CYBERdisk™ and WORMdisk™

Cyber-Defense Overview

Company Name: *GreenTec-USA, Inc.*

Cage Code: *6KCT1*

Products: *CYBERdisks™, WORMdisks™ & Servers*

E-mail: *info@greentec-usa.com*

Phone: *(703) 880-8332*

Company Website: *www.GreenTec-USA.com*

Primary company offerings:

- ✓ Cyber IT Hardware – Hardware level cyber-protection, always inside of the disk itself.
- ✓ System Integrator – Cyber-protection integration into existing or new solutions.
- ✓ Services Provider – Data migration, legacy data conversion to WORMdisks™.
- ✓ Other – Survivable systems & survivable data against viruses, malware & cyber-attacks.

Specific, unique products & services that we provide:

Write Once Read Many (WORM) hard disk drives are a unique, easy to use technology that protects both systems and data from malicious cyber-attacks. This technology, called CYBERdisk™ and WORMdisk™, protects the Master Boot Record (MBR) and partition tables on the OS boot disk from malicious cyber-attacks, prevents firmware viruses, prevents data sabotage, manipulation, deletion and reformatting, and protects against crypto viruses like Ransomware.

The technology uses standard interfaces, is plug-and-play, and is used like standard disk drives. It is Technical Readiness Level 9 (TRL 9), TAA compliant (made in the USA), has been deployed in government, commercial and financial applications and is available on several GWAC contract vehicles.

We would like to bring awareness to Government agencies that this technology exists today to defend our national IT assets against cyber-attacks. It is simple to use, and works like a typical disk drive with Windows, Linux and Mac systems.

This innovative approach protects data and systems by embedding the security where it belongs, at the lowest level, inside of the disk hardware itself, and it cannot be bypassed. They provide the Last Line of Defense to

protect sensitive data and the OS from cyber-attacks, at the core level, within the disk hardware, are OS independent and access permissions independent and the protections are always within the disk.

- **Survivable Systems = CYBERdisks** to protect sensitive parts of the OS boot disk from MBR, partition table and firmware cyber-attacks.
- **Survivable Data = WORMdisks** to protect static data files and critical data from sabotage, manipulation, deletion, re-formatting, Ransomware, firmware and data directed cyber-attacks.

Specific challenges that our products & services solve:

CYBERdisks™ and WORMdisks™ immediately benefit Government Information Technology applications that need their data or systems to be protected from cyber-attacks, insider threats, or accidental deletion caused by human errors.

Key advantages:

- Immediate and constant system and data defense against cyber-attacks and insider threats.
- Hardware security, not dependent on host, operating system, access controls or software, and cannot be circumvented.
- Easy to use like any other disk, it shows up as the C: or D: drive or as a mount point.
- Uses standard applications, supports standard file systems, native file formats, drag-and drop.
- Plug-and-play, may be a local SATA disk to a motherboard, or Host Bus Adapter (HBA), external USB, or network shared with standard NFS, CIFS, Samba, iSCSI protocols and interfaces.
- Data protection may be temporary in the case of frequent updates, or permanent with incremental enforcement, or the entire disk may be permanently locked for static data files.
- Instant full disk data lock down in the event of a cyber-attack detection on dynamic data files.
- Typical data encryption may prevent unauthorized disclosure, but it does not prevent re-encryption by crypto-viruses, data deletion, or disk re-formatting. WORMdisk technology couples with FIPS 140-2 encryption to protect data from disclosure AND to protect data from sabotage, manipulation and deletion. This is the only technology that can do both.
- Prevents Ransomware and firmware viruses which are nearly impossible to detect with AntiVirus tools.
- Supports online/offline/nearline/archive capabilities. Up to 100 year data shelf life.

Value that our products & services bring to the Government:

Specific use case examples include: Sensors and Intelligence Collections, Combat Support Systems, Communications Systems, Air, Ground & Sea Defense Systems, Forward Operating Base (FOB) Deployments, DoD 5015.2 Electronic Records Compliance, Regulatory Compliance, Logistics & Supply

Chain, Command and Control Systems, Industrial Control Systems, Acquisition Systems, Personnel Records, Medical Systems and Devices, Training Reference Material, Mobile Cloud–based Systems, Utilities and Power Grid, and Financial Infrastructure.

Current clients and deployments:

- **DISA:** Tech presentations to DISA CTO, DISA Cyber Risk Manager & DISA Infrastructure Executive. Sponsored for DISA CIO Technical Exchange meeting. DISA tested WORMdisks™ and CYBERdisks™ and DISA concluded that the products perform as advertised, and they were not able to change any data promised to be unalterable.

- **NIST:** GreenTec's technologies have been selected as a component in the NIST National Cybersecurity Center of Excellence (NCCoE) Data Integrity Project.

- **DHS:** Discussions with cyber groups to integrate our technology to protect audit log files for intrusion detection systems, and to help protect against election fraud with voting machines.

- **NIAP:** Working with the National Information Assurance Partnership (NIAP) to obtain Common Criteria Evaluation & Validation Scheme (CCEVS) certification.

- **U.S. Department of Justice (DOJ):** Thousands delivered for digital evidence collection for video surveillance.

- **Dell Solution Center (DSC) in Reston:** WORMdisks™ integrated and tested in Dell Generation 13 and Generation 14 server products.

- **Rosenthal Collins Brokerage Firm:** Deployed for protection of financial broker transactions.

- **Presidential Bank:** Financial data to be used for permanent records and email retention.

- **U.S. Bureau of Prisons:** To create permanent record of conversations for their deaf/mute prisoners.

- **Exxon Mobile:** For distribution of their software to ensure no viruses are injected.

- **Washoe County:** Conversion of their deteriorating microfiche land and tax records to be stored online on protected media.

- **DIGISTOR**: Partner for video surveillance applications.

- **Alcatel-Lucent:** Permanent long-term data storage retention.

- **Veterans Affairs:** Working with VA for Proof of Concept for 5 projects.

Our products are available on the following GWAC contract vehicles:

GSA Schedule 70, NASA SEWP 5, VA T4, CIO-CS

What is the competition for WORM technology?

For Write Once Read Many (WORM) technologies, on the low end DVD/CDROM are low-cost, readily available WORM technologies but are low-density and very slow. It is impossible to search 6TB of data on a DVD which would span over 1,200 DVDs, as compared to a single high-speed 6TB hard disk drive.

On the high-end, there are write protect WORM appliances (e,g. EMC Centera), that are software-based with vulnerable software controlling write permissions. They are very expensive, complex to use, have a history of being hacked and bypassed, and you need the entire appliance to protect your data. Further, you can remove disks from that appliance, re-format them and you have lost all of your data.

WORMdisks™ are the only hard disk drive technology that protects data at the hardware-level, are simple to use, protects from data sabotage, manipulation, destruction, re-formatting, crypto viruses (e.g. Ransomware), firmware viruses and other cyber-attacks and human error. They may be used as internal, external USB, or network shared storage.

CYBERdisks™ are the only hard disk drive technology that protects the OS boot disk's Master Boot Record (MBR) and partition tables from dangerous attacks like those that crippled Sony and Aramco Oil. Both CYBERdisks and WORMdisks also protect against firmware viruses.

Distinguishing features of our technology from the competition:

CYBERdisks™ & WORMdisks™ protect data against sabotage, manipulation, modification, deletion or re-formatting with security built into the disk itself. The security protection cannot be bypassed and it travels with the disk, regardless of operating system used or access permissions. Capacities scale from a single 500GB WORMdisk™, up to multiple Petabytes. They are available as internal disks, USB/eSATA external disks, or rack mount WORMdisk™ Storage Servers.