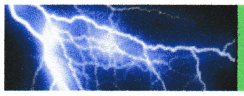
Technology
PowerArmor
SiSMART
SolidStor
SiSecure
LifeEST
Applications
Automotive
Data Center
Industrial
Interactive Kiosk
Medical
Military
Netcom
Video Surveillance
VoIP & Streaming Media
Select a Drive



PowerArmor
Eliminates the number one cause of field failures

Eliminate the number one cause of field failures - With patented technology deployed in thousands of OEM applications globally, PowerArmor® is field-proven to eliminate the number one cause of storage system field failures - drive corruption from an ungraceful power-down, brownout, power spike or unstable voltage level.

When power goes out, the result is often a corrupted drive and ruined data, resulting in costly unscheduled downtime as field technicians reformat drives, reinstall operating systems or return products.

Prevent drive corruption and lower the total cost of ownership - PowerArmor technology lowers the total cost of storage ownership by offering designers a time-proven solution that virtually eliminates the costly problems associated with drive corruption.

WhitePaper:
Eliminating Drive Corruption from Power Disturbances

How PowerArmor Works

Approximately three out of every four drive field failures are the result of power-related corruption. This means that brownouts, blackouts and even lightning strikes all contribute to the number one cause of RMAs among embedded systems storage.

In PATA Interfaces

PowerArmor incorporates voltage-detection circuitry, which serves as an early warning system against any unexpected deviation in the system's power supply. When a power fluctuation or interruption is imminent, the drive ceases its read/write function and instead transmits a busy signal to the host system. This assures no additional commands are received by the host until power levels normalize.
Address lines are latched, to make sure that all data is written to the proper location. This is a significant improvement over microcontroller-based flash cards, wherein address lines can drift and inadvertent writes can overwrite the operating system, file allocation table (FAT), master boot record (MBR), user data file or other critical file. Often, this happens when the power drops below the minimum operating level for the host while there is still enough power to power the solid-state drive. When this happens, the data "spills over" to other locations. The result is data is corrupted and/or the drive may not boot up on subsequent use.

In SATA and USB Interfaces

With a serial connection, the address is known before the data is even transmitted, so there is no need to latch the address lines. When the built-in PowerArmor detection circuitry detects a change in the voltage level, the drive signals the host system to stop transmitting data, suspending the host from sending and receiving any more data. The drive then finishes writing the remaining data and gracefully powers down. When power levels return, the drive powers back up normally and resets.

Conclusion

PowerArmor is completely transparent to the host system, and its function does not detract from system performance. This means that it works automatically and seamlessly, without the need to manually run scanning and recovery operations.

With its integrated voltage detection technology, PowerArmor eliminates drive corruption in the event of a power disturbance. Over the deployment cycle of the drive, this significantly reduces maintenance, warranty and other unscheduled downtime costs.

Technology

PowerArmor

SiSMART

SolidStor

SiSecure

LifeEST

Applications

Automotive

Data Center

Industrial

Interactive Kiosk

Medical

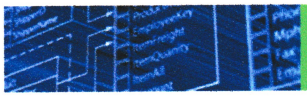
Military

Netcom

Video Surveillance

VoIP & Streaming Media

Select a Drive



SiSecure
Protects application data and software IP

Security breaches are rising - Pfizer, Agilent Technologies, Deloitte & Touché and the United States Air Force all have something in common - they all suffered theft of confidential personal, employee, and military information last year. In fact, in 2007 there were over 300 documented security breaches. www.datalossdb.org

Embedded system OEMs have greater challenges now than ever before to build robust security options into their products.

Protect application data and software IP - Integrated into every SiliconDrive SSD, SiSecure protects application data and software IP from theft, corruption, and accidental or malicious overwrites.

The user-selectable security options in SiSecure are ideal for applications requiring advanced levels of security such as data recorders, wearable and field computers, medical monitoring and diagnostic equipment, POS systems and voting machines.

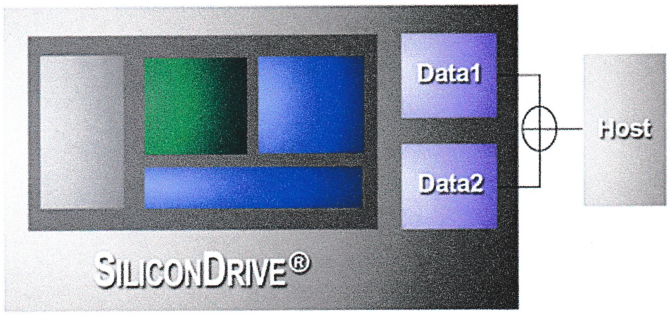
Discover more about SiSecure

- Security options for the toughest deployments
- Discover more about SiSecure technologies
- Confidential data protection
- Access control and permissions selection
- Multiple security zone creation

Security options for the toughest deployments:

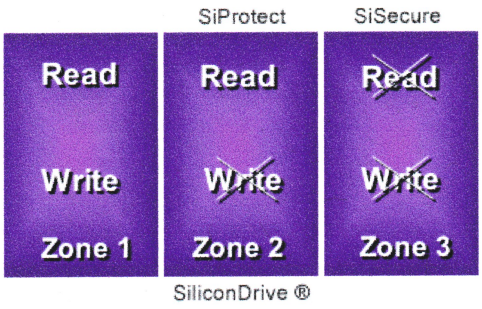
SiKey™ Ties SiliconDrive to a specific host and/or software IP

SiKey Software IP and Application Data Tied to a Specific SiliconDrive



- Host reads secure data through vendor-specific commands
- Data1 confirms the product is a SiliconDrive
- Data2 identifies the specific SiliconDrive
- Host uses this data to create encryption keys or other unique identifiers

SiZone™ Data zones with different security parameters



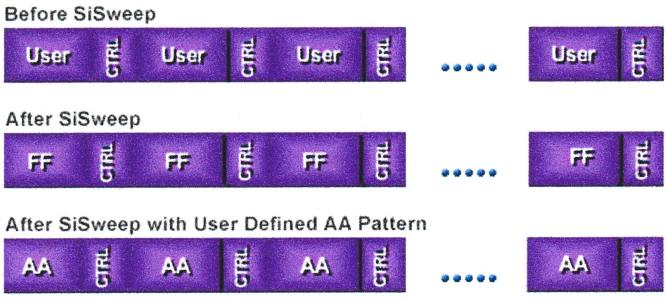
SiProtect™ Software for read-only or password-required read/write access

SiSweep™ Ultra-fast data erasure

Sectors: USER = UserData
CTRL = ECC, Bad Block and Other Information

Sectors: USER = UserData
CTRL = ECC, Bad Block and Other Information

SiScrub™ Ultra-fast data erasure followed by a programmed pattern



Sectors: USER = UserData
CTRL = ECC, Bad Block and Other Information

Ask yourself these questions: Would it be valuable to set your drive to be usable only on the originally intended host system? What about the value of securely storing an operating system and data on the same drive to cut storage costs?

Discover more about SiSecure technologies

Application data and software IP theft prevention - Patent-pending SiKey ties application data and software IP to a specific SiliconDrive to prevent unauthorized duplication.

Unlike consumer applications where security needs to be implemented in the removable device because the data must be available on multiple host platforms, security for OEM storage is tied to the host system which verifies the drive and creates unique encryption keys to prevent theft. If the storage device is removed from the original system, the data is rendered unreadable.

Tying security to the host system is especially useful to companies that routinely ship software IP upgrades that could be vulnerable to theft and to prevent security breaches such as the theft of flash cards containing sensitive information.

Example: A voicemail system provider sells software upgrades to either increase the number of users, or provide some type of system level improvement. The upgrade is shipped on SiliconDrive as a "kit." The voicemail system provider wants to ensure that the software is tied only to that specific SiliconDrive so that even if the software is copied onto another device, it will not work properly in the host system.

Confidential data protection

Patent-pending SiSweep, SiScrub and SiPurge rapidly and completely remove data to prevent sensitive data from falling into the wrong hands.

Applications include data recorders, medical and diagnostic equipment, POS systems or voting machines where data must be rendered unreadable by anything other than the original host system.

Technology	Descripition	Drive Reusable
SiSweep	Ultra-fast data erasure	Yes
SiPurge	Non-recoverable data erasure	No
SiScrub	Ultra-fast data erasure followed by a programmed pattern	Yes

Access control and permissions selection

In applications such as mobile, portable, wearable or handheld computers, patent-pending SiProtect works to prevent unauthorized access and/or unauthorized changes to data or files.

SiProtect employs software write protection for read-only access to prevent accidental or malicious overwrites or data tampering. In addition, SiProtect allows users to block unauthorized access to an entire drive by establishing a required password for read/write access.

Multiple security zone creation

Patent-pending SiZone enables every SiliconDrive to have up to five independent security zones with different security parameters for ultimate protection.

For example, application data, software IP and lookup tables can be stored in separate zones with different security parameters. Products such as wearable or field computers, industrial PCs or network security appliances can store sensitive data, databases, mission or patient data independently in each zone, providing maximum protection while decreasing costs by eliminating unnecessary storage devices.

Example: A gaming OEM manufactures video poker machines that use SiliconDrive as the storage technology. The machine has three different storage requirements, one to store and manage specific validation codes required by regulatory agencies, a second to store the game and its associated graphics images, and a third to provide player tracking statistics for casino marketing programs. Previously, the OEM needed three different storage products to accomplish this task, a secure EPROM for the validation codes, a CD-ROM for read-only access to the game itself, and a flash card for player tracking. All three requirements can now be satisfied by one SiliconDrive - with zone one implementing SiProtect to provide restricted access to the validation codes, and in zone two to provide read-only access to the game, and zone three to allow full read and write access to monitor player tracking.

Each zone can be configured with any combination of SiSweep and SiProtect.