



# The Leader in OT & IoT Security

[nozominetworks.com](http://nozominetworks.com)

[alexei.pinal@nozominetworks.com](mailto:alexei.pinal@nozominetworks.com)

[mdepina@kc-latam.com](mailto:mdepina@kc-latam.com)

# Market Forces Driving Change



## Digital Transformation

- New technologies, new use cases in every industry



## IT/OT Convergence

- Integrated teams and workflows need a single view



## Internet of Everything

- Juniper Research: 83 billion IoT connections by 2024; 70% in Industrial sector



## Threat & Risk Management

- Frequency and cost of targeted attacks continue to increase

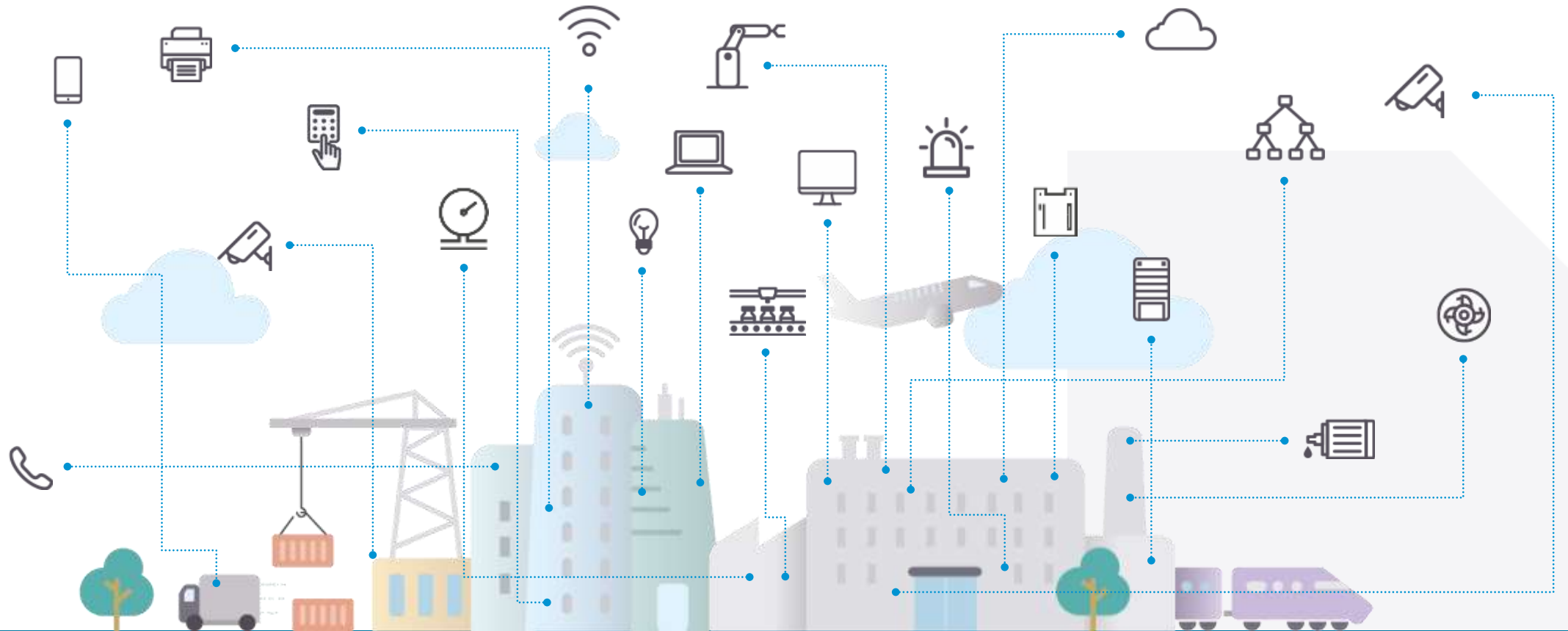


**5G is accelerating digital transformation across all sectors – everyone is connected to everything, and new use cases are speeding OT, IoT and IT convergence.**

Andrea Carcano, Co-founder and CPO,  
Nozomi Networks

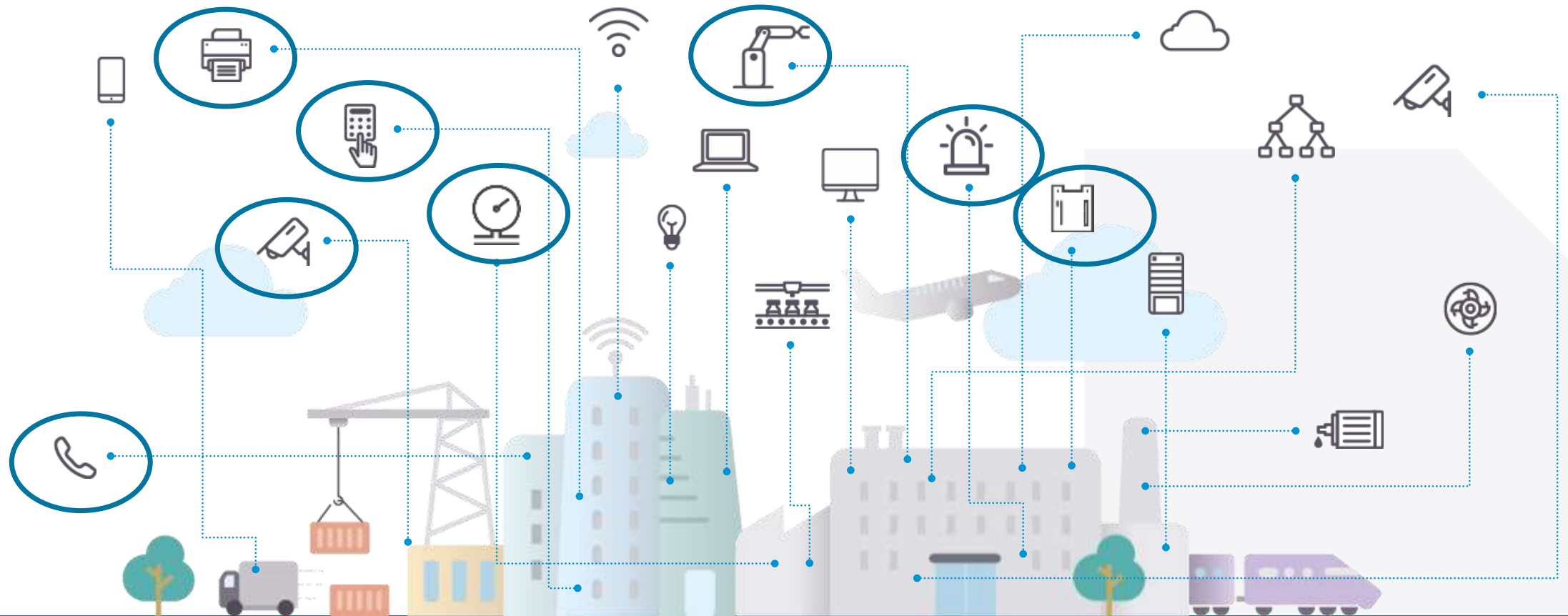
# Security and Visibility for Any Device, Anywhere

Accelerating digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats.

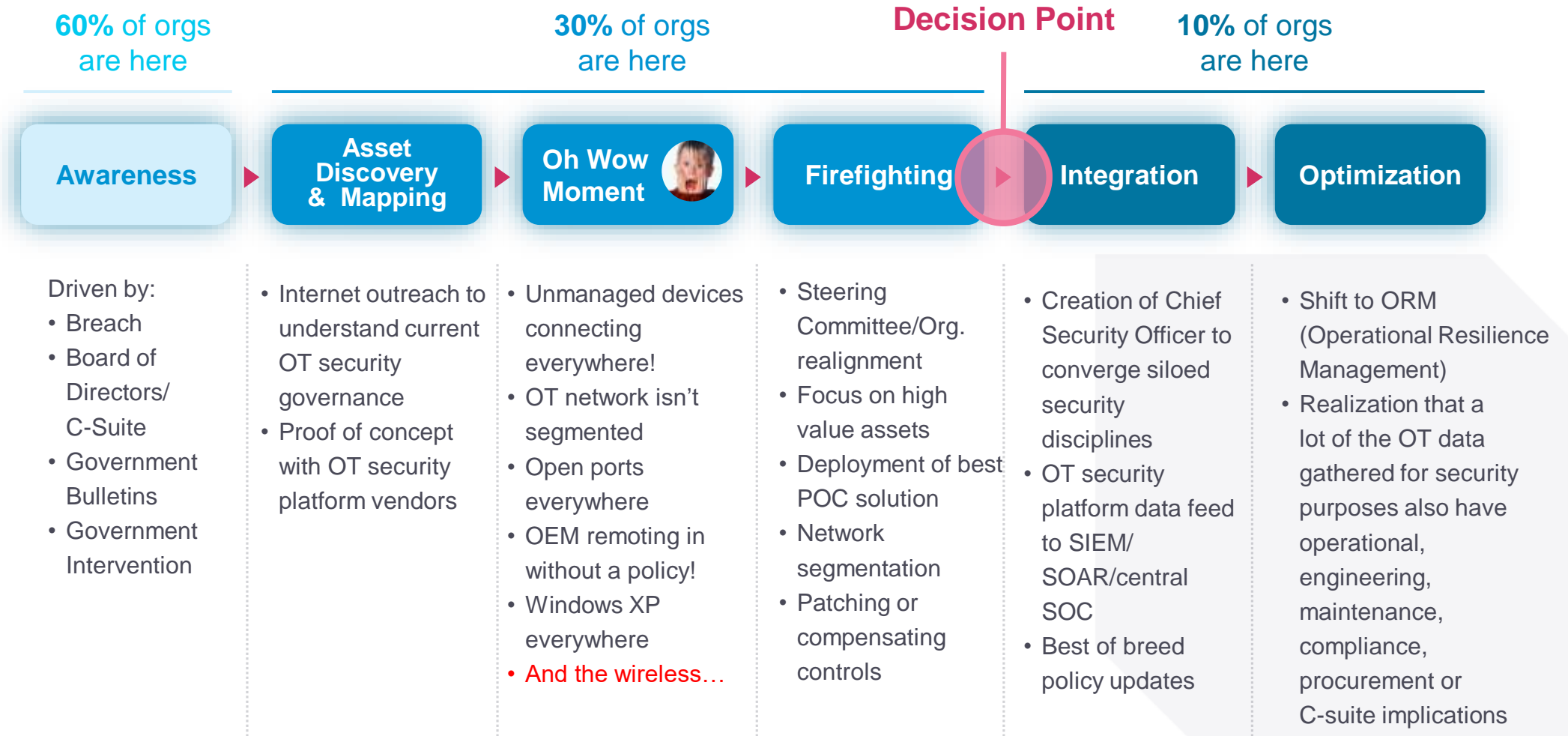


# Security and Visibility for Any Device, Anywhere

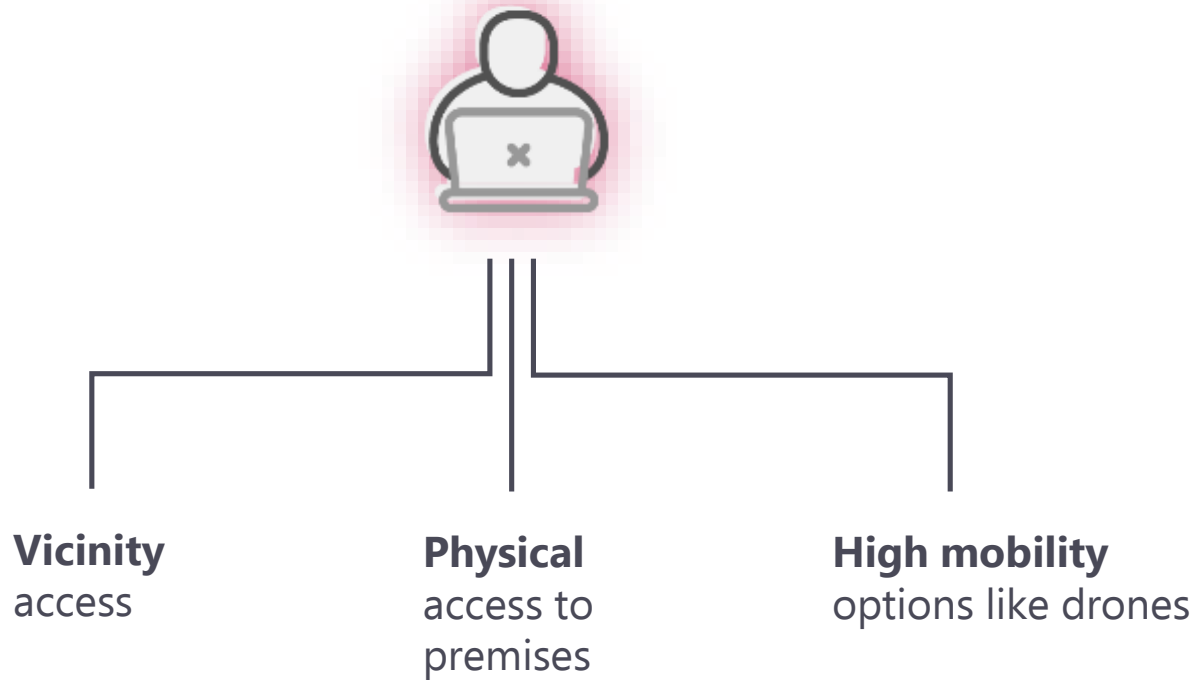
Accelerating digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats.



# The OT/IoT Security Journey



# Wireless Attacker options



It is often **hard to detect** malicious individuals and their equipment.

1. Vicinity Access:
2. Antenna-for-Hire.
3. Segmentation Hopping
4. Device Hijacking
5. Jamming (Denial of Service)
6. Unauthorized Network Access:
7. Rogue Access Points:
8. Evil Twin Attacks.
9. FragAttacks (Frame Aggregation Attacks
10. Wi-Fi Phishing:
11. SSID Squatting
12. AWDL (Apple Wireless Direct Link) Attacks.
13. Bluetooth Attacks
14. Cellular Network Attacks
15. LoRaWAN Attacks:.
16. Signal Jamming:
17. Sniffing and Eavesdropping
18. Replay Attacks
19. Brute Force Attacks

# Use Case

## Remote locations



### Problem

A natural gas company utilizes LoraWAN and cellular technologies in remote locations where gasoline flow is measured in pipes. Recent criminal attack attempts on utilities companies have turned the alarms and further security measures are required.



### Attacks

**Spoofing:** Act as a tower or a fake device, force people to connect to you. Send fake information.

Rogue Cell Towers, AKA Stingrays or IMSI Catchers, are used to hijack cellphone connections, allowing attackers to listen to calls and read texts. An attacker can even push malware to a vulnerable phone to hack it. It is a Man in the Middle Attack. (serving cell changes drastically the RSSI)

### LoraWan

Invalid Frame Counter → Frame counter received is less than the one previously already received  
Invalid Frame payload length → Length of the payload (the "data" field) doesn't correspond to the one declared in the rxpk packet

# Use Case

## Remote locations



### Problem

A natural gas company utilizes LoraWAN and cellular technologies in remote locations where gasoline flow is measured in pipes. Recent criminal attack attempts on utilities companies have turned the alarms and further security measures are required.



### Solution

Implement a solution to detect the appearance of rogue infrastructures like cell phone towers or LoraWAN spoofing devices, generate alarms to trigger immediate actions.






[www.nozominetworks.com](http://www.nozominetworks.com)


- 
- [mdepina@kc-latam.com](mailto:mdepina@kc-latam.com)


# Thank You!


Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.


# Asset Discovery & Monitoring

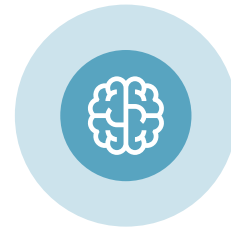
	Vendor	Rockwell Eng
	IP	192.168.0.10
	OS	Windows 7 / 2008 R2
	Patch Vuln	?

	Vendor	Honeywell
	IP	192.168.0.251
	Firmware	16.020
	Module #	0123

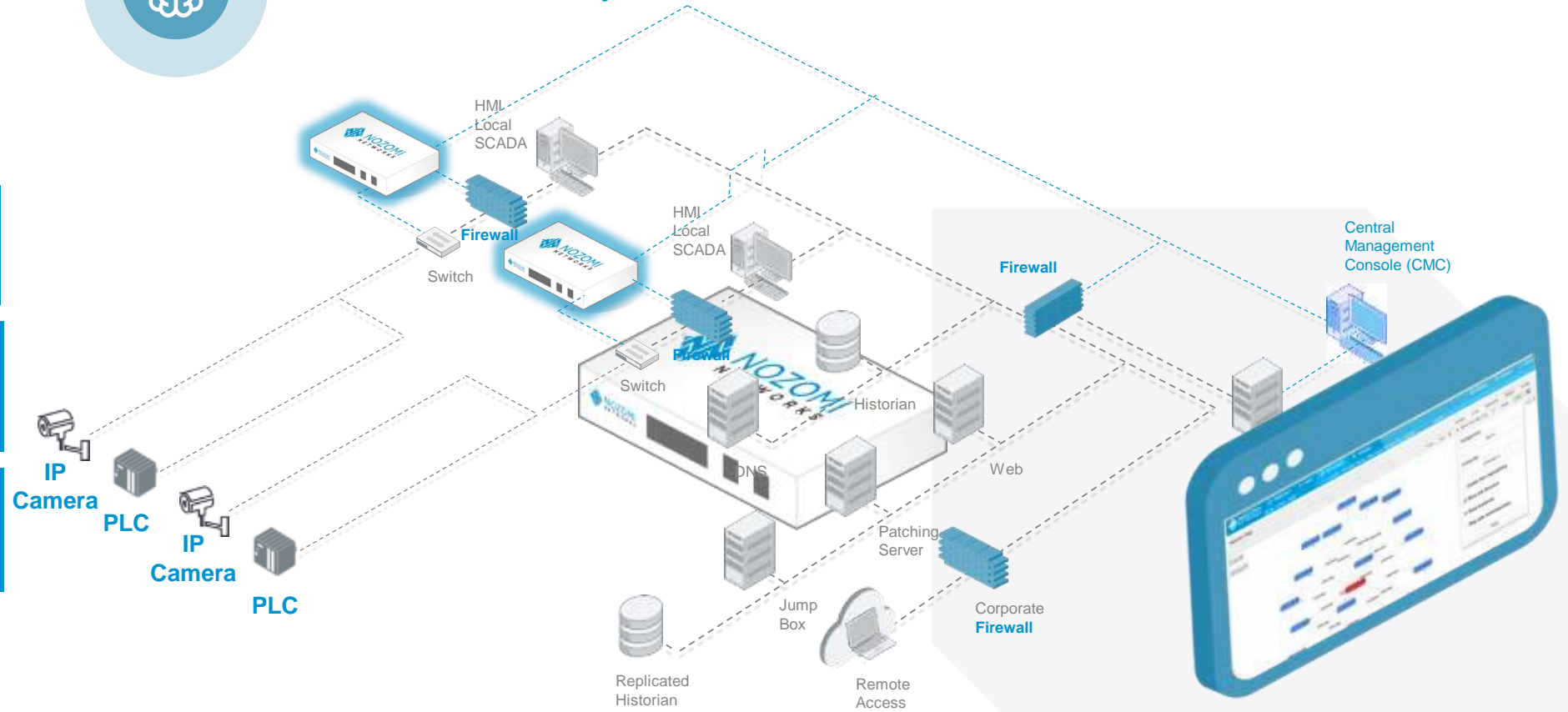
	Vendor	AXIS
	IP	192.168.0.144
	Firmware	6.50.2.3
	Model #	AXIS Q1615-E

	Vendor	Rockwell
	IP	192.168.1.80
	Firmware	?
	Module #	?

	Vendor	AXIS
	IP	192.168.50.128
	Firmware	8.20.1
	Model #	Q1615-E Mk II



AI-Enabled  
Passive Auto-Discovery



# Threat and Anomaly Detection for OT/IoT

## 1) Monitor

Guardian detects **anomalous behavior or threats** and generates an alert.

## 2) Detect

User-defined policies are rapidly examined and the appropriate corresponding action is triggered.

## 3) Respond

Integration with firewalls, NACs and EDRs enables rapid response (Node Blocking, Link Blocking, or Kill Session) and mitigates the issue.



**Dynamic Learning & Adaptive Learning Accelerates Network Learning and Anomaly Detection**

