Lars Larsson Lundsten, PhD
Cyber Security: Kritisk Infrastruktur
2026-03-26

welkin by elastisys

Secure-by-design i praktiken

Så bygger en applikationsplattform lager av säkerhet.

CLASSIFICATION: PUBLIC

Lars Larsson Lundsten, PhD
Field CTO

Cloud since 2008. Formerly with Axis Communications and research at Ericsson.

Thought leader on cloud and compliance w/ 25k+ followers on LinkedIn

welkin

What is your worst protected software?

And what can a hacker do if they get in?

welkin

STATUS QUO

Security + critical infrastructure in 2026

STRUCTURAL WEAKNESSES

Legacy communication protocols
→ Weak authentication & integrity (CISA)

Underinvestment in secure OT
→ Growing exposure in industrial environments (WEF)

Poor observability
→ Poor root-cause analysis & slow response (WEF)

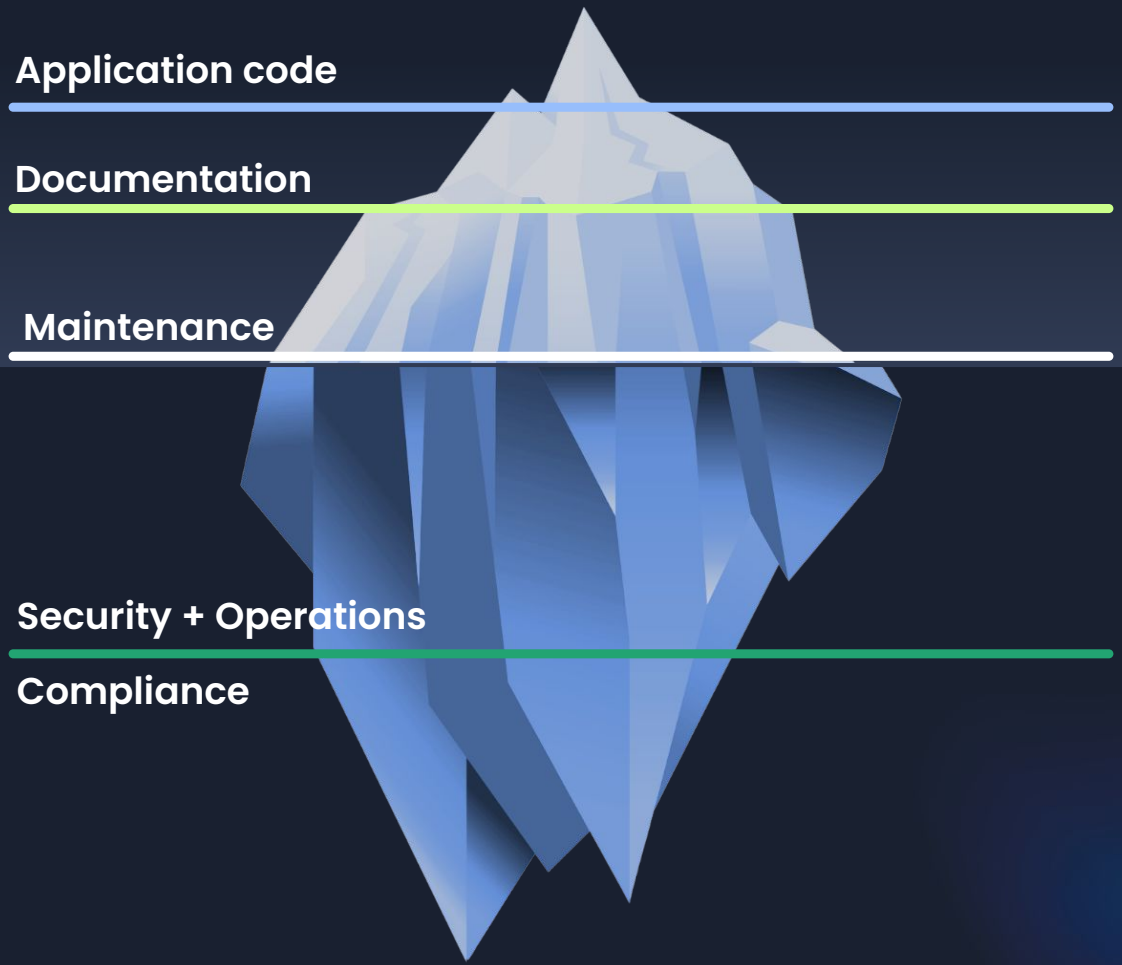
Supply chain fragility
→ Largest barrier to cyber resilience (WEF)

THREAT LANDSCAPE 2026

Escalating cybercrime & targeted attacks
→ National threat assessments (SÄPO, FRA)

Weaponization of vulnerabilities
→ Faster exploitation cycles

Cloud sovereignty risks
→ “Sovereignty washing” by hyperscalers



Mitigations

Trustworthy supply chains, and means to verify them

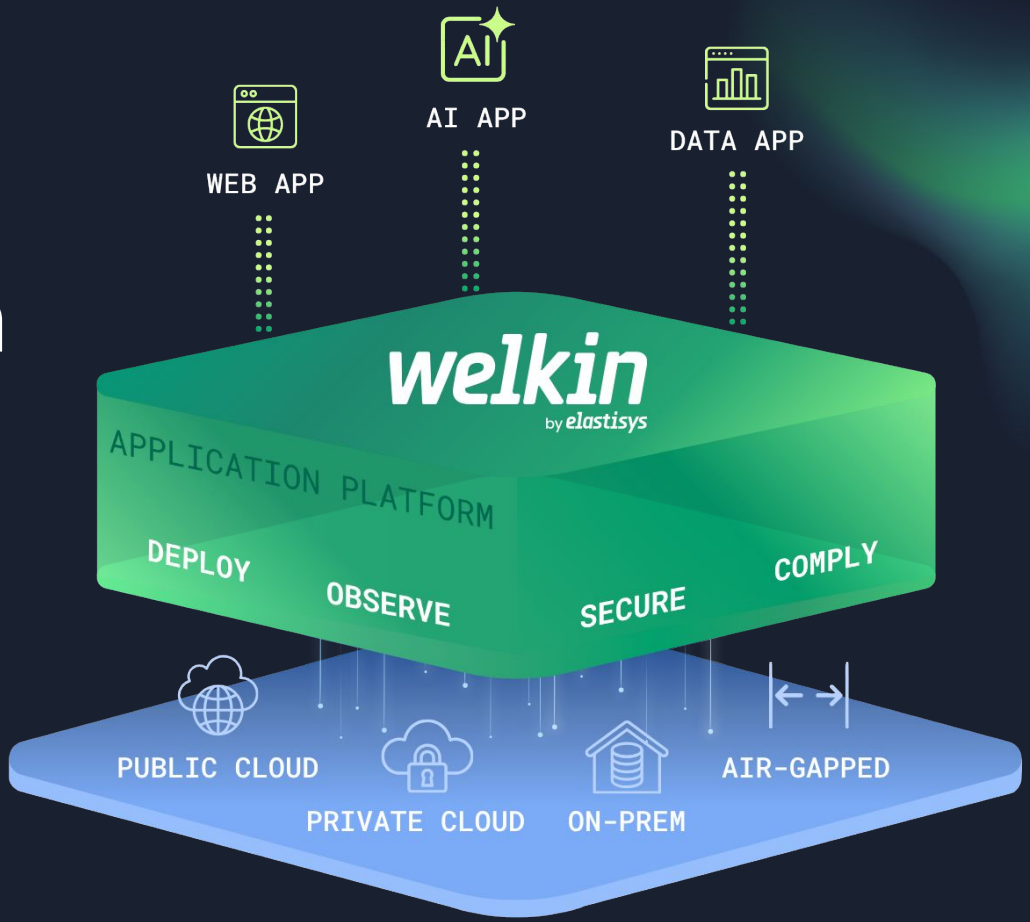
Tamper-proof and deep observability

Vulnerability management, intrusion detection, and isolation **in depth**

Enforce security best practices by deeply **embedding applications** in security they cannot violate

Security should be built into the PLATFORM

Security-hardened Application Platform



Security measures are not unique, your applications are

Raising the lowest bar

Isolate applications
Strict limits. Reduced capabilities. Only specifically allowlisted network requests.

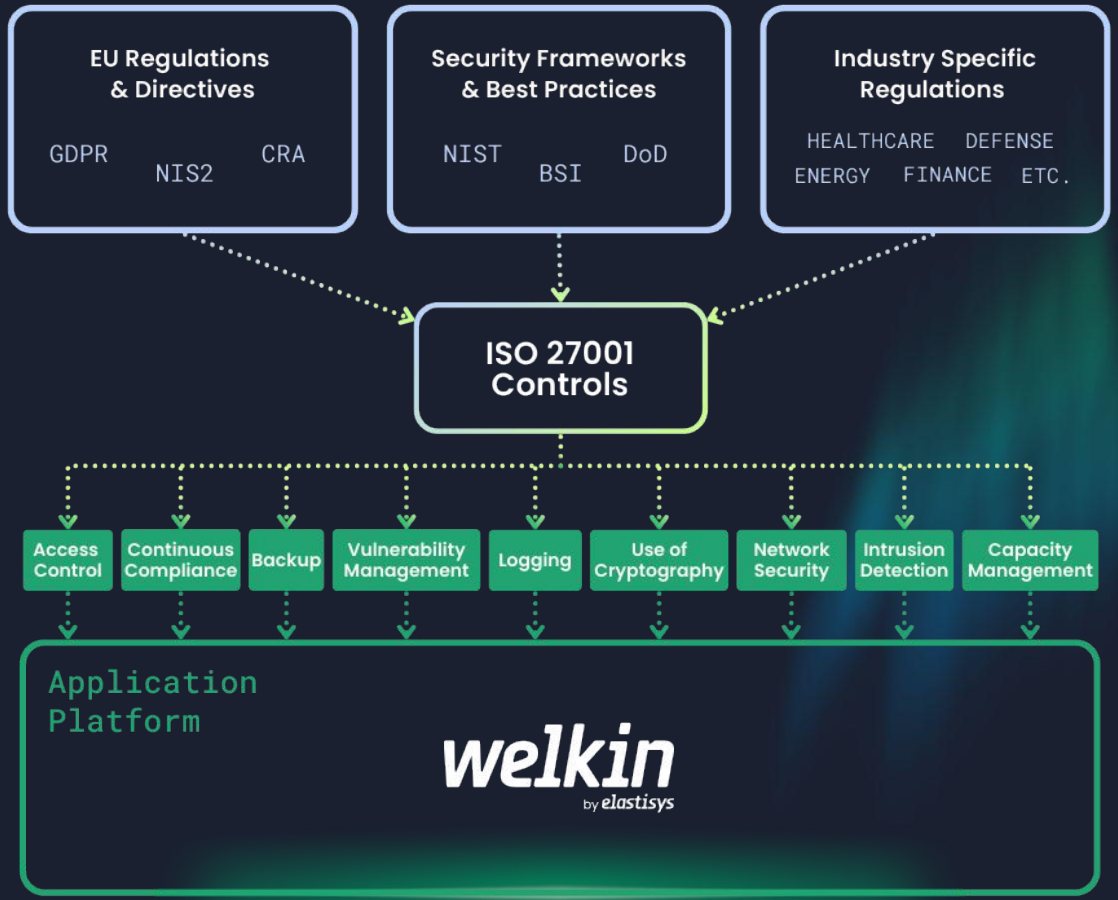
Force encryption everywhere
Network and storage.

Injected configuration
Inject secrets configuration securely.

Vulnerability and intrusion detection
Protect against the known and unknown.

Tamper-proof observability
Observe in depth from the outside. Tamper-proof records.

Fine-grained permissions
Both for humans and applications.



Summary

Critical infrastructure is under more cyber threat pressure than ever.

Security should be built into the platform.

Security measures are not unique, your applications are.

"Defense in depth" is *secure by design* in practice.

Connect on LinkedIn for more content

Lars Larsson, Field CTO
www.linkedin.com/in/llarsson/
lars.larsson@elastisys.com

Sources

SOURCES

Status quo for critical infrastructure

- US Cybersecurity and Infrastructure Security Agency (CISA)
  - "CISA Releases Guide to Help Critical Infrastructure Users Adopt More Secure Communication", 2026
  - Decades-old communication protocols with poor support for authentication and integrity checks are security concern

- World Economic Forum:
  - "The dangerous blind spot in critical infrastructure cybersecurity", 2025
    - Lack of investment in secure Operational Technology (OT)
    - Poor observability features leading to bad root cause analyses
  - "Global Cybersecurity Outlook 2026", 2026
    - Third-party and supply chain vulnerabilities is largest barrier for large companies to cyber resilience

Swedish cybersecurity

- "Handlingsplan 2026: Nationell strategi för cybersäkerhet 2025–2029", Regeringskansliet, 2026
  - MCF to collaborate with FRA and be supported by FMV, Försvarsmakten, Polismyndigheten, PTS and Säkerhetspolisen as well as Finansinspektionen and Sveriges Riksbank
- The Swedish Säkerhetspolisen (SÄPO) and Försvarets Radioanstalt (FRA) both state in their yearly outlooks that 2026 will be plagued by high cybercrime activity, use of vulnerabilities, and directed attacks on European and Swedish infrastructure (SÄPO, FRA)