ForceField™ WFS™

Simplified Data Security

PROTECTS DATA AS IT IS WRITTEN

Today's storage systems all suffer from the same vulnerabilities. Data files, documents, transactions, video, voting tabulation or other valuable content can all be sabotaged, manipulated, deleted, held Ransomware or worse, all without your knowledge.

Cyber-defense is failing at the network, system and application levels. Constant cyber-attacks and insider threats incur severe losses with staggering damages and escalating liabilities.

With current security designs hackers attack a lower layer in the security stack, bypassing the protections. Effective **security must be at the lowest layer in the stack**, with the data bits and bytes, inside of the disk hardware itself. This means that security travels within each disk drive and cannot be bypassed regardless of OS or credentials.

A new way of securing valuable data by simply saving it.

ForceField™ WFS™ is a new and different approach to data protection. Each data block is "Locked Down" as it is written. No need to wait for a file to be closed to protect it.

Hardware-level protection is implemented inside of the disk drive and cannot be bypassed since it is internal to each ForceField™ disk, at the lowest layer in the security stack, with the bits and bytes inside of the disk. The **ForceField WORMdisk™ File System (WFS) works in conjunction with the hardware** to ensure that every block of data can't be sabotaged, deleted, Ransomware and is strongly encrypted to prevent disclosure of your sensitive information.

Users may select permanent or temporary **protections for blocks, files, volumes and physical disks.** Protects from BOTH disclosure and from modification or deletion. Supports Volume and File Passwords, AES 256 Block Encryption, and simplified key management with crypto-erase features.

WORMdisk™ security protections cannot be bypassed or circumvented regardless of operating system or access permissions. They are used by **the NIST SP 1800-11 NCCoE Data Integrity project for protection against Ransomware and other malicious events**.

These technologies have been **validated by DISA** and are in use by many federal, state and local governments in addition to banks, credit unions, brokerage firms, oil & gas, telecommunications, media content and other organizations.

Uses patented and proven WORMdisk™ technologies to provide a protective umbrella around data the moment it is written with hardened data defense that hackers cannot break.

ForceField™ *Use Case Scenarios:*

- **Critical Data** - Neutralizes Ransomware, data sabotage, manipulation, deletion.
- **Important Documents, Files, Pictures, Video** – Immutable data.
- **Backups and Archives** – Safe and permanent, can't be deleted or Randomwared.
- **eMail Repositories** – eMail export & protect for records retention and compliance.
- **"Gold Image" Content** – Ensures binaries, executables, config and other data are pristine.
- **Financial Transactions** – Permanent real-time records, transactions and attachments.
- **Voter Fraud Prevention** – Every vote is immediately protected, prevents election meddling. High-speed I/O provides near instant secure voter recount.
- **Regulatory Compliance** – FINRA, SEC 17a3-17a4, DoD 5015.2, NARA & OMB, HIPAA.
- **Firewall Audit Log Files** – Firewall and router log entries are protected as they are created. Keeps hackers from deleting logs and covering their tracks.
- **Audit Logs** – Physical security and computer access logs cannot be manipulated or deleted.
- **Secure Files** – Documents, pictures, video, records and other important data files.
- **Permanent Records** – Land, tax, business, historical and other records requiring retention.
- **Legal Documents** – Contracts, immutable digital evidence and online court records.
- **Crypto-Currency** – Keep wallets, journals, trading information safe and protected.

The key difference is that ForceField™ protects data the moment it is written to the disk. If a hacker gets in, or if your system or application crashes, an insider attacks or a virus spreads, the data is already locked-down, protected and secure.

The ForceField™ **WORMdisk File System™ (WFS™)** API protects each data block and directory block as they are written, so no matter what happens, your data is safe and secure.

May the ForceField™ Be With You . . .

For more information, visit https://www.greentec-usa.com or call (703) 880-8332

NIST National Institute of Standards and Technology U.S. Department of Commerce
NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE
DATA INTEGRITY

Data Defense Cyber Defense
GreenTec™
www.GreenTec-USA.com

DEFENSE INFORMATION SYSTEMS AGENCY