FILESURE DEFEND

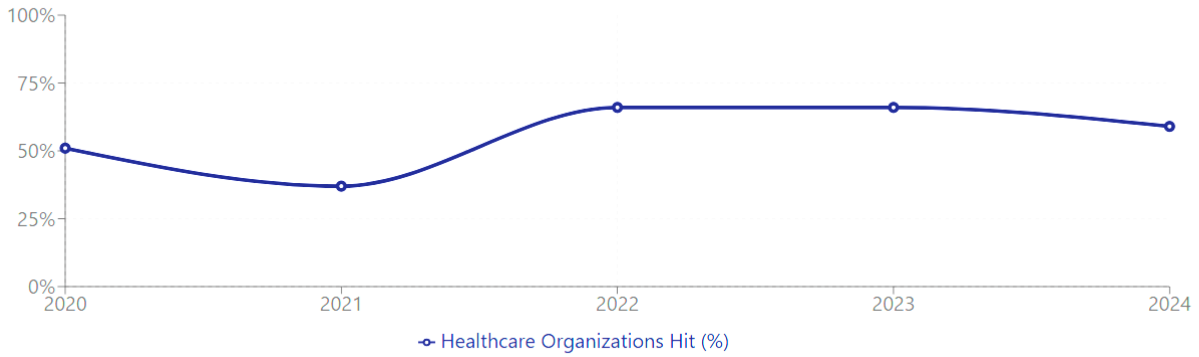
Protecting Healthcare's Critical Systems from Ransomware

THE THREAT LANDSCAPE

67% of healthcare organizations were hit by ransomware in 2023-2024, with **58% of attacks resulting in data encryption**. When ransomware strikes a hospital, an average of **58% of computers are impacted**.

The stakes are higher in healthcare than any other industry: - **$10.10 million**: Average cost of a healthcare data breach (highest of any industry) - **$2.73 million**: Average recovery costs (excluding ransom) - **$3.9 million**: Average ransom demanded from healthcare organizations - **66%**: Success rate of backup compromise in healthcare sector

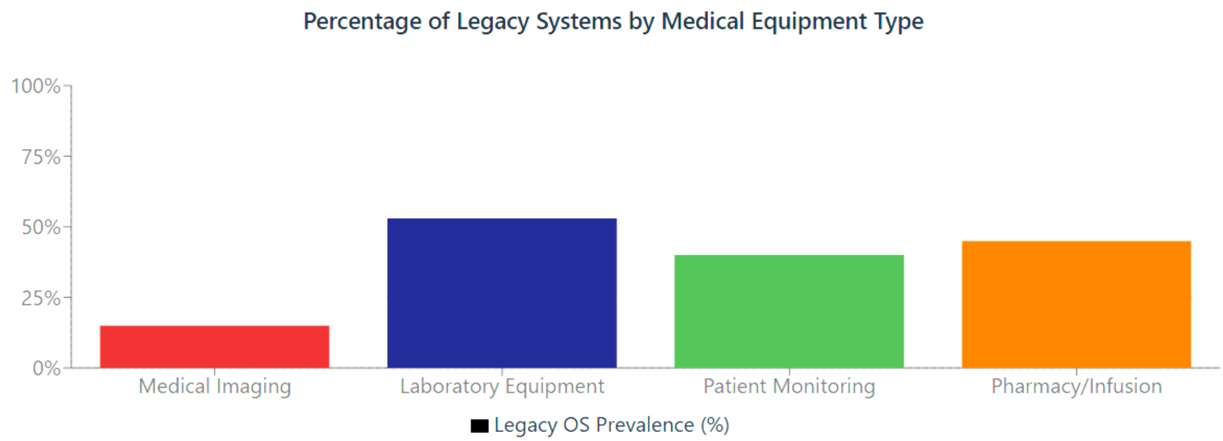
Healthcare Ransomware Attack Trends *Healthcare Ransomware Attack Rate 2020-2024*



THE LEGACY SYSTEM CHALLENGE

Healthcare facilities face a unique dilemma: critical medical equipment often relies on legacy operating systems (Windows XP/7) that cannot be easily upgraded:

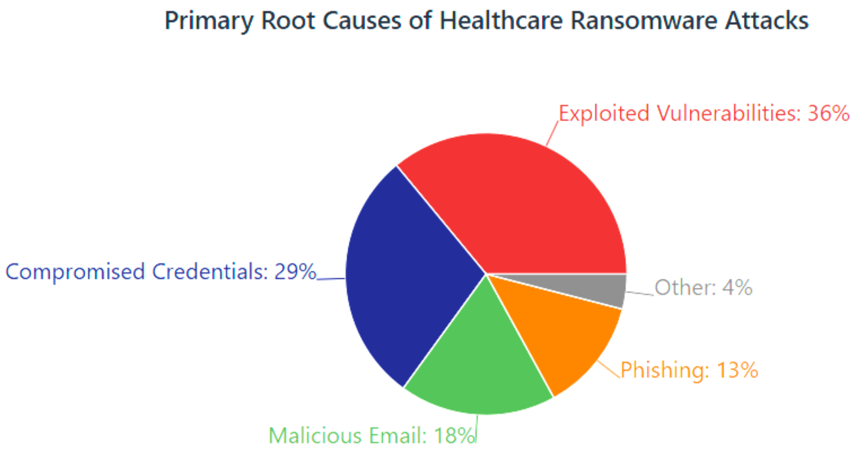
- **Medical Imaging Systems (PACS/RIS)**: 10-15% on legacy OS, $500K-$1M per machine to replace
- **Laboratory Equipment (LIS)**: 53% legacy prevalence, $100K-$300K per upgrade
- **Patient Monitoring Systems**: Embedded XP, $50K-$100K per bed to replace
- **Pharmacy/Infusion Pumps**: XP/7 only, $10K-$20K per pump upgrade



THE ROOT CAUSES OF RANSOMWARE ATTACKS

The majority of ransomware attacks in healthcare environments originate from:

1. **Exploited Vulnerabilities (36%)**: Unpatched security holes in Windows, browsers, or applications
2. **Compromised Credentials (29%)**: Stolen login information used by attackers to gain entry
3. **Malicious Email (18%)**: Emails with malicious attachments that install ransomware
4. **Phishing (13%)**: Emails designed to trick users into revealing credentials

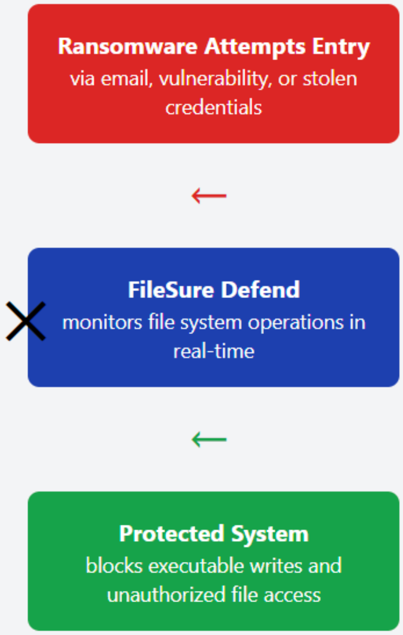


HOW FILESURE DEFEND PROTECTS YOUR SYSTEMS

FileSure Defend provides a cost-effective solution ($150/device) to protect vulnerable systems without expensive equipment replacement:

1. **Block Malware Installation**: Prevents any program from writing executable code to the hard drive, stopping ransomware before it can establish itself
2. **Application Whitelisting**: Limits access to protected files with a “White-List” of authorized applications, preventing data theft even if a system is compromised
3. **Simple Deployment**: Works on all Windows versions including legacy XP/7 systems, with centralized management and policy enforcement
4. **Minimal Impact**: No performance degradation on critical medical systems

FileSure's Protection Mechanism:

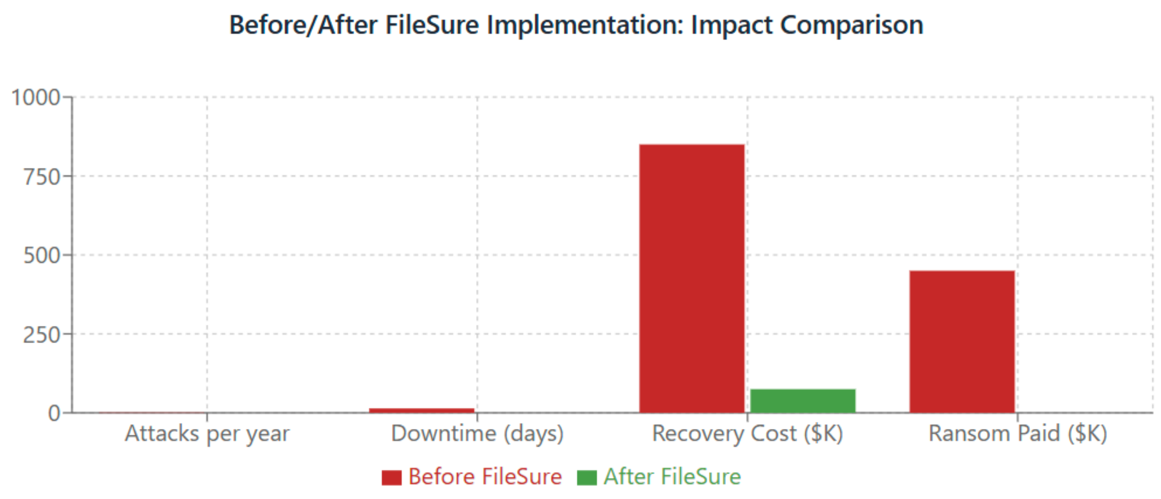

Ransomware Attempts Entry
via email, vulnerability, or stolen credentials
←
FileSure Defend
monitors file system operations in real-time
←
Protected System
blocks executable writes and unauthorized file access

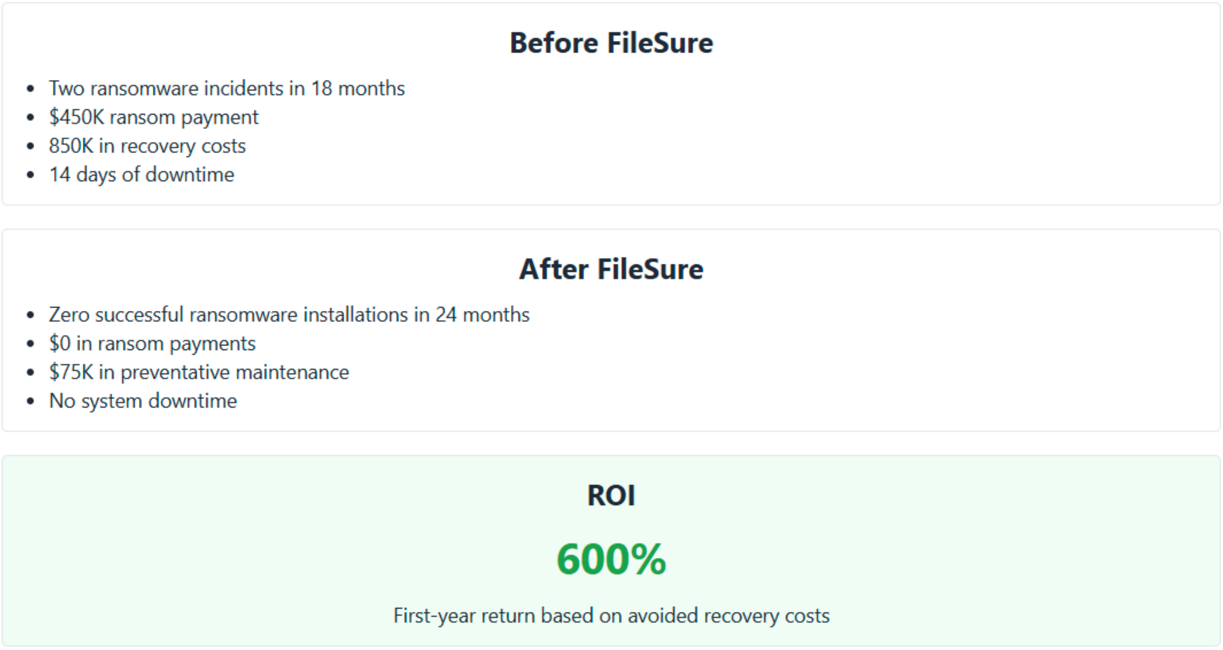
FileSure Defend prevents ransomware by blocking the writing of executable code to disk and limiting file access to only authorized applications

RANSOMWARE PROTECTION CASE STUDY

A mid-size hospital with 500 endpoints deployed FileSure Defend after discovering 25% of their medical systems relied on legacy Windows versions:

- **Before FileSure**: Two ransomware incidents in 18 months, one requiring $450K ransom payment
- **After FileSure**: Zero successful ransomware installations in 24 months
- **ROI**: 600% first-year return based on avoided recovery costs





Before FileSure

- Two ransomware incidents in 18 months
- $450K ransom payment
- 850K in recovery costs
- 14 days of downtime

After FileSure

- Zero successful ransomware installations in 24 months
- $0 in ransom payments
- $75K in preventative maintenance
- No system downtime

ROI

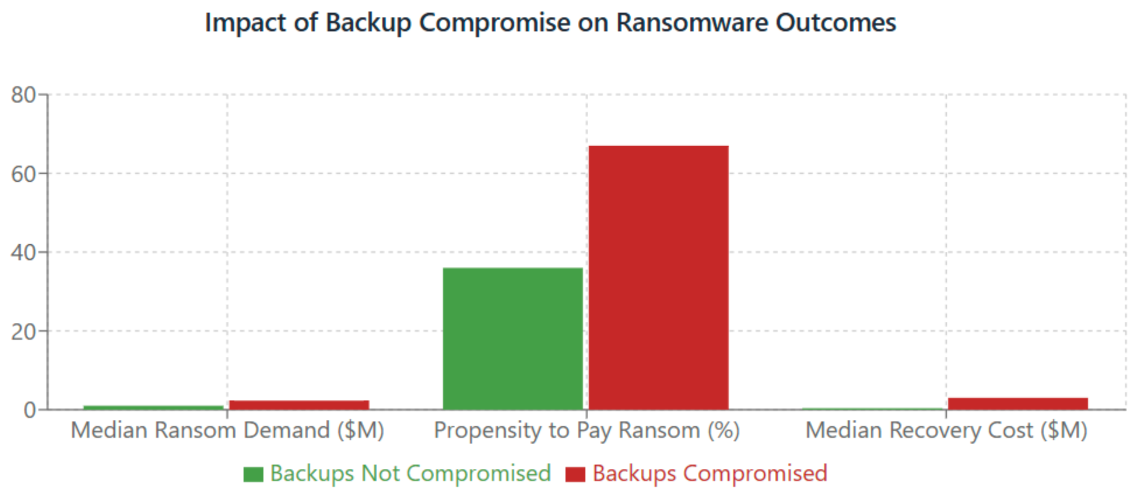
600%

First-year return based on avoided recovery costs

IMPACT OF BACKUP COMPROMISE

Organizations that had backups compromised reported considerably worse outcomes:

- **Ransom demands** were, on average, more than double that of those whose backups weren’t impacted ($2.3M vs. $1M median initial ransom demand)
- Organizations whose backups were compromised were **almost twice as likely to pay the ransom** to recover encrypted data (67% vs. 36%)
- **Median overall recovery costs** came in eight times higher ($3M vs. $375K) for those that had backups compromised



Backup Compromise Impact *Impact of Backup Compromise on Ransomware Outcomes*

GETTING STARTED

Schedule a demonstration to see how FileSure Defend can protect your critical healthcare systems. Implementation can begin with your highest-risk systems and expand across your network.

For more information, email us at: sales@bystorm.com

References: Data sourced from IBM Security Cost of a Data Breach Report 2022 and Sophos State of Ransomware 2024