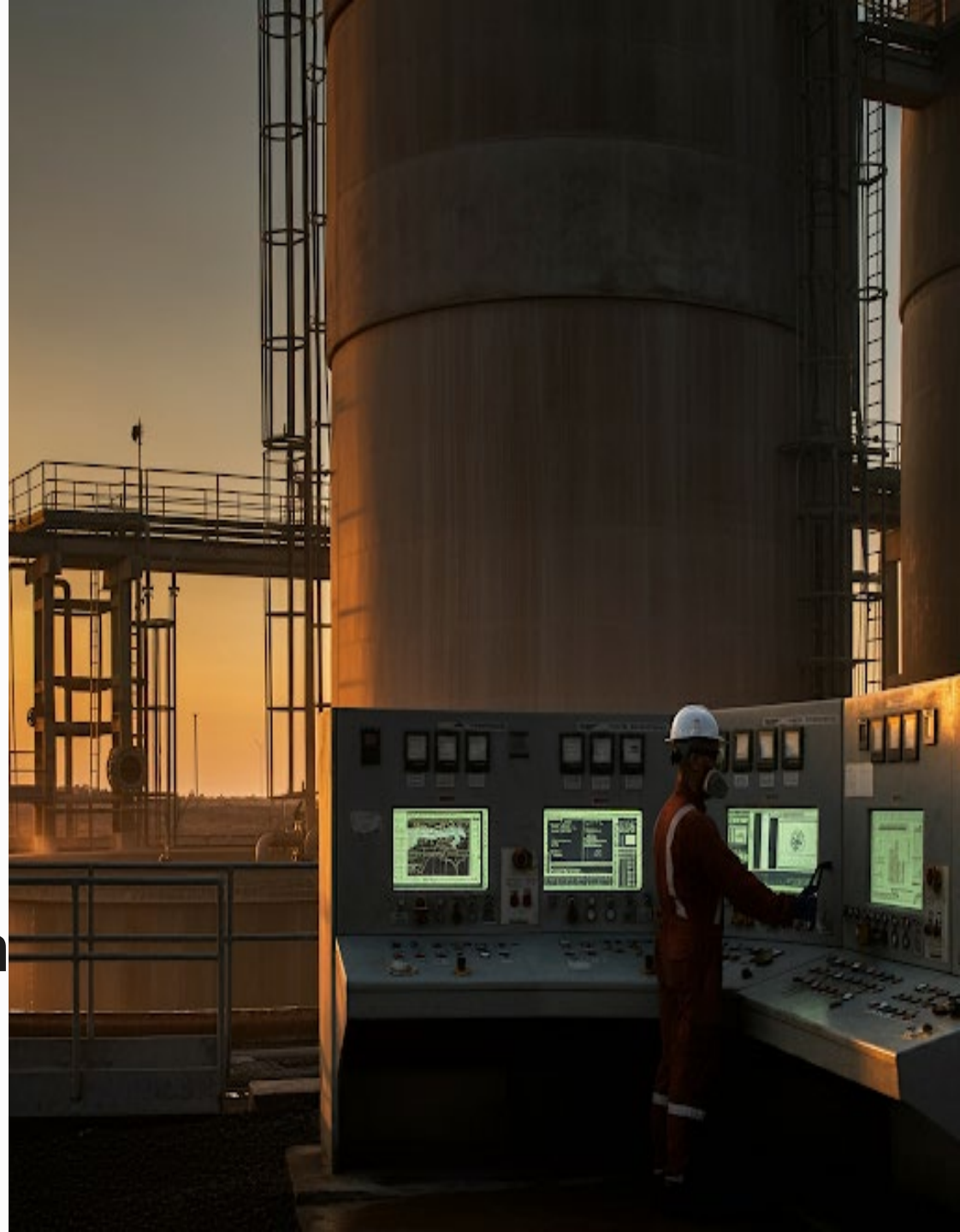
AGILICUS

Don Bowman

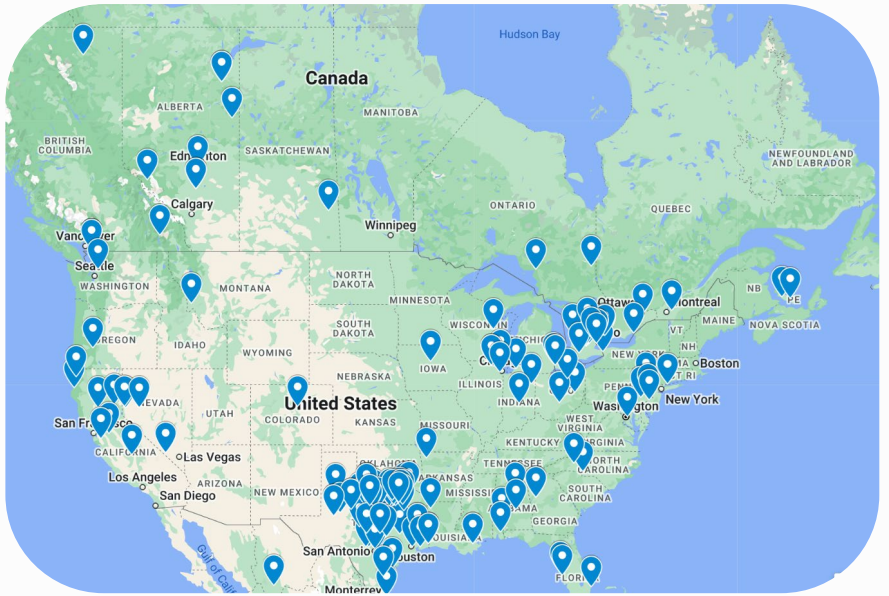
Securely but Simply enabling Remote Operations with Zero Trust

Agenda

- Introduction
  - Problem / Opportunity
  - Evolution, Current State
  - Risks
- Zero Trust Architecture
  - Concept
  - End User View
  - Benefits
- Case Study: Practical Implementation
- Conclusion, Q&A



My Perspective



Agilicus, Waterloo ON Cyber Security focusing on Industrial Control Systems (HMI, PLC, HIstorian, RTU, ..) in Wastewater

Simple, SaaS, **Zero Trust** best practices

1. Unified Authentication: all users in the ecosystem
2. Precise Authorisation: operator owns the rules
3. Seamless Access: modernise safely the air gap

Problem/Opportunity

Industrial technology has a long life

But it is evolving to become more IT-like

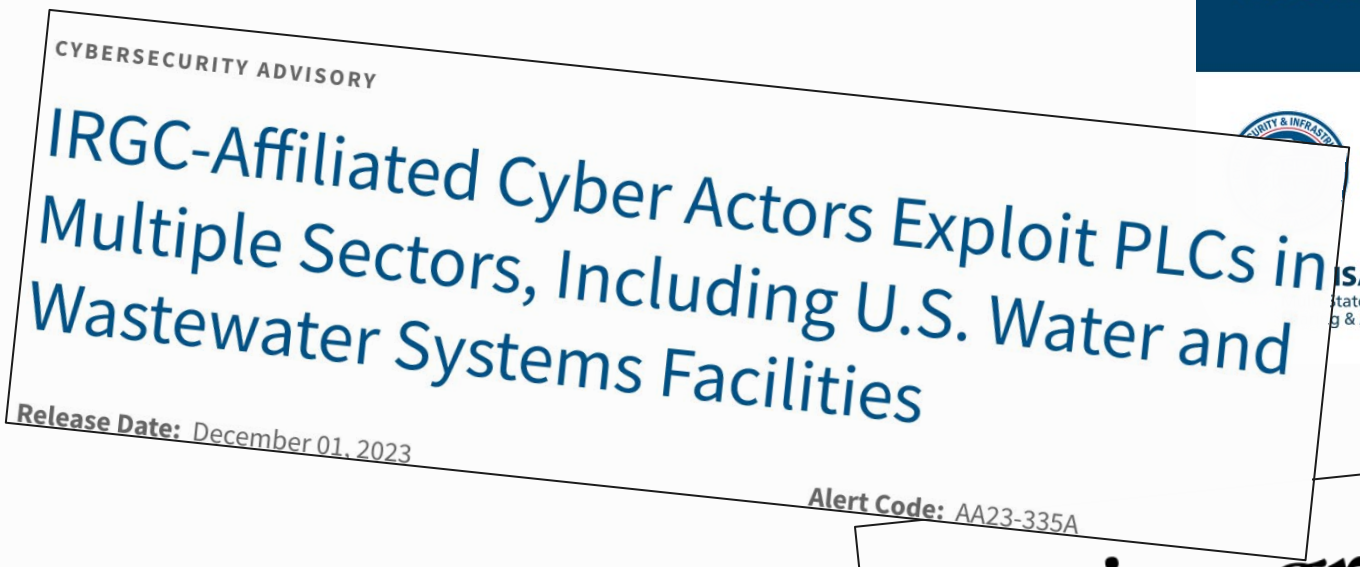
Thus skillsets specialise

Efficiency, predictive maintenance, MTTR…

Ecosystem of vendors, integrators, operators

Enable secure remote is non-zero-sum

But…



AGILICUS

The Needs

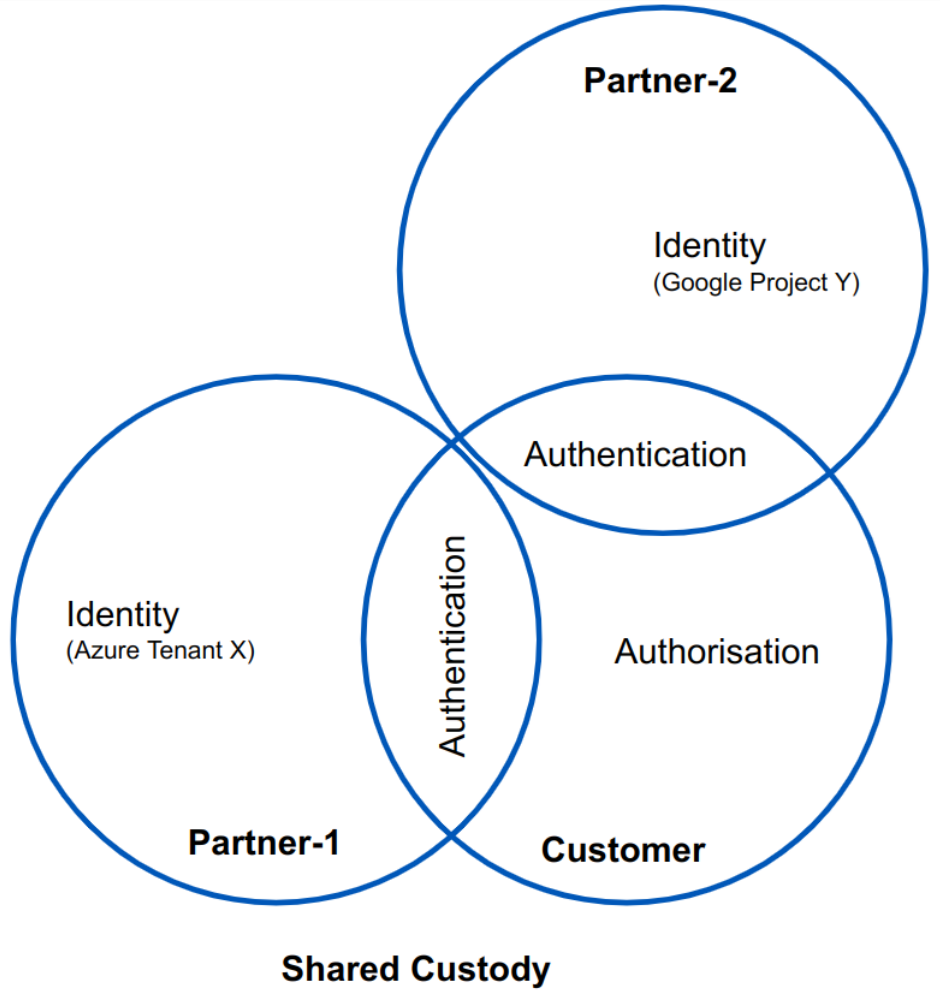
Industrial Control Systems have more life-span, more variation, more uniqueness than any IT infrastructure

- HVAC, BMS, Facilities
- HMI, PLC, ERP, …

And **more** constituents

- Integrator, Manufacturer, Contractor, Joint-Venture, Staff, Regulatory, …

Each have different **scope**, **risk**, **controls**

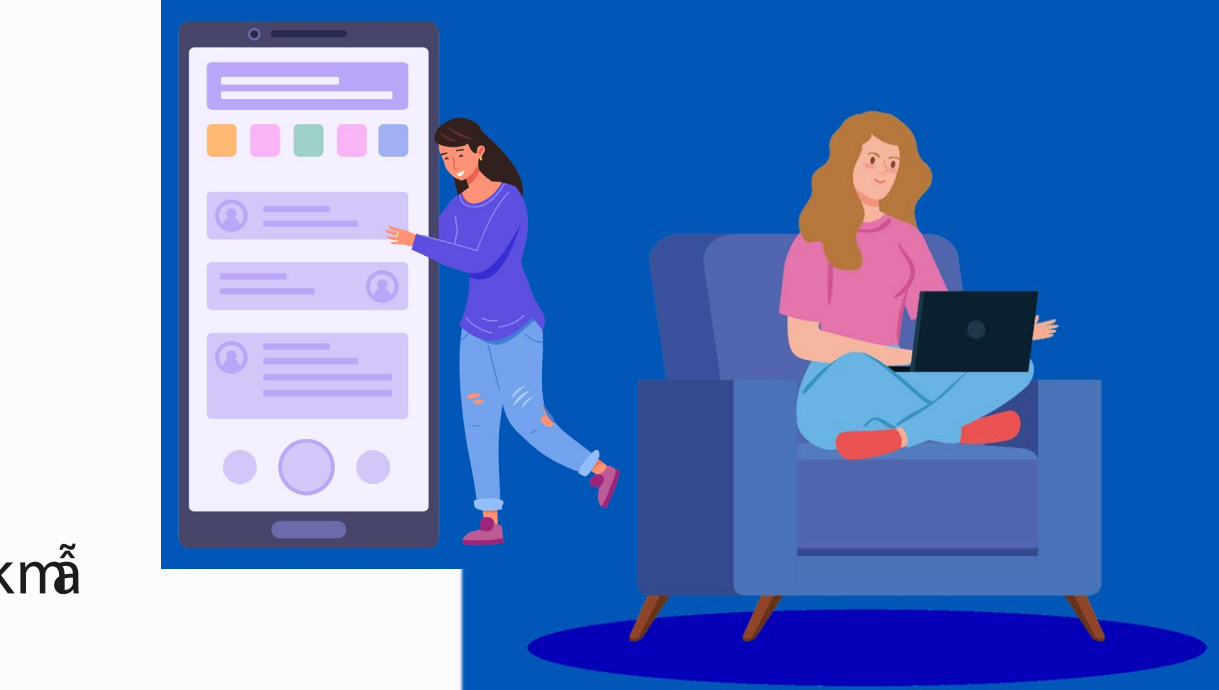


Connectivity Nirvana

Tx{"}i|tî¢ x{tm{|Ụ

- åẄẅ kkm|| "xwú "}qm'{m|x~{km| "ẄẄwmmì ã
- åT{xv "}qm'ux ki }rxwŞwm}¢ x{t "xn'v/"kqxrkmã
- å] w'}qm'l mrkm'xn'v/"kqxrkmã
- åe r}q"v/"|rwpuṁ|rpwîxw'k{ml mw}ri ụ ã

Any user.
Any Application.
Any Device.
Any Network.



AGILICUS

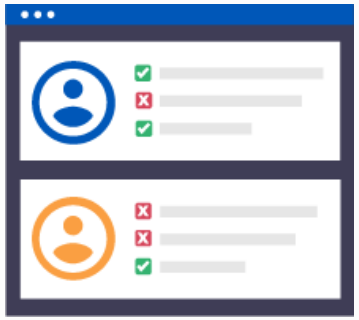
What is Zero Trust

Identity (WHO)

Every user (person) must be individually known and authenticated.

Authorisation (WHAT)

O| | rpw'y m{v r| | rx w| "
i wl "y{r¡ rumpm| "}x"~| m{| "
i wl "{m| x~{km| Õ



Access (HOW)

User are routed only to destination resources they are authorised for.

High Level User View

Its all web-based (my tablet, my phone, my laptop…no software)

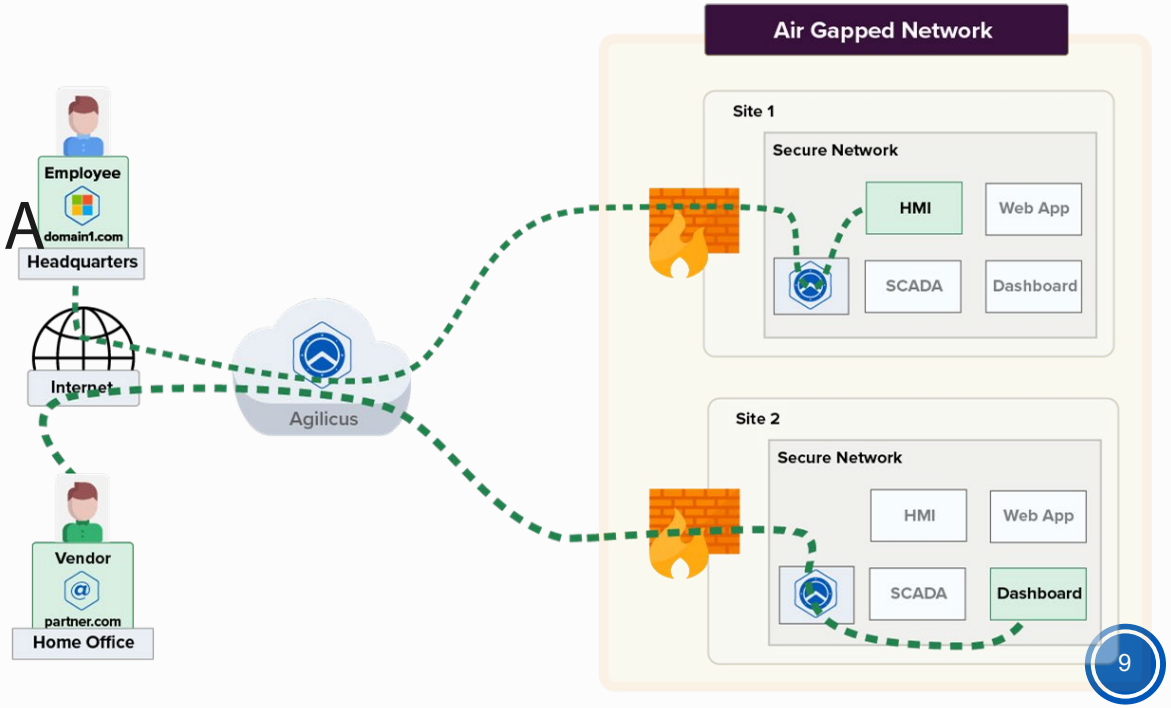
Its my existing company login (user@partner)

It's your authorisation (who can do what, do they need multi-factor)

Ideal for narrow-task workers

HMI, PLC program, PLC tags, SCADA Historian, Facilities, BMS, …

No layer 3, IP routes, subnets, 1 thing only



Case Studies (www.agilicus.com)

Midland Texas Transforms Water Purification Cyber Security

How the City of Kenosha Transitioned to Zero Trust

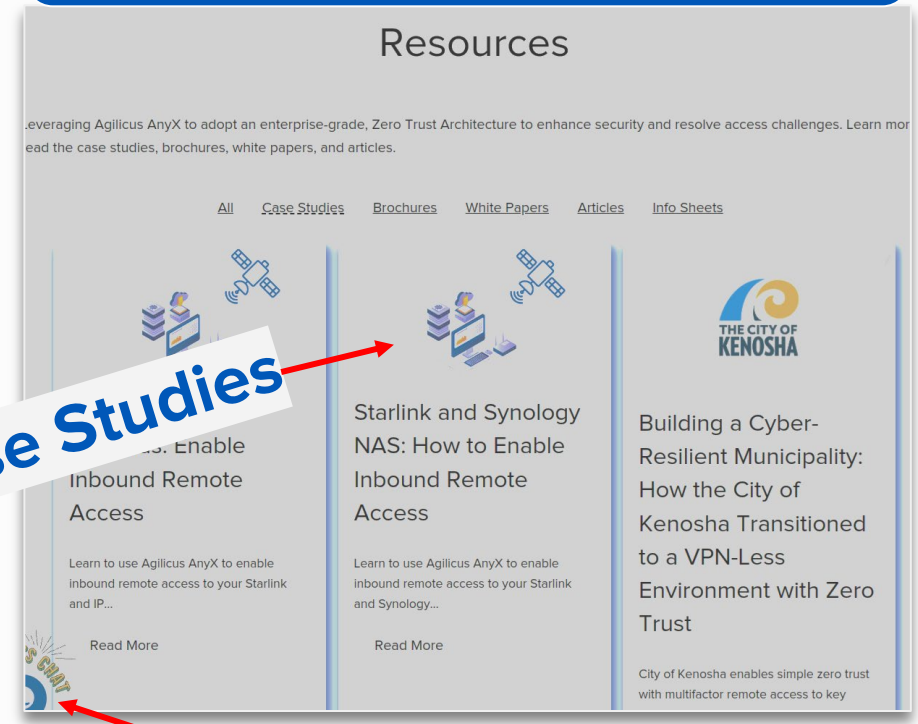
How the Town of Mono Future-Proofed its Cybersecurity Infrastructure and Transformed Municipal Operations

Call To Arms (Action)

1. Recognise the growing under-served
   a. Things get smarter and more specialised and more online
   b. Security gets more important
   c. Lateral traversal becomes more costly
2. Understand the VPN is not an appropriate solution for all
   a. Can't/Won't install your software
   b. Lateral traversal risk
3. Understand Single Sign On and Multi-Factor for all, not just your team
   a. No Shared accounts
   b. No new accounts
4. **Email/Call/Calendar/Smoke Signal** me (don@agilicus.com)

ENGAGE WITH US

Web
https://www.agilicus.com/



@Agilicus

Email
info@agilicus.com

Ask Me Anything!

https://www.agilicus.com | info@agilicus.com