FileSure for Healthcare: Technical Overview

How FileSure Protects Legacy Medical Systems

CORE TECHNOLOGY

FileSure uses a Windows file system filter driver that intercepts file operations at the kernel level, providing protection regardless of the Windows version (XP, 7, 10, or 11). This low-level integration allows FileSure to:

- Block executable file creation/modification - Prevents malware installation
- Restrict file access by application - Limits data theft and corruption
- Prevent file type changes - Stops bypass techniques like file extension manipulation
- Log all file access attempts - Maintains complete audit trails for compliance

PRE-CONFIGURED PROTECTION FOR MEDICAL ENVIRONMENTS

FileSure for Healthcare comes with pre-configured protection specifically designed for medical environments:

PROTECTION RULE SET 1: BLOCK MALWARE EXECUTION

- **Target**: Prevents creation/modification of executable files
- **File types blocked**: .exe, .dll, .vbs, .wsh, .ps1, .bat, .com, .scr, .ocx, .js
- **Operations blocked**: Write, Create, Rename, Delete
- **Application exceptions**: Legitimate update processes (configurable)

PROTECTION RULE SET 2: PREVENT DATA THEFT

- **Target**: Restricts access to sensitive files
- **File types protected**: .dat, .db, .mdb, .dbf, .pdf, .dcm (DICOM), custom formats
- **Access control**: File access restricted to authorized applications only
- **Operations protected**: Read, Copy

PROTECTION RULE SET 3: SYSTEM INTEGRITY

- **Target**: Prevents modification of system configuration
- **Files protected**: System files, configuration files
- **Operations blocked**: Modify, Delete, Rename
- **Allowed applications**: Only authorized system management tools

IMPLEMENTATION ON LEGACY MEDICAL SYSTEMS

FileSure is uniquely suited for legacy medical environments:

- **Compatible with Windows XP/7/10/11** - No OS upgrades required
- **Low resource utilization** - 2% or less CPU impact, 50MB memory footprint
- **No network dependency** - Protects standalone systems
- **No internet connectivity required** - Works in air-gapped environments
- **Works alongside existing security tools** - Compatible with antivirus solutions

DEPLOYMENT PROCESS

FileSure for Healthcare's simplified deployment focuses on immediate protection:

1. **Installation**: MSI package deployable via standard methods (GPO, SCCM, manual)
2. **Initial configuration**: Pre-configured with healthcare-specific protection rules
3. **Monitoring**: Local logging of security events, syslog integration available
4. **Maintenance**: Minimal ongoing management required

TECHNICAL SPECIFICATIONS

- **Supported OS**: Windows XP SP3 and newer
- **Hardware requirements**: 1GB RAM, 100MB disk space
- **Deployment methods**: MSI installer, silent install switches available
- **Management**: Local configuration, exportable settings for mass deployment
- **Logging**: Local Windows Event Log integration, syslog integration, exportable audit logs

UPGRADE PATH

When more advanced features are needed, seamless upgrade to FileSure Defend:

- **Centralized management console**
- **Real-time alerts and notifications**
- **Customizable security rules**
- **Advanced reporting capabilities**
- **Integration with SIEM systems**

For technical questions or to schedule a proof-of-concept deployment:

Email: support@bystorm.com