Nortal

Cybersecurity

Zero Trust Enterprise

The digital landscape in which organizations operate is a dynamic battleground, where bad actors continually refine their tactics to exploit vulnerabilities. Cybersecurity threats show no signs of diminishing; instead, they are poised to intensify with the use of adversary- AI algorithms.

NIST

Despite the growing awareness of the importance of cybersecurity, a significant number of organizations lack the necessary resources and expertise to fight against ever-changing cyber battleground. As a result, most organizations remain vulnerable to cyber-attacks that can lead to data loss, financial damage, and reputational harm.

Nortal Zero Trust Enterprise Service is designed to rapidly evaluate the maturity of current policies and controls, pinpoint high-risk gaps, and aid in the remediation process.

Assess

Identify industry specific risks against most valuable assets. Evaluate security policies, technical controls, and organizational threat awareness

Fortify

Minimize data breach and ransomware risk by implementing comprehensive and practical security controls across IT and OT systems

Verify

Elevate organizations preparedness with realistic cyber incident simulation and exercises coupled with capability development programs

$9.5M

Average cost of a security breach in US

*IBM

$700K

Median ransom demand in 2023

*Palo Alto Networks

82%

Percentage of ransomware attacks targeting mid-sized operations

*CoveWare

Nortal

Nortal is a leading digital security company, serving defense, energy, healthcare, manufacturing, and finance organizations globally. Our Zero Trust Enterprise Service, built on NIST CSF 2.0 framework and backed by the real-time threat data from our cyber research team, strengthen organizations' defenses against modern bad actors in a practical manner.

Risk Assessment

- Identification of Most Valuable Assets (MVA) and realistic risk scenarios
- Review of security policies, their adoption and enforcement
- Review of security architecture and existing technical controls
- Gap analysis and remediation action plan
- Assess of employee awareness and training

Zero Trust Controls

- Endpoint Protection
- Network Segmentation & Hardening
- Identity and Access Management
- Enhanced Authentication
- OT Security
- Data Protection and Loss Control
- E-Mail Protection
- Insider Threats
- Supply Chain Security
- DevSecOps

Attack Simulation

- Exercises based on MITRE ATT&CK framework to simulate likely sector-specific cyber attack campaigns
- Practice handling real-world scenarios, train teams and individuals, and test IT & OT solutions in realistic conditions with complex simulation environments
- Assess escalation and disclosure processes against regulatory compliance requirements

Nortal

The opportunity to redesign your future is now

Your frictions and frustrations are our insights and inspirations.

Let’s discuss!