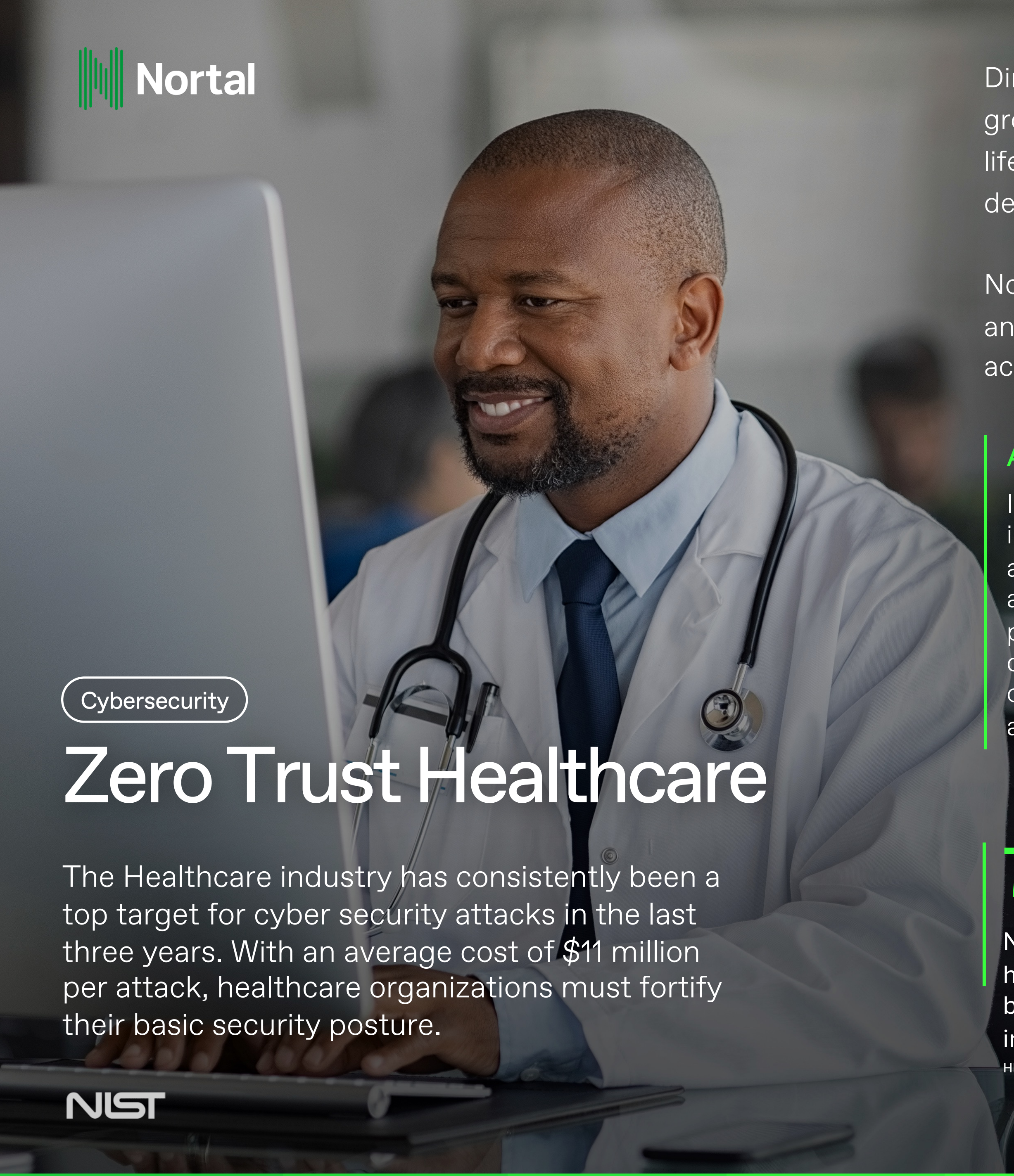
Nortal



Cybersecurity

Zero Trust Healthcare

The Healthcare industry has consistently been a top target for cyber security attacks in the last three years. With an average cost of $11 million per attack, healthcare organizations must fortify their basic security posture.

Directly targeted ransomware attacks aimed to disrupt clinical operations are a growing cyber threat to hospitals. Yet, 96% of hospitals are operating with end-of-life software, with known vulnerabilities across IT systems and connected medical devices.

Nortal ZeroTrust Healthcare Service guides organizations to rapidly assess, plan, and deploy practical safeguards to protect IT assets and connected medical devices across the organization.

Assess

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

Fortify

Minimize data breach and ransomware risks by implementing comprehensive and practical security controls across IT and connected medical systems

Verify

Elevate the organization's readiness with realistic cyber incident simulations and exercises coupled with capability development programs

725

Number of healthcare data breaches in US in 2023

HHS

$11M

Average cost of data breach in US healthcare in 2023

Verizon DBR

141

Number of hospitals impacted by breaches in US in 2023

Emsisoft

NIST

Nortal

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

NATO OTAN · UK Atomic Energy Authority · amazon · EAST TALLINN CENTRAL HOSPITAL · Ministry of Defence · comcast · Humana. · T · · Mobile · Johnson & Johnson · Ochsner

Risk Assessment

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

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!