"Tying storage security to the host system is a real concern for enterprise system applications. SiSecure was developed to allow host system manufacturers to maintain ultimate control to protect data and prevent theft."

Chris Kissel, Semiconductor Research Analyst, In-Stat
EXECUTIVE SUMMARY

Embedded devices have traditionally had limited security features. The small size of most embedded devices prevents extensive security features from being implemented, which is a big problem for Enterprise System OEMs who require data be rendered unreadable in the advent of a security breach. With Enterprise System OEMs, the host system must maintain ultimate control over security algorithms.

SiliconSystems has developed a comprehensive solution called SiSecure. With SiSecure, application data and software IP are tied to a specific drive, which means the host system can verify the drive and create unique encryption keys to prevent theft.

Confidential data can be removed at several levels, from ultra-fast data erasure to complete destruction of the master boot records, file allocation tables (FATs), or even the drive itself.

Write protection can be set up for read-only access, and password protection is available for read/write access. Design engineers can define up to five independent security zones with different security parameters for protection and flexibility.
**TABLE OF CONTENTS**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td>Background</td>
<td>2</td>
</tr>
<tr>
<td>SiSecure</td>
<td>3</td>
</tr>
<tr>
<td>Benefits</td>
<td>3</td>
</tr>
</tbody>
</table>

**INTRODUCTION**

SiSecure combines all the high-performance, high-reliability, and multi-year product lifecycle benefits of the standard SiliconDrive with a comprehensive suite of patented and patent-pending technologies that provide multiple security options to safeguard application data and software IP in embedded systems. Combined with SiliconSystems’ patented PowerArmor and SiSMART technologies, SiSecure provides the most secure, robust, and scalable storage platform for the most demanding embedded applications.

Applications requiring advanced levels of security, such as data recorders, wearable and field computers, medical monitoring and diagnostic equipment, POS systems, and voting machines are able to activate features such as ultra-fast data erasure and sanitization, data zones with independent security parameters, and secure areas for OEMs to access and create their own encryption/decryption keys. SiSecure protects application data and software IP from theft, falling into the wrong hands from deployments in high-risk areas, corruption, and accidental or malicious overwrites.

**BACKGROUND**

Historically, embedded devices have had limited security options available because of the engineering obstacles of designing robust security features into the small mechanical footprints required for embedded systems. Challenges such as storage components, processing power, battery life, and time-to-market and overall cost concerns, have limited many security features from being implemented in hard drives and traditional flash cards.
The security industry has focused on portable storage devices for the consumer electronics industry for users who want the security algorithm to travel with the storage device (such as, a USB thumb drive). This technology allows the user to protect and use the data on any system, whether it is an office PC, home computer, Internet kiosk, or other public computer. Software applications and user data are encrypted and password-protected using industry-defined security protocols, which become targets for Internet hackers.

Enterprise System OEMs operate under a different premise. Data must be rendered unreadable if the storage devices are removed from the systems for which they were intended. Highly-visible security breaches, such as a flash card with sensitive military documents being found in a bazaar in Bagram, Afghanistan, have become more prevalent as more and more embedded devices handle sensitive data.

In the Enterprise System OEM market, the host system must maintain ultimate control over security algorithms to protect data and prevent IP theft. These algorithms can be as simple as ensuring that the correct storage product is in the host, or as intricate as tying the software IP and application data directly to the storage device.

**SiSecure**

SiSecure is a comprehensive solution that overcomes the design challenges and performance trade-offs in hard drives and traditional flash cards to deliver an unprecedented level of embedded storage system security. SiSecure enables designers to easily integrate security to guard against critical data from falling into the wrong hands and software IP theft. In addition, SiSecure integrates a suite of low-level, SiliconSystems-specific commands that can be used by the host to create a completely proprietary, highly-configurable security algorithm.

SiSecure increases storage system flexibility, while decreasing cost by eliminating the need for storing information on multiple platforms based on security requirements. Benefits to OEMs include IP theft prevention, new market opportunities, and being able to capture untapped revenue streams and enhanced product differentiation.

**Benefits**

**Application Data and Software IP Theft Prevention**

SiliconSystems’ customers want to perform two key functions in their application to protect application data and software IP. First, there is a need to ensure that the end customer is using a qualified storage device in the system. In some instances, perhaps for warranty or service purposes, the OEM needs to know that the specific SiliconDrive originally shipped with the equipment is indeed still in the system. Second, there is a need to tie specific application data and software IP to the specific SiliconDrive for which it is intended to prevent theft and ensure software integrity.
SiKey ties application data and software IP to a specific SiliconDrive so that the host system can verify the drive and create unique encryption keys to prevent theft. With SiKey, any application that ties storage to the host system, such as companies that routinely ship software IP upgrades, can select the right level of advanced security to prevent theft.

**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 the 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 does not work properly in the host system.

Through the use of the SiKey technology and a SiliconSystems-specific command, the host can read two unique pieces of data that can be used for validation. The first data string identifies the product as being a SiliconDrive, and the second data string identifies the specific SiliconDrive. The host system can then use that data to create encryption/decryption keys for software IP and application data. While this method does not provide copy protection, it does inhibit the use of the particular software on any system other than the original host.

![Figure 1: SiKey](image)

**Figure 1: SiKey**
CONFIDENTIAL DATA PROTECTION

Applications requiring advanced levels of data security in high-risk environments, such as data recorders, wearable and field computers, medical monitoring and diagnostic equipment, POS systems, and voting machines, can employ SiliconSystems' patent-pending SiSweep, SiScrub, and SiPurge. These technologies rapidly and completely remove data from the SiliconDrive and prevent sensitive data from falling into the wrong hands.

These data security features can be initiated in two ways:

- Via software through a two-level command structure that greatly decreases the probability of initiating the functions inadvertently.
- Through an optional hardware initiation, like a switch or a push-button.

SiSweep

As illustrated in Figure 2 on page 5, the SiSweep function completely erases all data fields in the SiliconDrive. As a result, all user data, master boot records (MBR), and FATs are destroyed. While the actual recovery procedure is highly application-dependent, a functional equivalent of the following process is required to recover or re-use the SiliconDrive after the SiSweep command has been executed.

1. FDISK. This command re-creates the MBR and partition information.
2. FORMAT.
3. RE-LOAD. This command reloads the operating system and application data.

![SiSweep Figure 2](image-url)
Figure 3 and Table 1 on page 6 illustrate the benefit of SiSweep as an alternative to using standard ATA commands to erase/overwrite a SiliconDrive. For a 16GB SiliconDrive, sweep time is reduced from just under 44 minutes to just under 15 seconds. Figure 4 on page 7 shows that the effective data sweep rate of a SiliconDrive can exceed 1GBps.

![SiSweep Speed Benefit](image)

**Figure 3: SiSweep Speed Benefit**

**Table 1: Data Sweep Times in Seconds**

<table>
<thead>
<tr>
<th>Capacity</th>
<th>SiSweep</th>
<th>Standard ATA Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>32MB</td>
<td>3.4</td>
<td>5.2</td>
</tr>
<tr>
<td>64MB</td>
<td>5.9</td>
<td>10.4</td>
</tr>
<tr>
<td>128MB</td>
<td>2.8</td>
<td>20.7</td>
</tr>
<tr>
<td>256MB</td>
<td>3.3</td>
<td>41.4</td>
</tr>
<tr>
<td>512MB</td>
<td>4.9</td>
<td>82.9</td>
</tr>
<tr>
<td>1GB</td>
<td>5.9</td>
<td>166.5</td>
</tr>
<tr>
<td>2GB</td>
<td>6.8</td>
<td>333.5</td>
</tr>
<tr>
<td>4GB</td>
<td>8.3</td>
<td>671.5</td>
</tr>
<tr>
<td>8GB</td>
<td>13.8</td>
<td>1343.9</td>
</tr>
<tr>
<td>16GB</td>
<td>14.7</td>
<td>2621.7</td>
</tr>
</tbody>
</table>
SiPurge takes SiSweep one step further by not only eliminating all user data, MBRs, and FATs, but also by erasing control blocks and SiliconDrive firmware, as shown in Figure 5. SiPurge is a non-recoverable operation, which means the SiliconDrive cannot be re-used after this command is executed.
Figure 5: SiPurge
**SiScrub**

SiScrub is a command created to allow SiliconDrive to be used as a drop-in replacement for magnetic hard drives in applications that require multiple write/erase cycles before the drive is deemed “sanitized” or “scrubbed.” It is generally well-known that ghost images can still reside on the magnetic media of hard drives, even after an erase. Writing and erasing multiple times eliminates this issue. In solid-state drives, an erase is actually a write of all zeros followed by a write of all FFs, which in itself is a “scrubbing” methodology. SiScrub is not technically required to completely sanitize the SiliconDrive, but may still be needed if the customers do not want to re-write their requirements based on the move to solid-state.

![SiScrub Diagram](image)

**Figure 6: SiScrub**

**Access Control and Permissions Selection**

SiliconDrive with SiSecure integrates a set of proprietary commands that allow the host system to set, change, or delete a unique password that locks and unlocks the data space of a SiliconDrive. These features have been found to be highly effective in safeguarding against illegal spying or piracy of sensitive information.
SiPROTECT

SiProtect enables the user to block unauthorized access to an entire drive by establishing a required password for read/write access.

Figure 7: SiProtect — Password Required
SiProtect also employs software write protection for read-only access to prevent accidental overwrites or data tampering.

![SiProtect](image)

**Figure 8: SiProtect — Read-Only Access**

**Multiple Security Zone Creation**

SiliconSystems' patent-pending SiProtect and SiSweep are security technologies which, when used by themselves, allow the user to adjust the security parameters of the entire SiliconDrive.

**SiZone**

SiZone allows the design engineer to define up to five independent security zones with different security parameters for ultimate protection and flexibility. This is especially important in applications such as wearable computers or industrial PCs, where application program information, sensitive documents, and classified data can be stored independently with unique security parameters.

**Example**

A gaming OEM manufactures video poker machines that use a SiliconDrive with SiSecure as the storage technology. The machine has three different storage requirements:

- One to store and manage specific validation codes required by regulatory agencies.
- One to store the game and its associated graphics images
- One 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.
- A flash card for player tracking.

All three requirements can now be satisfied by one SiliconDrive with SiSecure:

- Zone one implementing SiProtect to provide restricted access to the validation codes.
- Zone two implementing SiProtect to provide read-only access to the game.
- Zone three to allow full read and write access to monitor player tracking.

SiZone is enacted by a series of SiliconSystems-specific commands that enable the user to:

- Define up to five zones
- Define and change the following for each zone:
  - Beginning and ending logical block addresses
  - Password (though the use of the SiProtect command)
  - Security:
    - Unprotected = full read and write access
    - SiProtect = read-only access or no access without a password
    - SiSweep = ultra-fast data erasure

### SiSecure Technologies

<table>
<thead>
<tr>
<th>Technology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SiKey</td>
<td>Ties the SiliconDrive to a specific host and/or software IP.</td>
</tr>
<tr>
<td>SiZone</td>
<td>Data zones with different security parameters.</td>
</tr>
<tr>
<td>SiSweep</td>
<td>Ultra-fast data erasure.</td>
</tr>
<tr>
<td>SiScrub</td>
<td>Ultra-fast data erasure followed by a programmed pattern.</td>
</tr>
<tr>
<td>SiPurge</td>
<td>Non-recoverable data erasure.</td>
</tr>
<tr>
<td>SiProtect</td>
<td>Protection software for password-required, read/write, or read-only access.</td>
</tr>
</tbody>
</table>

Each zone can be configured with any combination of SiSweep and SiProtect, or the zone can have full read/write operation, providing the ultimate in protection and flexibility.
SiliconDrive with SiSecure also includes the following SiliconSystems’ base technologies:

- PowerArmor, which eliminates drive corruption
- SiSMART, which calculates remaining useful life

**RELATED INFORMATION**

All SiliconSystems’ security technologies are easy to implement and integrate into the host application software. User-defined security applications can be created around these custom commands with complete flexibility as to what specific technologies are implemented in the final application. Application notes detailing the exact implementation of the proprietary SiSecure commands are available under the NDA from a SiliconSystems’ Field Application Engineer.
SiliconSystems’ performance tests, ratings, and product specifications are measured using specific computer systems and/or components and reflect the approximate performance of SiliconSystems’ products as measured by those tests. Any difference in system hardware or software design or configuration, as well as system use, may affect actual test results, ratings, and product specifications. SiliconSystems welcomes user comments and reserves the right to revise this document and/or make updates to product specifications, products, or programs described without notice at any time. SiliconSystems makes no representations or warranties regarding this document. The names of actual companies and products mentioned herein are the trademarks of their respective owners.

SiliconSystems®, SiliconDrive®, SiliconDrive II®, SiSecure™, PowerArmor™, SiSMART™, SiKey™, SiZone™, SiProtect™, SiSweep™, SiPurge™, SiScrub™, SiliconDrive USB Blade™, and the SiliconSystems logo are trademarks or registered trademarks of SiliconSystems, Inc. and may be used publicly only with the permission of SiliconSystems and require proper acknowledgement. Other listed names and brands are trademarks or registered trademarks of their respective owners.

© Copyright 2008 by SiliconSystems, Inc. All rights reserved. No part of this publication may be reproduced without the prior written consent of SiliconSystems.