Nortal

Cybersecurity

Operational Technology Security

In today’s rapidly evolving manufacturing landscape, the security of operational technology (OT) is paramount. Cyber threats targeting OT systems can disrupt production, compromise safety, and lead to significant financial loss.

Recent cyberattacks on Industrial Control Systems (ICS) have exposed alarming vulnerabilities, leading to production halts, safety risks, and hefty financial losses. High-profile incidents like the ransomware attack on a major pipeline operator and the infiltration of a global food processing company highlight the urgent need for robust OT security measures. With increased need for connectivity, and improved sophistication of cyber threats, securing ICS must be central to operational strategy.

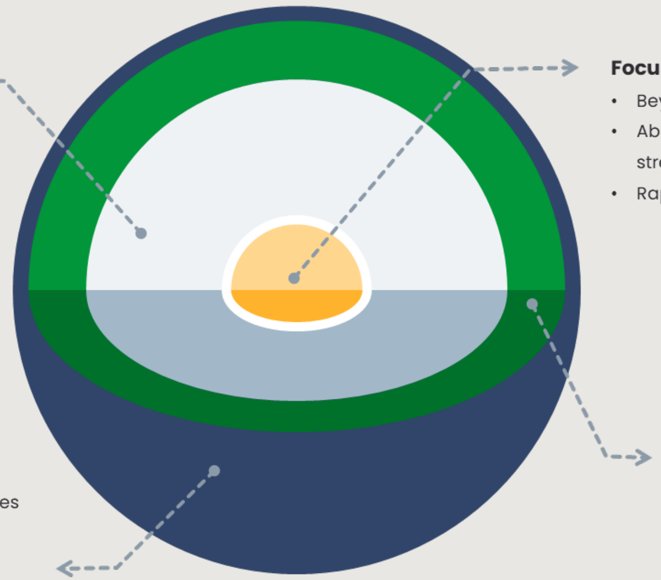
Nortal Advanced OT Security

Unlike traditional consultancies, our expertise is forged in defending military installations, vessels, and data centers against the most sophisticated state-level threats.

We don’t just adapt commercial security practices, but bring a fundamentally different approach, that anticipates and mitigates threats at a level most civilian-focused security firms can't match. This means your critical OT and IT systems benefit from security strategies designed to withstand the most extreme and sophisticated attacks imaginable.

Nortal is a leading digital security company serving defense, energy, healthcare, manufacturing, and finance organizations worldwide. Leveraging our robust security R&D capabilities, we help our customers protect against not only today’s threats but also the threats of tomorrow.

Advanced OT Security Methodology, unique to Nortal, integrates military-grade security practices with industrial operational requirements - a combination not found in standard cybersecurity offerings.



Advanced Threat Modeling

- Based on nation-state actor capabilities and tactics
- Consideration of blended cyber and electronic warfare scenarios
- Anticipation of zero-day vulnerabilities and advanced persistent threats

Focused on Resilience:

- Beyond checkbox compliance to operational continuity
- Ability to maintain critical functions under severe stress
- Rapid recovery and adaptation capabilities

Holistic Multi-Domain Assessment:

- **Cyber:** Network architecture, access controls, encryption, incident response
- **Operational:** Process controls, failsafes, redundancy measures
- **Physical:** Access restrictions, environmental controls, power systems
- **Personnel:** Security clearances, training, insider threat mitigation

Proven in Extreme Environments

- Methodology refined in naval platforms operating globally
- Adapted for data center complexities and scale
- Aligned with emerging regulations (DORA, NIS2, SEC rulings)

Nortal

The opportunity to redesign your future is now

Your frictions and frustrations are our insights and inspirations.

Let’s discuss!