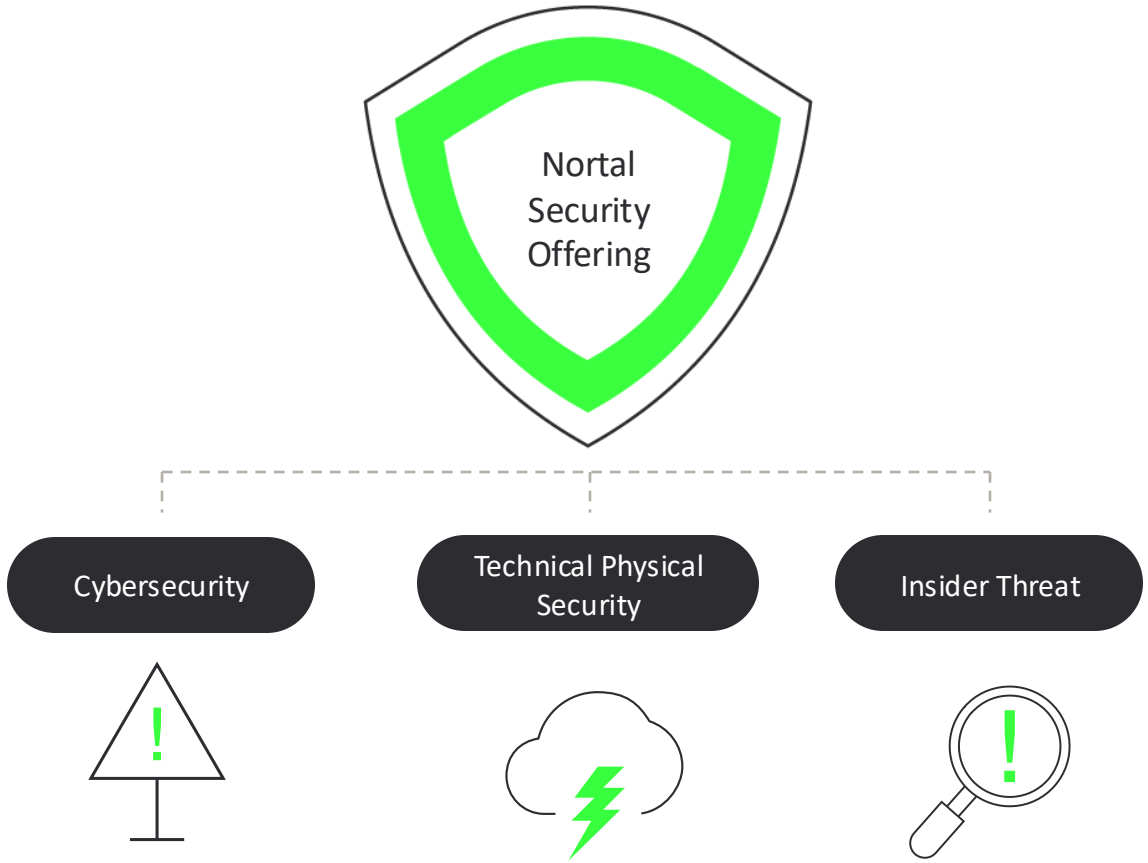
What aspect of your healthcare organization's security keeps you up at night?

Securing patient data, safeguarding critical medical systems, and ensuring compliance with regulations such as HIPAA are fundamental priorities in healthcare.

Nortal delivers cutting-edge solutions that integrate advanced encryption, AI-powered threat detection, and zero-trust security frameworks. These technologies protect sensitive information, secure connected medical devices, and mitigate cyber threats. By fortifying patient trust and enhancing the resilience of healthcare operations, we empower providers to deliver uninterrupted, secure, and fully compliant care.



Nortal's Triple Shield Approach: Comprehensive, Adaptive, Resilient Security

Cybersecurity

Defend patient data and critical systems while ensuring compliance with HIPAA and protection against cyberattacks.

- Risk Assessment: Uncover vulnerabilities in electronic health records (EHRs), IoT medical devices, and telemedicine systems.
- Zero Trust Framework: Implement stringent access controls for sensitive patient data, ensuring only authorized personnel have access.
- Threat Detection and Response: Real-time monitoring and AI-driven threat mitigation to prevent breaches before they impact care delivery.
- Data Protection: Advanced encryption safeguards sensitive patient information from unauthorized access or loss.

Technical Physical Security

Safeguard hospitals and medical assets with advanced access controls designed to protect patients, staff, and critical infrastructure.

- Access Control Systems: Secure hospital wings, pharmacies, and data centers with advanced biometrics and layered security.
- Surveillance and Monitoring: AI-powered monitoring ensures real-time awareness of physical threats across healthcare campuses.
- Incident Response Plans: Tailored protocols for healthcare environments to ensure swift recovery after security events.

Insider Threat Management

Proactively address insider risks to safeguard patient safety and protect sensitive data from internal threats.

- Behavioral Analytics: Predict and address risks posed by employee negligence or malicious actions, safeguarding both patient data and physical assets.
- Training and Awareness: Educate healthcare staff on best practices for protecting patient information and recognizing security risks.
- Simulation Drills: Test organizational resilience against real-world scenarios, such as ransomware attacks or data breaches.