

WHITE PAPER

Phoenix ™

Secure from the START

Phoenix Core Managed
Environment



Table of Contents

1.0	Introduction	1
2.0	Why learn about FirstWare	1
3.0	Customer benefits	1
4.0	Phoenix's opportunity	1
5.0	FirstWare basics	1
6.0	Accessing the FirstWare space	2
7.0	FirstWare - A closer look	3
8.0	Phoenix CME console - the FirstWare GUI	4
9.0	Phoenix FirstWare Applications	4
10.0	Summary	5

1.0 Introduction

This White Paper is your first step towards learning how you can take advantage of Phoenix Technologies' cME (Core Managed Environment). This paper describes the basics of FirstWare and explains how to enable the FirstWare Space, which is Phoenix's cME-enabled host protected area. This paper specifies hard disk requirements, as well as FirstBIOS and FirstDisk requirements to protect and access the FirstWare Space. Finally, it provides information on each of Phoenix Technologies' FirstWare applications, which reside in the FirstWare Space.

2.0 Why learn about FirstWare?

Phoenix Technologies' FirstWare environment is best described as a "bomb shelter" within the PC. The environment protects important data from disaster and provides a tamper-proof environment for applications that are always available—even when the primary operating system is damaged or missing.

3.0 Customer benefits

With Phoenix cME, users can access diagnostics and self-healing capabilities, Internet access, and remote desktop builds, even after a major malfunction. Phoenix cME enables the creation and management of a secure "host protected area" (HPA) of the hard drive, where Phoenix cME Certified applications reside—the Phoenix FirstWare™ product family. These applications help diagnose and recover PCs if the operating system malfunctions and the applications are stored in a trusted environment embedded securely in the system. A future release will enable third-party developers to write their own applications for storage in this tamper-proof area. For more information, see the Phoenix cME FAQ at http://www.phoenix.com/resources/phoenix_cme_faq.pdf.

4.0 Phoenix's opportunity

Phoenix is uniquely positioned to address customer needs. Our product offering is leading the industry, incorporating the latest standards and most advanced technology, supplemented by unique enhancements. In addition, our products offer OEMs and System Builders the ability to create a dedicated, protected area of the hard disk drive. Since access to this "bomb shelter" section of the drive is tightly controlled by our Phoenix FirstBIOS architecture, a user's system

can be quickly restored to its original OEM status, should the integrity of the drive's contents be compromised.

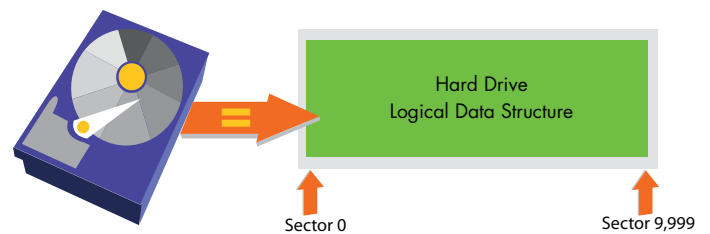
5.0 FirstWare basics

The FirstWare Space provides advanced pre-OS capabilities to end users; it enables them to access data, information, and programs securely. The FirstWare Space creates a trusted environment embedded securely in the system for not only pre-OS FirstWare Applications, but also data accessible from the FirstWare Applications running on the host operating system. Because FirstWare is dependant on the hard drive on which it is stored, a basic understanding of hard drives will help you understand FirstWare.

5.1 Hard drive basics

Usually, all of the data stored permanently on a computer is stored on a hard drive. The logical storage blocks are presented to the BIOS in a linear fashion from a storage address of 0 all the way up to a number that represents the physical limits of the drive, as shown in Figure 2. The drive's firmware handles all data transfers between the drive components themselves and the rest of the system.

Figure 2 The hard drive logical data structure



5.2 Enabling the FirstWare Space

The FirstWare Space is Phoenix's implementation of the host protected area (HPA), as first defined in the ATA-5 specifications. Basically, it is a protected area of the hard drive reserved for storage of critical data and applications in a container segregated from the rest of the hardware by an internal "firewall" of sorts. This area can be accessed even when the primary OS is not functional; however, it is completely secured and inaccessible to viruses and corruption during normal operations.

This protected storage area is accomplished through the use of an ATA command called SETMAX. Issuing a SETMAX command to the hard drive allows the drive to report to the rest of the system that its maximum storage address (reported max) is lower than its actual physical storage limit (native max), as shown in Figure 3.

Figure 3 Hard drive vertical data structure—with FirstWare Space



When the reported max is lower than the native max, the storage areas on the drive between the reported max and the native max are made secure and inaccessible to the rest of the system. This protected storage area is the FirstWare Space.

For FirstWare to function, the computer's hard drive must be ATA-5 compliant. The drive must also support ATA security extensions. FirstWare cannot be installed on SCSI drives or older ATA drives. The FirstWare package includes a DOS application called the FirstWare Hard Drive Compatibility Checker, which checks drives for compliance to the ATA-5 specifications.

6.0 Accessing the FirstWare Space

The FirstWare Space is usually accessed at boot time through a keystroke—typically the ALT key—during the POST (Power on Self-Test). When the key is pressed, the FirstWare Space is opened and the first Service Area (Phoenix cME Console) in the FirstWare Space is booted.

To access the FirstWare Space, it is necessary that the computer be equipped with either FirstBIOS or FirstDisk, explained in the following sections.

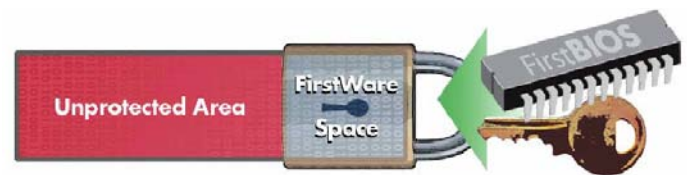
6.1 FirstBIOS and FirstBIOS Pro

FirstBIOS and FirstBIOS Pro are the new Phoenix Technologies versions of BIOS (Basic Input/Output System) that utilize FirstWare technology. They allow secure access to the FirstWare applications through a graphical interface, the Phoenix cME Console. These new

BIOS versions enhance the efficiency and speed of the BIOS Power on Self-Test (POST) and control all access to the FirstWare Space. When the FirstWare Space is locked down, an internal access password is used, and that same password is needed to open the FirstWare Space.

When a computer is equipped with FirstBIOS, the BIOS holds the key to opening the FirstWare Space, as illustrated in Figure 4. Once the machine is committed and the FirstWare Space locked, only the BIOS can expose it, and the access password is changed with every opening and closing of the FirstWare Space. This is the best and most secure way to use FirstWare.

Figure 4 FirstBIOS—the key to the locked FirstWare Space



6.2 FirstDisk – FirstWare access for non-FirstBIOS systems

When a non-FirstBIOS motherboard is used, Phoenix Technologies' FirstDisk software must be installed on the target system to enable the FirstWare features in the system. FirstDisk provides the required initialization and runtime support for executing FirstWare applications in the FirstWare Space. With FirstDisk, FirstWare applications can run on any system regardless of the system or BIOS vendor. FirstDisk support is installed after you install the FirstWare applications.

FirstDisk is a small application that is installed into the boot track of the hard drive. When the system boots to the MBR (Master Boot Record), shown in Figure 5, FirstDisk is activated and waits for the necessary keystroke (ALT) to activate FirstWare. If the key is not pressed, booting proceeds normally. If the key is pressed, FirstDisk launches into the FirstWare Space.

Figure 5 FirstDisk access to the locked FirstWare Space



FirstDisk uses the MBR on the hard drive to control access to the FirstWare Space. While the FirstWare Space is always protected from viruses, hackers and other disasters, problems with the exposed MBR can render the FirstWare Space inaccessible until the MBR is repaired. FirstBIOS is the most reliable way to use FirstWare. Since the access is controlled by the BIOS, it is always available and does not have problems with drive corruption.

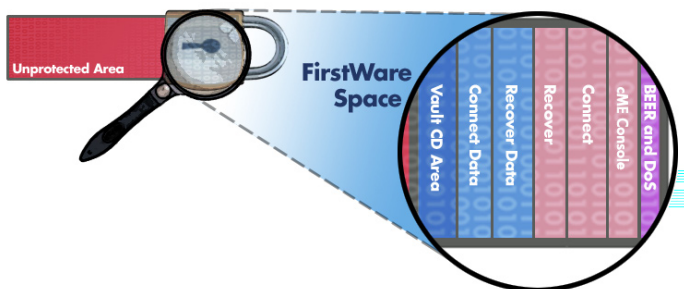
7.0 FirstWare – A closer look

So far we have been looking at FirstWare as a whole, but the real functionality of FirstWare lies in the layers of functionality that you can build into it. This section gives you a closer look inside the FirstWare Space.

7.1 Service Areas

The FirstWare Space is divided into multiple sections. Each section is called a Protected Service Area or simply Service Area. In Figure 6, all the “magnified” sections—except the BEER (BIOS Engineering Extension Record) and DoS (Directory of Services), which comprise the index—are Service Areas.

Figure 6 The FirstWare Space Service Areas and index



A Service Area is to the FirstWare Space as a partition is to main area of the hard drive. Like a partition, a Service Area can be bootable or simply contain data. A Service Area may contain:

- A FirstWare application
- Data files for a FirstWare application
- CD content that is accessible from Windows using FirstWare Vault

A maximum of 13 Service Areas can be contained in the FirstWare Space.

7.2 Protected Service Area (PSA) files

A PSA file is a file that contains all the contents, properties, and boot files for a Service Area. FirstWare Builder is a tool used by OEMs and System Builders to import PSA files into the FirstWare Space as Service Areas. A PSA file has the file extension .psa and can be stored on any network share or standard Windows file system.

7.3 The Directory of Services (DoS)

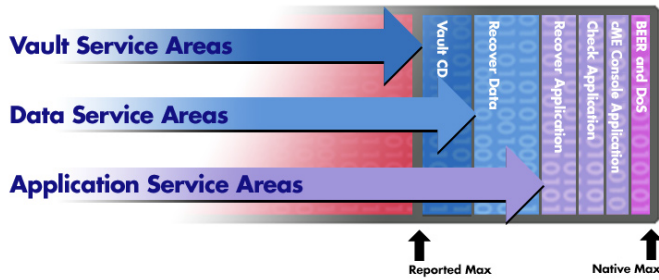
The DoS is located at the end of the FirstWare Space and is the table of contents for the FirstWare Space. Every available Service Area in the FirstWare Space will have an entry in this DoS so that the Phoenix cME Console can quickly access the size, location and parameters for each Service Area. The Phoenix cME Console is the GUI interface that acts as the FirstWare “desktop” when FirstWare is first launched.

7.4 Service Area ordering and security concerns

Although it is possible to load Service Areas into the FirstWare Space in any order, security concerns dictate that bootable Service Areas and signed application Service Areas be located at the end of the drive while data-only Service Areas such as Vault CD Service Areas be located toward the front of the drive.

This arrangement is recommended so that the data Service Areas can be made available from within Windows while maintaining the integrity and security of the application Service Areas. When these data Service Areas are located toward the front of the drive, as shown in Figure 7, FirstWare needs to expose only these data areas for the FirstWare applications running on Windows, thus leaving the bootable application Service Areas (e.g., Console, Check, and Recover applications) fully protected.

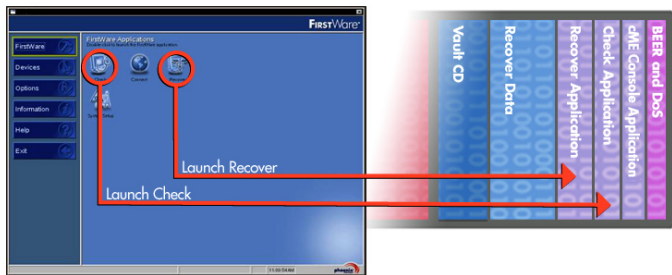
Figure 7 FirstWare security segmenting



8.0 Phoenix cME Console – The FirstWare GUI

As one of Phoenix Technologies’ FirstWare applications, the Phoenix cME Console is the graphical interface used to access other FirstWare applications or Service Areas that reside in the FirstWare Space. The cME Console window displays when end users press the designated FirstWare key during boot-up. As the primary interface for accessing services in the FirstWare Space, the cME Console must be installed as the first Service Area in the FirstWare Space. The cME Console presents a menu of FirstWare applications and offers other options, such as a choice of language for the interface.

Figure 8 Phoenix cME Console screen—launching FirstWare applications



Because FirstWare always boots to the first Service Area and the cME Console is the only means to access the other Service Areas, CME Console must be installed as the first Service Area in the FirstWare Space.

9.0 Phoenix FirstWare applications

This section describes the current FirstWare applications offered by Phoenix Technologies. Because Phoenix has designed the FirstWare

Space with an open architecture, other third-party applications will become available in the future. All FirstWare applications are installed by OEMs and System Builders with the FirstWare Builder utility. Because of the nature of the FirstWare Space—a secure area that cannot be tampered with, the ability to make any changes to FirstWare Space contents is limited to the OEM or system builder creating and populating the FirstWare Space. The FirstWare Space is not designed for use as a file system to be changed by end users or even IT personnel. It is an area to be defined and controlled only by OEMs and system builders. In this way, the integrity of the applications and data files installed in the FirstWare Space is maintained, and the purposes of the FirstWare applications described below are not compromised.

9.1 FirstWare Recover

FirstWare Recover lets end users quickly and easily restore the original factory image (including the OS and factory-installed applications) without a boot disk or recovery CD. Because FirstWare Recover is securely built into the PC, there is no need to ship recovery CDs. FirstWare Recover will restore the entire hard disk drive—or just the “C:” partition—to its original condition. Recover eliminates the need for costly system returns under warranty.

The recovery image stored in the FirstWare Space is created by OEMs or System Builders during manufacturing. Therefore, the image consists only of the original factory image, including the OS and factory-installed applications. There is no user backup capability to store any user data into the FirstWare Space today, because such capability could compromise the area.

FirstWare Recover has a non-destructive restore that will not overwrite user data if the PC’s hard drive has been set up with two or more partitions and users have stored their data files in the second (non-bootable) partition. Since Recover can restore either the entire drive or just one partition at a time, a System Builder or PC manufacturer can set up user data settings on a separate partition from the OS. Then Recover can restore only the boot partition containing the OS. There are some Recover image size restrictions involved in restoring a single partition.

9.2 FirstWare Vault

FirstWare Vault is a Windows application that accesses CD data placed in Vault Service Areas in the FirstWare Space. This lets you store CD content and special applications in highly compressed form.

The stored information is accessible to end users as a virtual CD within Windows, utilizing the special FirstWare Vault software. The raw data itself is invisible to Windows and immune to disk formatting and partitioning software. FirstWare Vault is the only FirstWare application that end users do not access from the CME Console. Phoenix provides the tools to import any CD image the PC manufacturer or system builder chooses during manufacturing. Therefore, the PC manufacturer or system builder must take responsibility for any licensing or copyright issues associated with distributing the contents of the CD application in the FirstWare Space.

Once the system is shipped, users cannot add or remove any factory-installed virtual CDs from the HPA in a FirstBIOS system. Although this limits flexibility, this ensures the greatest level of integrity and security. It also ensures that the user can access the CDs as intended by the manufacturer/system builder. A future release will allow the ability to remove virtual CDs without compromising security.

9.3 FirstWare Connect

FirstWare Connect is the first Internet “spare tire” for users. It is an emergency browser for the FirstWare Space. You can configure Connect so that it connects directly to your support site, even if Windows, or any other operating system, is not functioning. With this secure connection, end users can download OEM patches, updates, instructions, and special utilities—everything they need to troubleshoot and fix their problems.

9.4 FirstWare Check

In the event of a system failure, FirstWare Check gives end users a fast, easy-to-use, in-depth diagnostic tool that identifies hardware problems so that end users do not need to call technical support. If the problem turns out to be software-related, end users simply find their recovery CDs and re-image or reinstall their OS and software. Or better yet, they run FirstWare Recover and FirstWare Vault to restore the OS or factory-installed applications—without CDs.

10.0 Summary

With Phoenix Technologies’ FirstWare, a part of the Phoenix Core Managed Environment (cME), system builders and PC (and digital device) manufacturers can now offer their customers the next generation of PCs and digital devices. End users can have diagnostic, recovery, and Internet access tools available in a cME-protected area of their hard drives. This FirstWare Space, which is completely secure when used with a FirstBIOS motherboard, and which is easily accessible even after OS crashes, provides an innovative way to make end users’ lives easier and to differentiate manufacturer and system builder offerings. The raw data itself is invisible to Windows and immune to disk formatting and partitioning software. FirstWare Vault is the only FirstWare application that end users do not access from the CME Console.

Secure from the START

Phoenix Technologies is a global market leader in device-defining software that enables endpoint security from the start. The company first established dominant industry leadership over 25 years ago with BIOS software. From this unique foundation of core level expertise and firmware offering the highest levels of reliability, Phoenix has created a portfolio of innovative software products that simply and easily identify and restore devices, thereby assuring users unparalleled endpoint security and availability.

Phoenix Technologies Ltd.

915 Murphy Ranch Road
Milpitas, CA 95035 USA
408.570.1000 main
408.570.1001 fax

800.446.9202 North America sales
781-BUY PTEC Outside North America sales

©2005 Phoenix Technologies Ltd. Phoenix and Phoenix Technologies are registered trademarks of Phoenix Technologies Ltd. All rights reserved worldwide. All other brand or product names are the trademarks and property of their respective holders.

0000-XX000