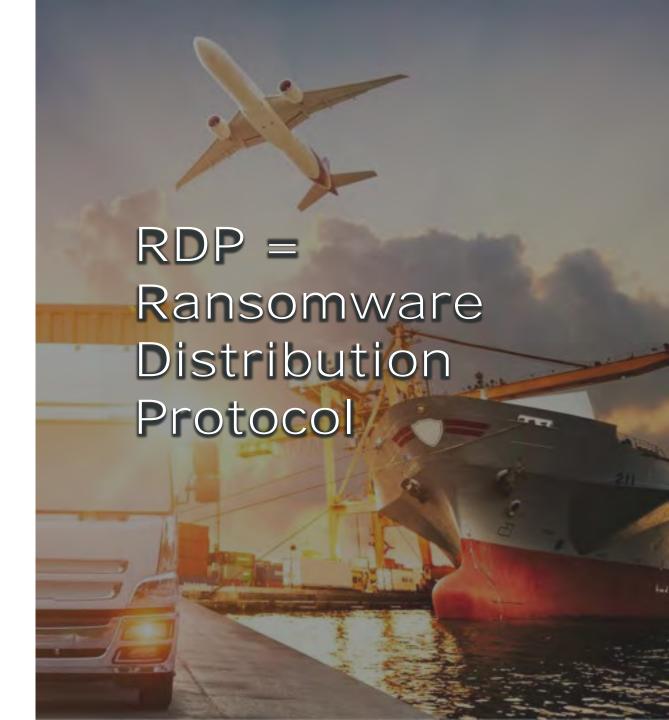
Create a contingency plan or work around

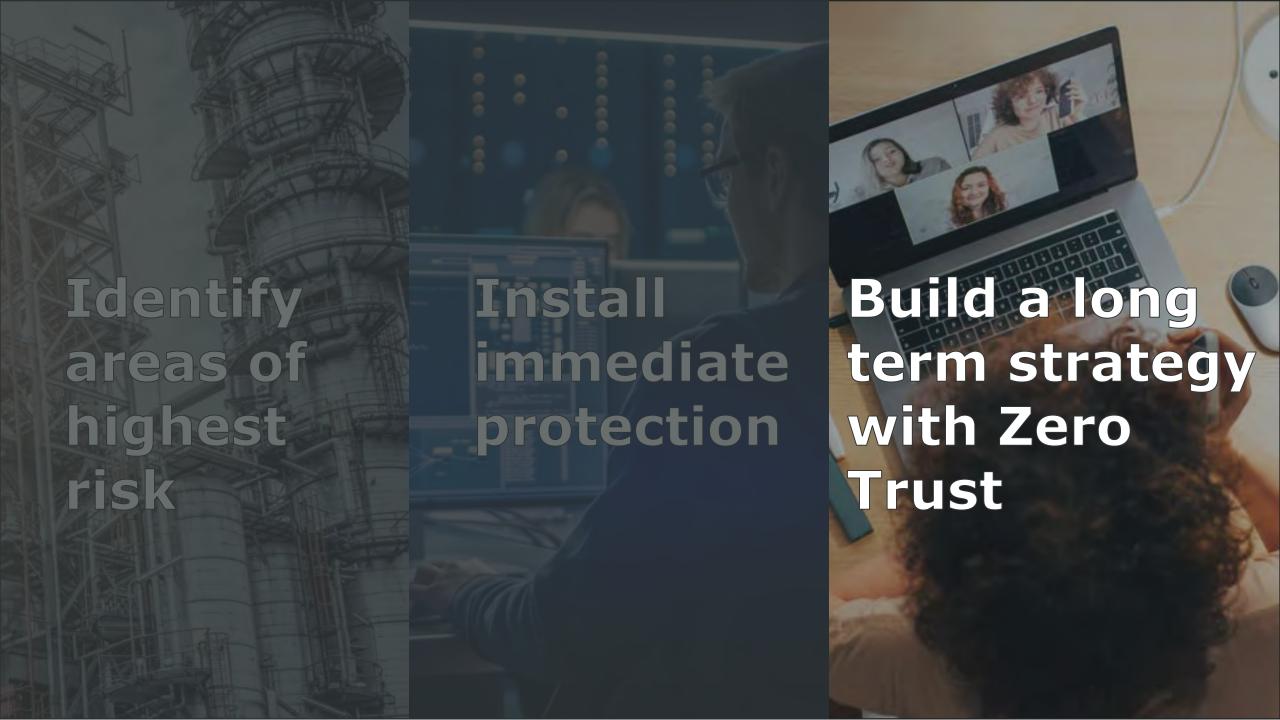




How Ransomware Moves

- 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





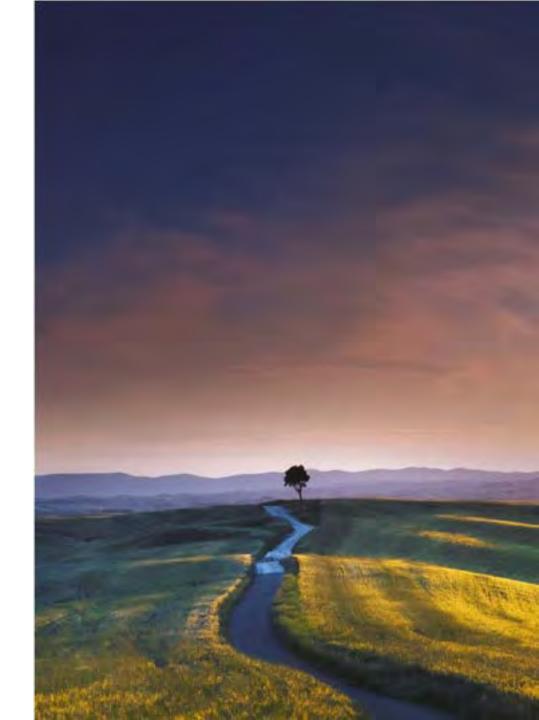
Security Strategy shift

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



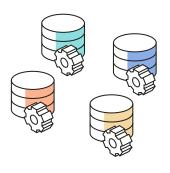
Next generation perimeter, restricting access to verified users

Zero Trust Segmentation



Control communication between verified systems and assets

Zero Trust Data Security



Provide reliable restoration of data



What is Zero Trust Segmentation?

Zero Trust is an information security module that denies access to applications and data by default. Zero Trust advocates these three core principles:

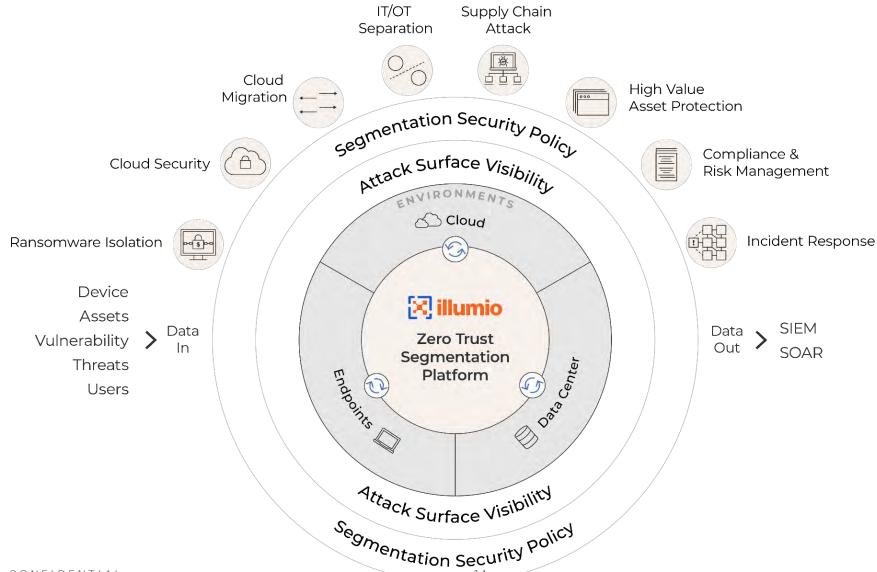
- All entities are untrusted by default;
- Least privilege access is enforced
- Continuous and adaptive



Zero Trust Segmentation is the application of these 3 core principles to secure connectivity between resources



Illumio Zero Trust Segmentation Platform





Zero Trust Segmentation - It delivers actual results

Ransomware Scenario Fmulation

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

Initial Setup

01

- Configure micro-segmentation solution software
- Test and certify agent deployment
- Deploy agents
- Label workloads

Visibility & Risky Ports

Coarse segmentation and administrative access

03

- #2 Centralized visibility
- Integrate to SIEM and develop use cases
- Gain reactive incident response capabilities
- #3 Enforce policy on high risk ports (e.g., Telnet, FTP, Email, etc.)

- Enforce environmental segmentation (e.g., Dev and Prod)
- #3 Enforce highly connected ports & administrative access (e.g., RDP and SSH)
- Enforce core services policies (e.g., AD, NTP, etc.)

Application protection

04

- Enforce other wellknown ports (e.g., databases, common utilities)
- #4 Enforce first wave of application specific enforcement (e.g., Ringfencing)
- Protect Backup and Restoration Data

Continued optimization & operationalization

05

- Continue application specific enforcement
- Integration into incident response processes
- Proactive control over unwanted lateral movement
- Integration into new server builds
- Secure Automated Sequences & CI/CD



\$20M/year in app downtime savings

5 cyber disasters averted per year

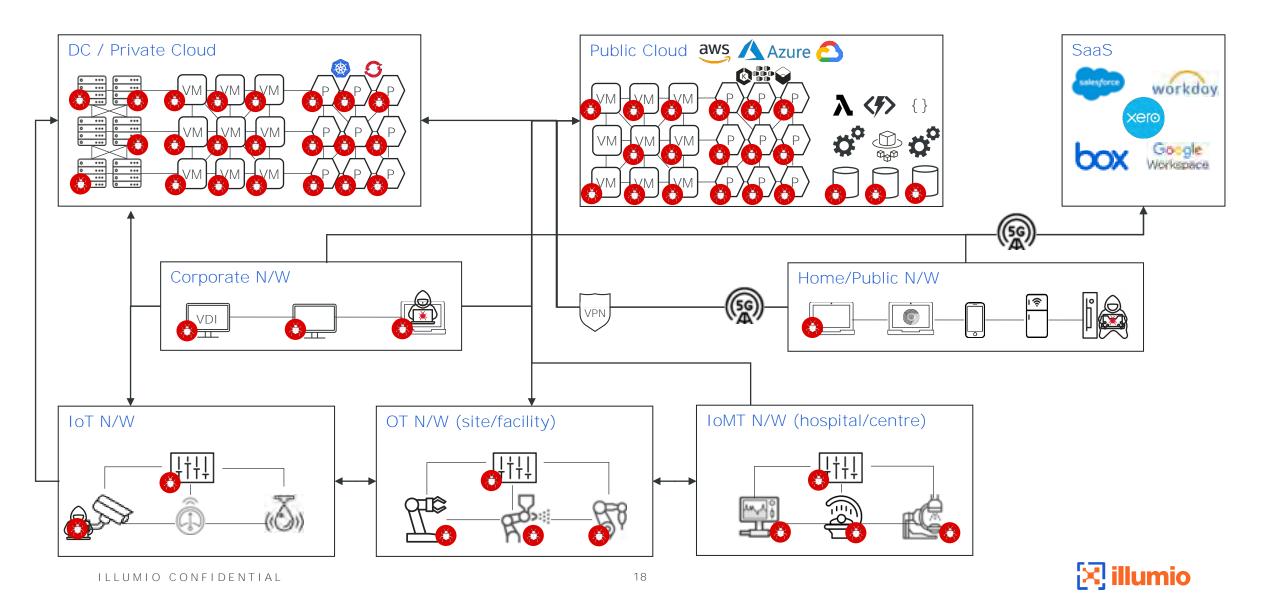
14 digital/cloud projects accelerated per year

68% faster MTTR

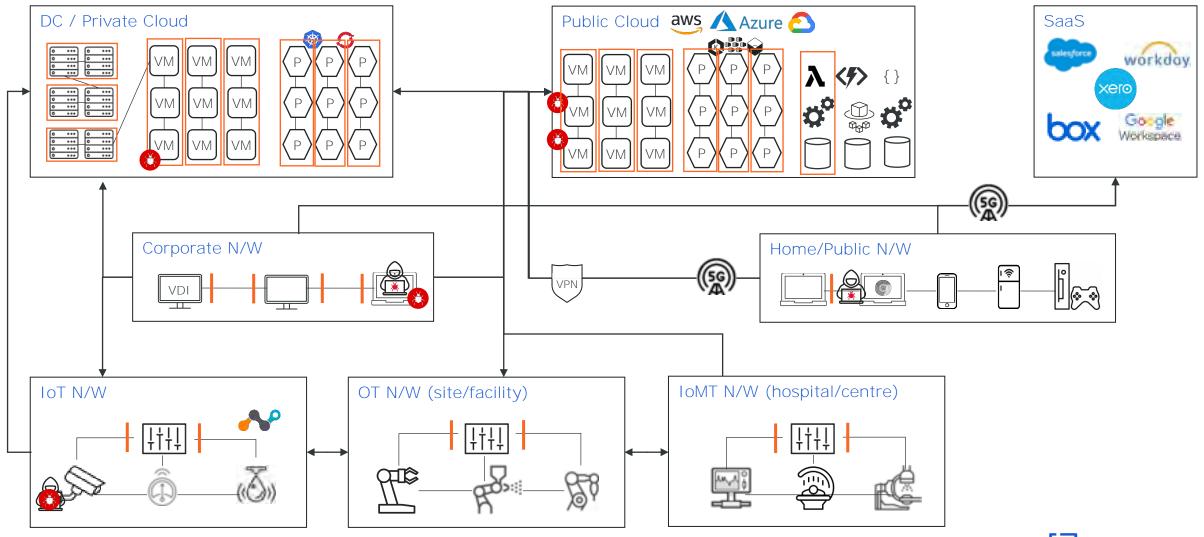




Helping you go from this



To this



We're at Exhibitor Booth 09

Email:

Louis.Cheung@illumio.com

Register our 90 mins
Online Workshop Ransomware Containment





Thank you

