EESTI RAUDTEE

evr.ee

Implementing Zero Trust @ Estonian Railways

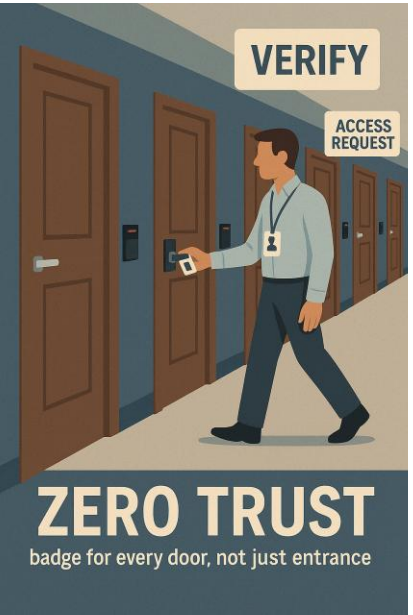
Tõnu Tammer
CIO
01.12.2025

Tõnu Tammer

- 2 years – CIO of Estonian Railways
- 5 years – Director of CERT–EE
- 9 years – various positions at Home Affairs (diplomat, CSO, project manager, CQO)
- 2024 – Knight of the Order of the White Star, 4th Class for promoting cybersecurity
- 2022 – Member of TOP100 influencers in Estonia

What is Zero Trust?

- **Zero Trust** is not a product but 15 years old concept / mindset / strategic aproach
- Think of Zero Trust as requiring a badge for every door, not just the building entrance. Even if you’re inside, you must prove your identity and intent at every step.



- **Verify Explicitly:**
  Always authenticate and authorize based on all available data points – user identity, device health, location, service, and anomalies. This is enforced at every access attempt, not just at login.
- **Least Privilege Access:**
  Users and systems are granted only the minimum access rights required to perform their tasks. This limits the potential damage from compromised accounts or devices.
- **Assume Breach:**
  Operate under the mindset that a breach may have already occurred. Segment access, monitor continuously, and minimize the blast radius of any incident.

Why jump on the new train?
The IT world we know...

NIS2D and GDPR: cost of prevention becomes cheaper than risk of impact / fine

we're under attack (surprise, surprise! ☺)

all the time! (again, surprise ☺)

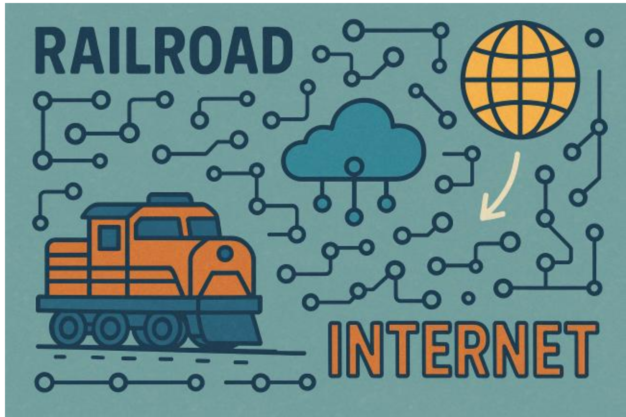
legacy

lack of MFA

huge stash of different technology

Users outside of office

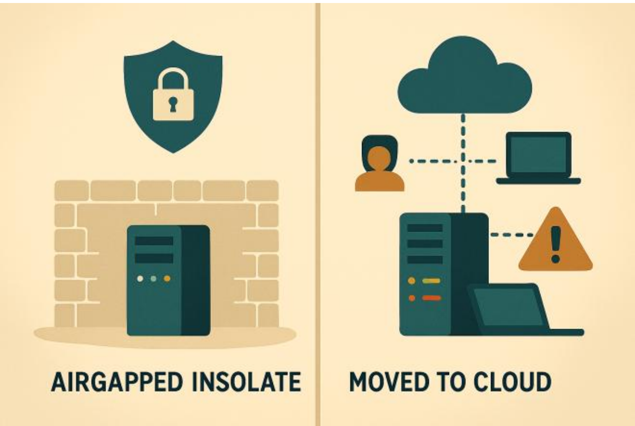
Why jump on the new train?
The OT world we (don't) know...



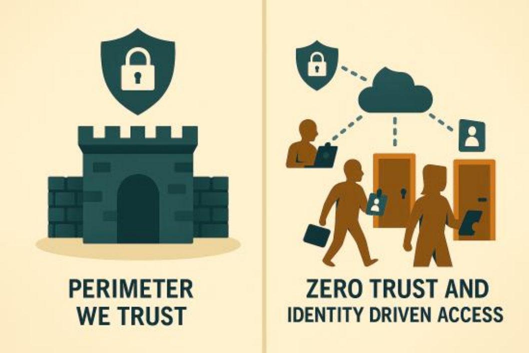
airgapped and isolated

vs

moved to cloud and connected



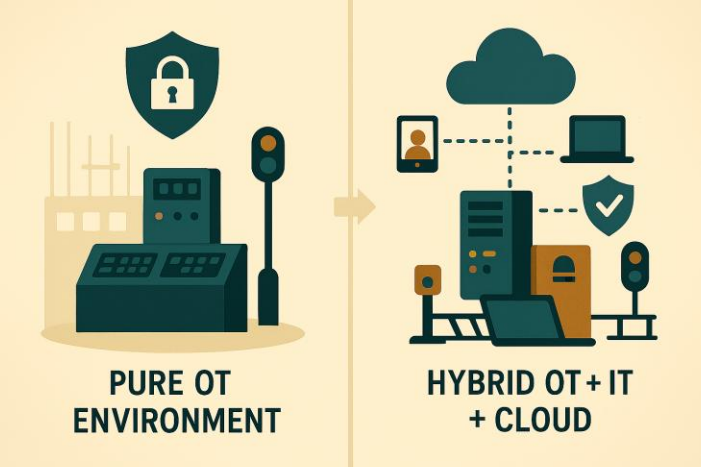
perimeter we trust
vs
zero trust and identity driven access



pure OT environment

vs

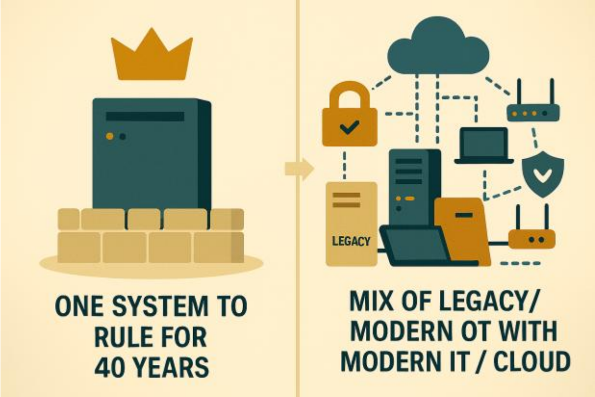
hybrid OT + IT + cloud



one system to rule for 40 years

vs

mix of legacy/modern OT with modern IT / cloud


ONE SYSTEM TO RULE FOR 40 YEARS
LEGACY
MIX OF LEGACY/ MODERN OT WITH MODERN IT / CLOUD

Key takeaways

Microsegmentation has never been easier

MFA access on all applications incl. legacy

Access based on device

Access based on external validation (4 eyes principle)

Partners get what they need not all routes

Zero Trust works in the context or rail

Thank you!

Questions?

What did you patch today?