ACER ProShield

Table of Contents
Revision History........................................................................................................3
Legal Notices ...........................................................................................................4
Executive Summary .................................................................................................5
Introduction ............................................................................................................5
Protection against unauthorized access .................................................................6
Why ACER ProShield ..............................................................................................7
ACER ProShield .....................................................................................................9
   Credential Manager ..............................................................................................9
   BIOS Settings .....................................................................................................10
   Data Protection ..................................................................................................11
   Data Removal .....................................................................................................14
   Remote Manageability .........................................................................................14
Frequently Asked Questions ..................................................................................16
Attachments ..........................................................................................................19
### Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1</td>
<td>09.09.2010</td>
<td>Roy Lin (#3574)</td>
<td>Initiation of white paper</td>
</tr>
<tr>
<td>V1.1</td>
<td>10.12.2010</td>
<td>Roy Lin (#3574)</td>
<td>Add HP comparison &amp; ProShield Key Diagram</td>
</tr>
</tbody>
</table>
Legal Notices

Information in this document is subject to change without notice. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Acer Inc.

Acer may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Acer, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2010 ACER INC. ALL RIGHTS RESERVED.
Executive Summary

ACER ProShield is a security and manageability tool at the heart of ACER security strategy for business notebooks and desktops. This single client console application integrates all security and BIOS under a common architecture and a single user interface. Many features are assembled under this common architecture building a vast client security center such as BIOS migration, data encryption, data removal, credential manager, and remote management. A range of optional innovative hardware securities are also included such as Trusted Computing Group (TCG) standards and Secure Encryption Drives (SED). The integration of these features is designed to address business customer need for better protection against unauthorized PC access. ACER ProShield will also provide stronger protection to data stored locally or accessed over the network.

Introduction

More and more people are using their computer for mobility and internet connection; this is causing an increase in data security threats. Business customers whose sensitive data will have a direct impact are increasingly worried about the health of their computer systems.

ACER begins to notice the growing data security trends and started to devote resources to solving this problem. Data security is not a problem that can be viewed as an individual part, but required it to be viewed along with the other components. ACER has built a solution that brings many technologies together that not only ensures the protection of the client devices, but also helps ensure that the client devices will not become the point of vulnerability that would threaten the entire IT infrastructure.

ACER’s proactive efforts have led to the development of ACER’s solution, ACER ProShield. ACER ProShield not only meets the above requirements, but also is scalable and able to manage new threats and can be easily integrated with new future technologies. ACER ProShield has been designed for the SMB market. Our research concluded that SMB does not have the time or resources to use a full version security product like HP Protecttool. They require a simple security solution with emphasis on BIOS settings, password protection, and data protection.
Protection against unauthorized access

There are many technologies today that businesses can choose from to implement client device security. Many of the technologies are great as an independent product offering, but it is difficult to integrate the technologies seamlessly into one product offering. Even if it is possible to integrate the technologies into one seamless product offering, it may be challenging to make the client devices secure.

These are some of the features that are offered in the client device security through different technologies:

- Biometrics will be more important as the technology gains acceptance as a security hardware and also as it becomes a product that will enhance the ease of use for the computer validation.
- The Trusted Platform Module (TPM) embedded security chip produced by the Trusted Computing Group (TCG) is the ultimate client device security standard, and is available in ACER products.
- Data Removal using the latest US Department of Defense (DoD) approved 5220.22-M standard for cleaning and sanitizing. The DoD 5220.22-M data removal uses three pass algorithm method. First algorithm pass sanitizes with "zeroes", second algorithm pass sanitizes with "ones", and the last algorithm pass with random bytes.

Many client devices include security features exist within the BIOS. The features include the following:

- Boot Order Setting is the ability to change the BIOS boot order. The ability to arrange the boot device first into groups (HDD, ODD, Removable, & LAN) and then arrange the devices in each group.
- Port and device control.
- Import and export BIOS settings.

Many of the security features are based on industry standards and have a high integration capability. There are still challenges for a seamless integration preventing the features to be fully compatible. Challenges such as:

- The integration between the technology and the user ability of the features
- The difficulties of managing between the client and server infrastructure. The
lack of a seamless integration from small company to large company.

- The lack of education in remote management that prevents full understanding and full 100% usage between client and server architecture.
- The inability to be used in multiple devices.
- The limitation of not being able to be scalable as new technology and new opportunities become available.

The ACER ProShield is security software that was designed to addresses these challenges with the help of third party software. This security software is a complete solution providing all the features and functions in one software package. In addition, the architecture of the solution is designed to be scalable and flexible to add new technologies as they become available.

Why ACER ProShield

ACER ProShield is only the first step in client security software unified with a common user interface and common architecture across ACER commercial notebooks and commercial desktops. This extensive framework is designed to allow additional security software functions to be added and customized into the ACER ProShield infrastructure. This architecture provides the ability for long term support of client security strategy for all ACER commercial product lines. The benefits are extended to the commercial customer through ease of use, management, and the addition of security hardware features for the client devices.

The client security software is a combination of a myriad of functionality through plug in software modules. These software modules are introduced to produce a better protection against unauthorized access to the PC. These software modules are also providing an ease of use to commercial customer’s local PC and network access.

There are many features to support multiple user authentication using different security technologies such as biometric fingerprint reader, TPM or embedded security chips, and password authentications. Users are also protected under another layer of authentication protection when they log into Microsoft Windows PC. ACER ProShield is designed to include the easy to use single sign-on that will store and protect the passwords used daily by the commercial user in accessing their local PC, network and applications.
Other features such as BIOS Migration, Data Encryption, and Remote Management provide an ease of use to both the local user and IT management. Data Encryption will further increase the security of the local PC through Personal Secure Drive (PSD) or through an available optional SED. BIOS Migration also provides the ability to enable and disable port/device lock. This feature will prevent the local PC from sharing sensitive data through USB ports and through devices. IT management in obtaining asset IDs and BIOS updates is accomplished through Remote Management. ACER ProShield is designed with integration of remote management into one user interface not only for convince, but most importantly for simplicity to the IT manager.
ACER ProShield

An all-in-one security solution, Acer ProShield provides an embedded security solution to address the following points of vulnerability:

- Securing the device against unauthorized access
- Protecting local storage
- Securing the network

Five pillars of protection
Acer ProShield includes five modules that will secure your device from unauthorized access and intrusion.

Credential Manager – Password, Bio-Protection, TPM configuration
BIOS Migration – Boot sequence and device security
Data Encryption – Personal secure drive, file and folder encryption
Data Removal – File shredder
Remote Manageability – ProShield remote UI

Credential Manager

The first layer of protection is pre-boot authentication. Pre-boot authentication occurs immediately after turning on the computer and before the system has loaded. This stage is important to prevent access and manipulation of passwords that are susceptible with the operating system loaded.

Pre-boot authentication can be handled in three ways:
1. Power-on password – the user is required to enter a password on boot.
2. TPM – on systems containing a TPM, the user is required to enter a key pass phrase on boot.
3. Bio-Protection – on systems containing a bio-protection device, the user is required to use their finger print on boot.
BIOS Settings

Securing the BIOS is the next step in securing the system from unwanted access. Regular operating system password authentication can be bypassed with alternative boot methods (i.e.: USB drives and CD/DVD), thus it is important to secure the boot sequence and devices.
With Acer ProShield, you can set the order of the boot sequence and enable/disable devices.

Boot options are:
HDD, ODD, LAN, Removable

Port devices to enable/disable:
USB, CardBus, eSata, serial ports, parallel ports

Built-in devices to enable/disable:
Wi-Fi, LAN, webcam, Bluetooth, ODD, bio-protection, TPM, microphone, speakers, modem
Data Protection

Computers are lost, stolen, and succumb to malicious software that steals data. Data encryption will protect sensitive information from prying eyes if such an event occurs. Acer ProShield implements full volume data encryption all the way down to an individual file.
ProShield Cryptography Diagram
Data Removal

Data removal becomes important during decommissioning of company assets. When a system is recycled or disposed of, hard drives left on the machine need to be properly scrubbed of data. Hard drives left unprocessed often contain recoverable personal and company information. To resolve this issue, Acer ProShield includes a file shredder, which completely removes data from the drive.

Remote Manageability

This module allows Acer Client Manager to control the functions of Acer ProShield from a remote station. The flexibility of remote management allows efficient use of IT resources and timely implementation of security updates.
Frequently Asked Questions

Q. Is ACER ProShield for installation in notebook or desktop?
A. ACER ProShield is installed in 2011 notebook and desktop models starting December 2010.

Q. What add on modules are available for ACER ProShield?
A. ACER ProShield currently has the five pillars or modules
   - BIOS Migration
   - Data Encryption
   - Data Removal
   - Credential Manager
   - Remote Manageability

Q. What authentication technologies are supported by ACER ProShield?
A. ACER ProShield currently supports the following authentication technology and is designed to support future authentication technologies.
   - Biometric (fingerprint) authentication
   - Password authentication

Q. Is pre-boot authentication available in ACER ProShield?
A. Yes, pre-boot authentication is available with both biometric (finger) authentication and password authentication.

Q. Does ACER ProShield client support TPM embedded security chip?
A. ACER ProShield is designed to use TPM for client support. ACER has partnered with Wave Systems to provide a solution that enable TPM chip key management. Infineon and St Micro are important security partners that will provide the TPM hardware. ACER ProShield Credential Manager has the capability to integrate with TPM embedded security key management to provide a single sign-on in one user interface.

Q. How does Credential Manager differ from other single sign-on solution?
A. The benefit of ACER ProShield is that they bring together the technologies into a single easy to use security solution. The Credential Manager is an integral part of ACER ProShield and provides the user authentication feature for ACER ProShield.
Q. Will TPM be compatible with Credential Manager?
A. TPM will be compatible with Credential Manager if TPM is available. The password vault of the TPM will store the encrypted password.

Q. What if the user has multiple windows account?
A. The user will be able to create a different user identity in each windows account.

Q. Is ACER ProShield supported on non ACER computers?
A. ACER ProShield is only supported on ACER 2010 commercial notebooks and commercial desktops.

Q. Does ACER ProShield have remote management?
A. ACER ProShield has partnered with Altiris from Symantec for remote manageability. Altiris is a valued partner that provides a 60 day trial version to be evaluated by the customer. A full version can be purchased from Symantec website with pre-approved discounts for ACER commercial customers.

Q. What is the BIOS difference compared to previous ACER commercial BIOS?
A. ACER current BIOS have a consistent WMI interface for all commercial notebook and commercial desktops. The WMI interface provides a consistent output of data that provides the data for asset management and BIOS remote update. The BIOS will be able to boot order setting, port setting, built-in device configuration, export BIOS setting to a file, import BIOS setting from a file, and BIOS setting encryption.

Q. Is ProShield compatible with Secure Encryption Drive (SED)?
A. ACER ProShield is compatible with SED for all 2010 commercial notebooks. SED encryption software can be purchased through Wave Systems and the hardware is purchased through your authorized ACER re-seller.

Q. Does ACER ProShield enable/disable port and device?
A. ACER ProShield will enable/disable port and device through the BIOS level. This feature is one of the innovative features designed into the commercial BIOS. This will allow the user to close all USB ports and external ports on the computer. The ability to lock data devices to provide a secure local PC that protects data security. The BIOS level encryption provides an additional layer of protection compared to the OS level encryption.

Q. Will ProShield be different between ACER commercial vs. Gateway commercial?
A. 
ProShield will not be different between ACER commercial and Gateway commercial.

Q11. Why was ACER ProShield design not as robust as HP ProtectTool?
A. ACER ProShield has been designed for the SMB market. Our research concluded that SMB does not have the time or resources to use a full version security product like HP Protecttool. They require a simple security solution with emphasis on BIOS settings, password protection, and data protection.
### Attachments

HP Protecttool versus ACER ProShield

ACER ProShield BIOS Setting is very competitive against HP Protecttool. ProShield includes the basic BIOS settings such as asset tag, boot order, and password setting for user and supervisor. Advance BIOS features are also included such as device enable/disable for USB port, LAN, 3G, TPM, Card Reader, BT, and WLAN. BIOS is using WMI to import/export BIOS settings from one computer to multiple computers to ensure standardization of the BIOS configurations.

<table>
<thead>
<tr>
<th>Features</th>
<th>HP</th>
<th>ACER</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BIOS settings</strong></td>
<td>Support 1st stage: Yes</td>
<td>Support 1st stage: Yes</td>
</tr>
<tr>
<td>(Generic)</td>
<td>Asset number, Ownership, Password policy, Boot order, Boot dev enable/disable,</td>
<td>Asset tag, Boot order, Password settings (User and supervisor), power on password, D2D</td>
</tr>
<tr>
<td><strong>BIOS settings</strong></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>(Special)</td>
<td>Fan always on in AC, SATA mode, Dual Core, Instant-On, WLAN Btn, Wake on USB...</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Device control</strong></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>(ON/OFF)</td>
<td>Cardbus, USB Port, Express card, WLAN, Fingerprint, ODD, LAN, Camera, BT, Modern, Microphone, Audio</td>
<td>WLAN, BT, USB Port, LAN, 3G, TPM, Card Reader</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BIOS Settings</th>
<th>Data Protection</th>
<th>Data Removal</th>
<th>Credential</th>
<th>HP</th>
<th>ACER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Features</td>
<td>Support 1st stage</td>
<td>Detail</td>
<td>Support 1st stage</td>
<td>Detail</td>
<td></td>
</tr>
</tbody>
</table>
ACER ProShield has a full feature Data Protection that includes Full Volume Encryption, Personal Secure Drive, and File Protection. ACER designed ProShield to be more robust compare to HP Protecttool because we believe that individual users in the SMB market will want to secure their own data from unauthorized access.
Data Removal is a function that will help protect intellectual property by completely deleting the file and folder. Currently when a file or folder is deleted, a residue can be found inside the HDD. The ACER ProShield shredder, certified by the United States’ Department of Defense, will have three passes to completely erase the file and folder. There will be no possible way to recover the erase file or folder.
Credential Manager will authenticate your device with fingerprint, login password, and TPM. ACER ProShield uses software and hardware for authentication.