

FileSure for Healthcare

Ransomware Protection for Legacy Medical Systems

THE CHALLENGE

Healthcare organizations face a critical security gap: **67% of healthcare organizations were hit by ransomware in 2023-2024**, with attacks successfully encrypting data in 58% of cases. When breaches occur, hospitals average **\$2.73 million in recovery costs** - excluding any ransom payments.

Most vulnerable? Legacy Windows XP/7 systems connected to critical medical equipment:

- **Medical imaging (PACS/RIS):** 10-15% still on legacy OS, \$500K-\$1M per machine to upgrade
- **Laboratory systems (LIS):** 53% on legacy systems, \$100K-\$300K per upgrade
- **Patient monitoring:** Often embedded XP, \$50K-\$100K per bed to replace
- **Pharmacy/infusion pumps:** Legacy control systems, \$10K-\$20K per pump upgrade

THE SOLUTION

FileSure for Healthcare provides immediate protection for these vulnerable systems without requiring expensive equipment replacement or OS upgrades:

- **Blocks malware installation** by preventing any program from writing executable code
- **Maintains system integrity** by preventing unauthorized modifications to critical files
- **Prevents data theft** through application whitelisting that restricts file access
- **Protects connected equipment** by securing legacy OS interfaces
- **Simple deployment** with pre-configured protection, requiring minimal configuration

THE INVESTMENT

- **\$150 per device/year** - a fraction of equipment replacement costs
- **No server infrastructure required** - operates independently on each device
- **Compliance-ready logging** - maintains audit trails on each protected endpoint
- **Upgrade path** to full FileSure Defend enterprise solution available when needed

PROVEN RESULTS

FileSure's technology has successfully blocked ransomware attacks that bypassed traditional antivirus solutions by preventing the initial infection phase - even on systems running outdated operating systems.

NEXT STEPS

1. Schedule a 30-minute technical demonstration
2. Identify 3-5 high-risk systems for initial protection
3. Deploy proof-of-concept implementation
4. Measure security improvement with before/after vulnerability assessment

Contact: sales@bystorm.com | www.bystorm.com