



**Closed Circuits for Information:  
360° Data Protection  
for the Enterprise**

**This page left intentionally blank**

## Executive Summary

The powerful combination of legislation, negative PR, and legal liability has ensured that data protection is perhaps the most important information technology challenge facing organizations today. The solution landscape is overflowing with solutions that promise to address just a single aspect of data protection, but for the under-resourced and overstretched CIO in a typical enterprise, implementing multiple point solutions is simply not a practical option.

The Secuware Security Framework (SSF) is designed to overcome those issues and provide a comprehensive security operating system that overlays and integrates with Windows to protect the organization's data, no matter where it may be residing. SSF delivers *Closed Circuits for Information*, ensuring that only authorized individuals using authorized applications on authorized devices are able to access authorized data. It enables the application of highly granular security policies for storing and accessing data on fixed and removable media as well as in network folders, so that information is available to those who are authorized to use it, but not to anyone else. These protections and controls are implemented in a data-centric design which minimizes the amount of administrative work and integrates tightly with Active Directory and other LDAP-based directory services.

This paper briefly reviews key data protection issues and Secuware's track record in the information security marketplace, before entering into a thorough review and analysis of the Secuware Security Framework and how it can be implemented to resolve the most critical data protection issues facing organizations today.

## Table of Contents

Executive Summary .....	3
The Data Protection Problem .....	5
The High Cost of Insecure Data .....	5
What is the Data Protection Problem and How Can It Be Solved? .....	5
The Secuware Security Framework .....	6
Overview and Benefits .....	6
Key SSF Customers .....	7
The Secuware Security Framework in Depth .....	9
Product Architecture .....	9
Simple and Scalable Deployment and Administration .....	10
Client distribution .....	13
Creating and revising user security policy .....	13
Creating and revising computer policies .....	13
Creating and revising policies for local hard disk encryption .....	13
Creating and revising policies for non-local storage .....	14
Creating and Managing Data Access Controls for specific devices .....	14
Application Access Controls .....	15
Transparent Data Protection for End User Systems .....	15
Bootting up .....	15
Normal system usage .....	17
Key Technologies .....	18
Encryption Types .....	18
Pre-Boot Authentication .....	19
Application Control .....	19
Comparison with Market Alternatives .....	20
Overall .....	20
PKI-related issues .....	20
Microsoft Vista BitLocker .....	20
Product Specifications .....	22
Client .....	22
Administration Console .....	22
Supported Servers .....	22
Supported Directories .....	22
Company History and Background .....	23

*This white paper is for informational purposes only. Secuware makes no warranties, express or implied, in this document.*

*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 Secuware, Inc.*

*© 2007 Secuware, Inc. All rights reserved. Secuware and the Secuware logo are registered trademarks of Secuware, Inc. Secuware Security Framework and Crypt2000 are trademarks of Secuware Inc. All other marks are the property of their respective owners.*

## The Data Protection Problem

### The High Cost of Insecure Data

Data Protection was number 1 on the *Most Critical Issues for the Next Two Years* list in the recently completed 2006 CSI/FBI Computer Crime and Security Survey<sup>1</sup>. Dramatically illustrating the importance of the Data Protection issue, spam was in contrast reported as a critical issue by only 15% of survey respondents.

This response is hardly surprising in light of the legal and regulatory environment facing CIOs today. In business sectors as diverse as financial services, manufacturing, and e-commerce, as well as government, a data breach or loss must be reported publicly, even a suspected breach or loss; by 2006, security breach notification laws had been introduced in at least 35 states<sup>2</sup>, and non-compliance can attract fines running into the millions of dollars. We are all aware of the numerous, highly publicized news stories concerning lost or stolen laptops and CDs containing confidential information about hundreds of thousands, even millions of people.

The non-financial consequences of a data loss or privacy breach include public embarrassment, loss of good will, and damage to reputation. The financial consequences are such that some organizations may never recover; these include legal, investigative, and administrative expenses, as well as adverse shareholder and customer reactions, opportunity loss, and crisis management. Then there is the cost of retaining customers through the provision of information hotlines and complimentary credit monitoring subscriptions<sup>3</sup>. One study found that 20% of consumers affected by a corporate data breach terminate their relationship with the company, and 5% will hire a lawyer<sup>4</sup>. Probably the CIO's worst nightmare today is the prospect of seeing his company's name in a *Wall Street Journal* story about data loss.

### What is the Data Protection Problem and How Can It Be Solved?

Data protection encompasses data privacy and data access control, and this is clearly a large, multi-faceted enterprise-wide problem with many different issues and problems:

- Laptops lost or stolen outside of the office with highly confidential information<sup>5</sup>
- Employees copying confidential information to mobile devices such as flash drives without authorization
- "Inside jobs" by employees who misappropriate confidential information for personal financial gain, or by cybercriminals who infiltrate businesses<sup>6</sup>
- Employees downloading for their personal use applications which contain viruses or Trojan Horses designed to steal corporate data
- Limited resources for security enforcement

*"Only a small number of the data breaches reported to the [Government Reform] Committee was caused by hackers breaking into computer systems online. The vast majority of data losses arose from physical thefts of portable computers, drives, and disks, or unauthorized use of data by employees". – Government Reform Committee, Staff Report, October 13, 2006*

The key challenge facing IT and security management today is identifying and deploying a solution that protects data privacy and controls data access regardless of location, and is *operationally* effective. An overly complex solution will not provide effective security, because it will never be maintained or supported adequately in an era of tight budgets. And end-users will simply refuse to work with security products that put too many barriers between them and their productivity, regardless of the promised benefits.

In developing and implementing a comprehensive data privacy and access control solution, the CIO and his staff are faced with a bewildering number of choices, most of them only partial solutions. A cobbled-together combination of multiple different point products is almost certainly going to suffer from functional overlap, functional gaps, multiple management consoles, and duplication of administrative tasks. Confusion, high maintenance costs, and security vulnerabilities are an almost inevitable result. The preferred solution is one that delivers

- Comprehensive data protection and access control in a single, flexible package
- Low management overhead (headcount and specialized skills)
- End-user transparency
- Tight integration with the existing IT infrastructure

The *Secuware Security Framework (SSF)* is an enterprise solution that is designed from the ground up to protect corporate data and control access to information regardless of location or storage medium.

## The Secuware Security Framework

### Overview and Benefits

Secuware Security Framework (SSF) ensures that only *Authorized Individuals* using *Authorized Devices* and running *Authorized Applications* can access *Authorized Data*. While SSF integrates directly with all major LDAP-based directory services, Active Directory is used as the example implementation throughout this paper.

A Pre-Boot Authentication process, tightly integrated with Windows and Active Directory, ensures that strong user authentication is required for any data or system access. This process leverages investments in existing security infrastructure and eliminates the need for a separate Identity Management system.

A data-centric approach to media and file encryption enforces data privacy and access controls. Additional data access controls allow system access only to authorized USB and Firewire devices. Application control limits user access to a predetermined list of approved programs. As a side benefit, application control delivers an additional layer of defense against viruses, Trojan Horses and other malware by preventing the accidental or deliberate activation of unapproved executables. Application control also contributes significantly to system stability, as users always have known, tested application configurations.

This combination of controls creates *Closed Circuits for Information* - zones of security that protect corporate data in much the same way that a CCTV system displays images only in a restricted area. The resulting tight integration with Windows results in a "secure operating system" that protects data from the boot process onwards.

SSF architecture is low-overhead and highly scalable, comprising a lightweight Windows Client and a Management Console. It does not require its own servers or a dedicated database and database server. The client is easily deployed using standard software management tools.

Security configuration and administration (policy creation) is performed through directory snap-ins. System administration (assigning policies to users and systems) is handled through the standard directory console.

Security policies, in the form of *user and computer profiles* containing *encryption keys*, are stored in the directory as schema extensions. For security, the encryption keys are not directly available to either security or system administrators. Policies take effect at the next login or Group Policy Object push.

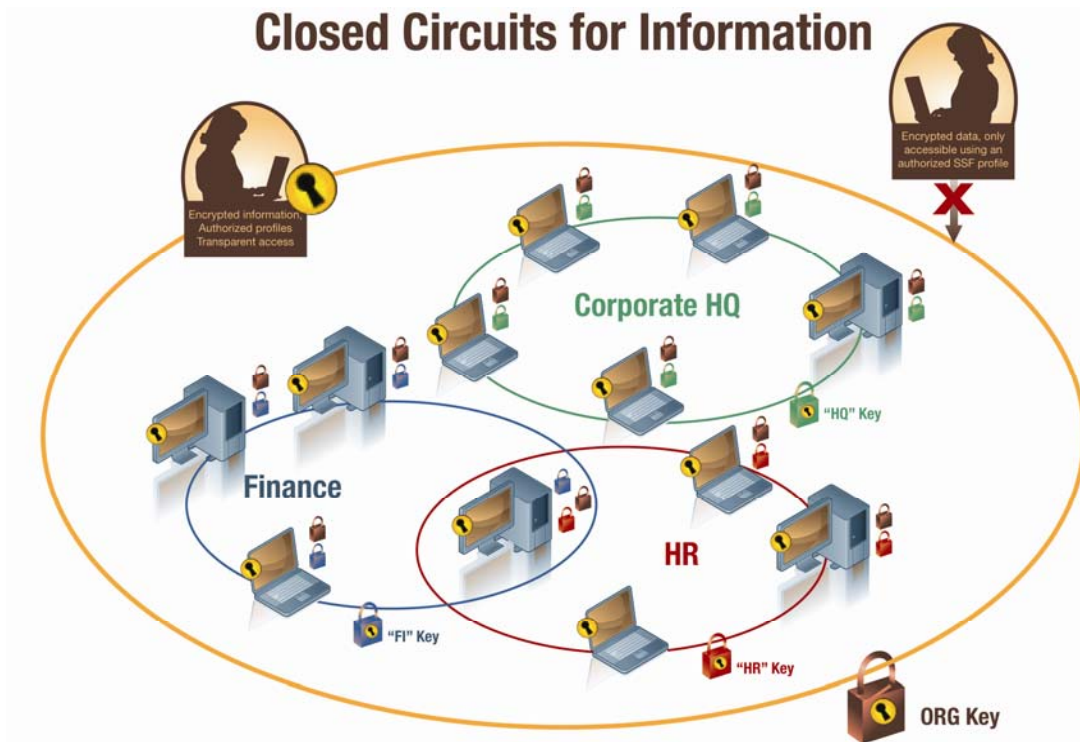


Figure 1: Secuware Security Framework creates Closed Circuits for Information

SSF provides data protection using symmetric encryption keys. One key is used for local hard disk encryption and additional encryption keys are assigned to non-local storage, including removable media, USB and FireWire devices, and network folders. Each encryption key is associated with a “named device”; there can be multiple named devices for a given device type, such as CD/DVD. Named devices can be assigned to any number of different *user* and *computer profiles*, allowing for highly granular security policies. This elegant and straightforward approach eliminates the complex issues associated with a PKI, as discussed in the section on *PKI-related issues* below.

SSF provides additional data access controls through *profiles* for *authorized devices* and *authorized applications*. If an *authorized device profile* is in force, only pre-authorized devices will be able to communicate with a system, whether or not the data on the device is encrypted. If an *authorized applications profile* is in force, only those applications that were pre-approved by the security administrator can be run by the user.

### Key SSF Customers

SSF is used by more than 300 corporate and government customers worldwide, protecting over 500,000 Windows systems.

- *Agencia Estatal de Administración Tributaria (AEAT, the Spanish IRS)* has implemented SSF on 35,000 systems to protect confidential taxpayer information. AEAT has implemented Closed Circuits for Information to prevent data leakage from local hard disks, floppy disks, CD/DVDs, USB devices and network folders.
- *WalMart Mexico* uses SSF for data protection in the on-site banks in its Mexican stores. Because the Active Directory forest is located at corporate headquarters in the US, Wal-Mart

Mexico has deployed ADAM (see the section on *Simple and Scalable Deployment and Administration* below) to allow security and systems administrators in Mexico to manage local SSF deployments.

- *Warner Brothers Mexico* uses SSF to protect clients' intellectual property and prevent piracy by enforcing tight access controls on its mobile employees' laptops.
- *Telefonica Móviles (the Spanish national cell phone company)* has deployed SSF on 10,000 workstations to guarantee the confidentiality of all customer information stored on its systems, preventing unauthorized devices from connecting with Telefonica systems as well as the execution of unauthorized applications.
- *Iberdrola*, Spain's largest utility company, has customers throughout Southwestern Europe and has deployed SSF on 12,000 systems to protect the energy supply chain from cyber terrorism and other electronic threats.
- *BBVA*, one of the largest banks in Spain with branches in many countries in Europe, Latin America, and the US, has implemented SSF to protect confidential information on the laptops of senior executives.

## The Secuware Security Framework in Depth

### Product Architecture

SSF comprises an Administration module, implemented as an Active Directory MMC snap-in, and four separate client modules, as shown in Figure 2 below. Three of the client modules create and enforce policies, and the fourth records all relevant security events for later analysis for security event and forensic purposes.

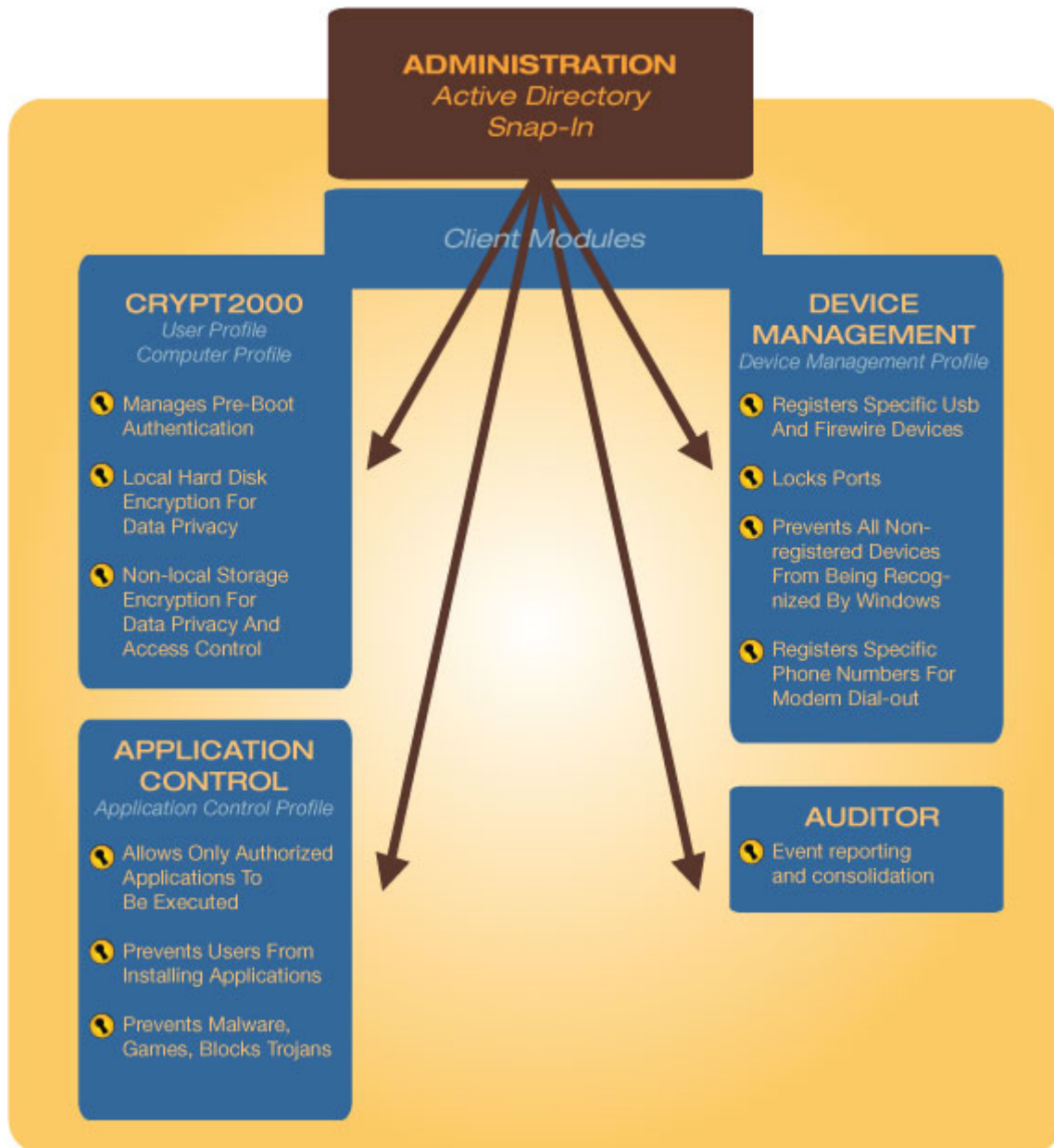


Figure 2: SSF client modules, can be installed in any combination and execute policies created by the Administration module

SSF deployment can start with any of the three policy modules, although in practice most companies start with *Crypt2000*. The *Administration* module is always required, as it is used to create and manage policies. Figure 3 below shows how each module protects data access during the various stages of system operation from pre-boot to shutdown.

As previously noted, there is no requirement for a security server or a policy database, which greatly simplifies deployment and reduces implementation costs.

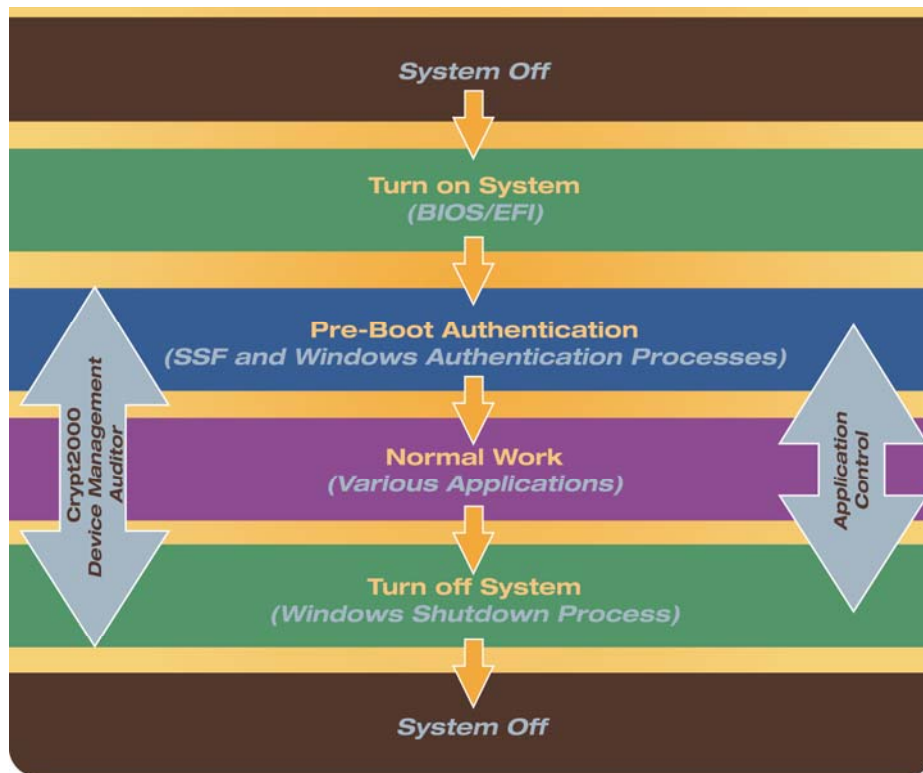


Figure 3: SSF provides active protection the entire time that a system is active

### Simple and Scalable Deployment and Administration

Data-centric, centrally managed policies for endpoint systems are at the heart of SSF. Policies are created and stored as extensions to the Active Directory *Users and Computers* schema. Once stored in AD, policies are pushed out to users at the next user login or Group Policy update.

The overall configuration of the AD forest, in terms of trees, domains, sites, number of objects, trust relationships, system populations, delegation of responsibilities, etc., is completely transparent to SSF.

**Note:** For customers who do not want third-party applications to extend the AD schema, or who want to implement decentralized delegation of responsibilities, SSF also supports ADAM<sup>7</sup>.

*Active Directory Application Model, or ADAM, was designed by Microsoft to address deployment scenarios related to directory-enabled applications. It is a lightweight version of Active Directory that can run as a simple user service on Windows 2003 Servers or even on Windows XP with SP1. To simplify usage, ADAM uses many of the same administrative tools as Active Directory. ADAM uses the same APIs as Active Directory for easy application integration.*

Table 1 below summarizes how the various aspects of data privacy protection and data access are implemented within Active Directory:

Security Policy Area	SSF profile (module)	Application Directory Object Class
Pre-Boot Authentication	Computer profile (Crypt2000)	Systems
Authentication and Local Disk Encryption Options	Computer profile (Crypt2000)	Systems
Data Privacy Protection for local Hard Disk	Device encryption key (Crypt2000)	Systems (via computer profile)
Data Privacy Protection and Data Access Control for removable media devices (CD/DVD, USB, FireWire, floppy disks)	Device encryption keys, one per named device. (Crypt2000) Assigned to one or more user profile(s).	Users (via user profile) Systems (via computer profile)
Data access to specific USB/FireWire devices	Device Management profile (Device Management)	Users Systems
Application control	Application control profile (Application Control)	Users Systems

Table 1: How Security Policies are implemented with SSF

SSF enforces a division of responsibilities between the security administrator and the system administrator. Only the *security* administration may create and modify policies, create *encryption keys*, and assign encryption keys to *user* and *system profiles*. Only the *system* administrator may implement SSF security policies with users and computers. This division of responsibilities ensures that administrators perform tasks within their respective areas of expertise, thus enhancing overall corporate security through the elimination of a single point of (human) failure.

This division of responsibilities is summarized in Table 2 below

Security Administrator	System Administrator
Implement corporate security policies for strong authentication Implement corporate security policies for data privacy and data access	Create users Create systems Apply policies to users and systems
Create whitelists (device management profile) of registered and approved USB and Firewire devices	Apply device management profile to users
Create whitelists (application control profile) of approved applications	Apply application profile to users
Creates auditing profile for files and folders Reviews audit reports for security incidents	Apply auditing profile to users

Table 2: SSF Enforces a Strict Division of Responsibilities Between Security and Systems Administrators

The *security administrator* uses the Secuware Active Directory MMC snap-in shown in Figure 4. All policies are created and managed by the security administrator through this snap-in. The SSF snap-in should be installed only on *security administrators'* systems.



Figure 4: Policies are created and managed by the security administrator through an Active Directory snap-in. The system administrator implements the security policies, using the four schema extensions for the Users and Computers schema in Active Directory, as shown in Figure 5. To enforce the division of responsibilities, this AD schema console should not be accessible to security administrators.

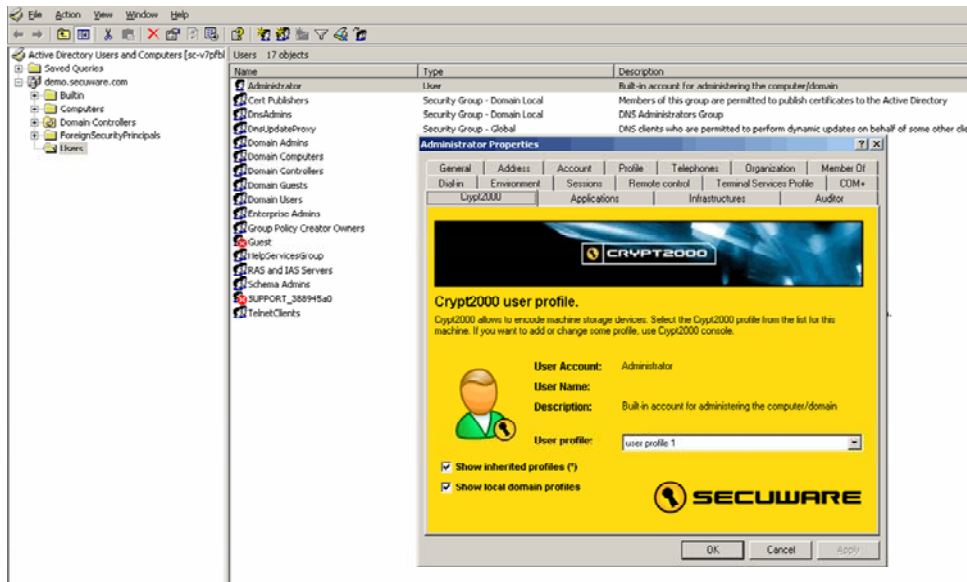


Figure 5: The system administrator uses the four extension tabs created by SSF in the Users and Computers schema to apply policies to users and systems

## Client distribution

The SSF client is an *msi* module which can be deployed and installed automatically using any of the major network-based software distribution tools, such as Microsoft SMS or equivalents from Tivoli, Computer Associates, etc. Alternatively, the SSF client can be installed using a log-in script.

## Creating and revising user security policy

The policy profiles and device encryption keys are created by the security administrator, using the Crypt2000 element of the SSF snap-in. Once created, these policies can be assigned by the system administrator to a user or groups of users using the Users and Computers Administrative Properties Window as shown in Figure 5 above.

Users are assigned *one and only one* Crypt2000 *user profile*, eliminating confusion about which policies apply to which users. This approach simplifies policy creation, enforcement, and management. A Crypt2000 user profile is mandatory; optionally, users can be assigned a *Device Management* and/or an *Applications profile*.

A *user profile*, once created, can be assigned by the system administrator to:

- The entire domain
- Multiple domains within an AD
- An organizational unit (OU) within a domain, for example a department or branch location
- An individual user
- Any combination of the above

There is no practical upper limit to the number of different user profiles that can be created for one Active Directory forest. However, in practice, one large Secuware customer (over 10,000 users) has created only three different user policies, one for senior management, one for mid-management, and one for all non-management employees. Other organizations have created larger numbers of profiles, with separate profiles for employees in different functional organizations.

## Creating and revising computer policies

Each system has an associated *computer profile* that applies to all users of that system. This profile is used to enforce strong authentication through the pre-boot authentication, to set choices for the allowable authentication credentials, to enable/disable Windows advanced authentication options, and to force/not force users to enter a name at every login. This profile also holds the key for local hard disk encryption and the selection of user profiles for when the user is connected or not connected to the domain.

Once the Pre-Boot Authentication process is complete, the local hard disk encryption key, contained in the *computer profile*, is used to decrypt files *on demand*. (Note that the disk itself always remains encrypted, protecting all files even if the system is powered down abruptly in the middle of normal work.)

## Creating and revising policies for local hard disk encryption

The security administrator can specify whether or not the local hard disk must be encrypted; s/he must first create a "named" device," as shown in Figure 6. This "named device" is then assigned to one or more computer profiles. The system administrator assigns the computer profiles to systems, as described above.

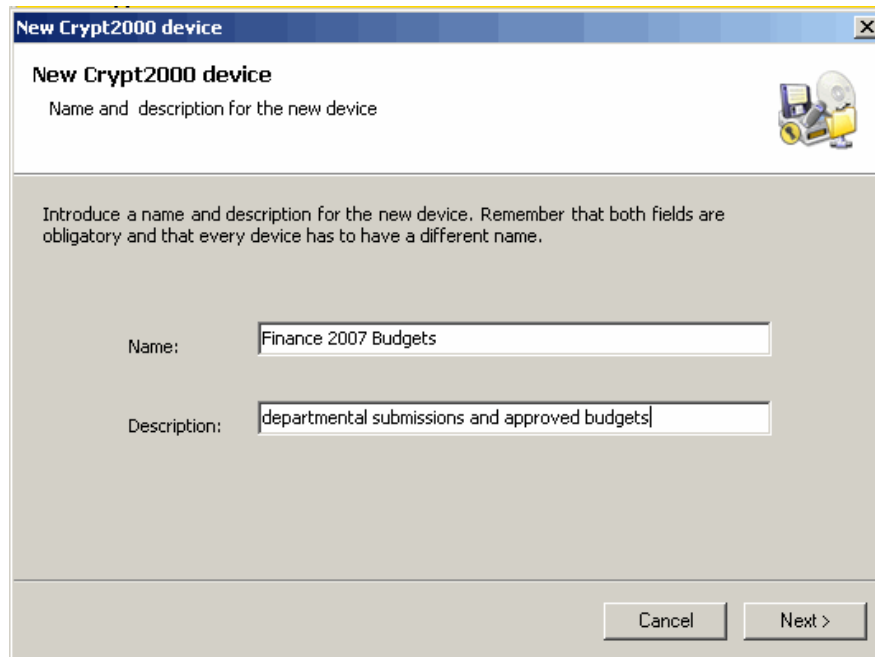


Figure 6: SSF can create a new “named device” for use with one or more user and computer profiles

## Creating and revising policies for non-local storage

The *security* administrator can specify which kinds of *non-local* data storage devices can be used to access protected data. Non-local storage includes CD/DVDs, USB and Firewire devices, floppy disks, and network folders.

To allow for highly granular security policies, each non-local storage device access control is “named.” There can be multiple “names” for any given type of storage device, and a unique symmetric encryption key is created for each such device control.

Once named device controls are created, they are assigned by the *security* administrator to one or more *user profiles* and *computer profiles*. All users or all computers with a given profile share a device encryption key and thus have access to files and media protected by that named device’s encryption key. Since a given named device can be included in multiple user or computer profiles, users or computers with different profiles can have access to the same files and media. All other users and computers, with different profiles that do not contain that given named device encryption key, are denied access to those files and media.

For removable drives, floppy disk and CD/DVD, USB and Firewire drives, every medium used in one of these drives is encrypted with physical encryption (see *Physical Encryption* and *Removable Media* below) for maximum security.

## Creating and Managing Data Access Controls for specific devices

The Device Management module is used to create *device management profile whitelists* for specific devices by filtering on USB, Firewire and modem ports. Only those devices on the whitelist can be accessed, whether or not the data files on those devices are encrypted.

The *device management profile* can also filter on *dial up numbers* for modems, allowing the security administrator to limit a modem user to only pre-approved dial-up destinations.

A specific device is registered on the whitelist by the *security* administrator and the serial number recorded. Once on the whitelist, authorized devices are assigned to users by the *system* administrator by associating that *device management profile* with a user.

## Application Access Controls

Application Control ensures that users can run only those applications and browser plug-ins that have been pre-approved by the security administrator. No other applications or plug-ins can be executed or installed, including any that may be downloaded by the user.

The Application Control module can be implemented in a variety of ways, ranging from minimal or no use to selective deployments to a full enterprise deployment. Because application control tightly controls system use, it can be very useful to restrict specific groups of workers, such as contractors, to running certain applications, especially in those companies where only a few standardized system configurations are deployed to many different groups of workers.

Each different applications policy is contained in an *application profile* created by the *security* administrator. The application control policy is applied to users by the *system* administrator.

### Potential for granularity in SSF security policies

There are no dependencies between user profiles, computer profiles, device management profiles, and application control profiles. Different user and computer profiles may have some encryption keys in common, and others that are unique or different.

## Transparent Data Protection for End User Systems

### Booting up

SSF controls the PC from the moment that it is first turned on. *Pre-Boot Authentication* ensures that only an authorized user can boot the system or access the contents of the local hard drive.

The Pre-Boot Authentication process prevents an attacker from bypassing the internal hard disk and booting the system using techniques such as:

- Rescue disk created by Windows<sup>8</sup> or by anti-virus or disk partitioning utilities
- Windows installation media
- Bootable USB flash drive loaded with Windows<sup>9</sup>
- CD with a self-contained “Live Operating System” such as *Knoppix*<sup>10</sup>.

This approach also prevents an individual from removing the SSF-encrypted hard disk and placing it in another system as a second physical hard drive, since the individual will not be able to successfully complete the pre-boot authentication procedure that enables decryption of files on the hard disk.

Once the system completes BIOS (or EFI) initialization, SSF displays a customizable login-screen similar to the one shown in Figure 7 below.



Figure 7: The Pre-Boot Authentication process unlocks the system and boots into Windows in a single step

The Pre-Boot Authentication window can be customized to:

- Publish corporate messages and other motivational materials
- Remind employees of key security or other corporate policies
- Provide help desk contact information

The Pre-Boot Authentication process is completely integrated with the normal Windows login process. Users provide their usual Windows userID and password, smartcard, or USB token, to authenticate themselves.

### **Login If the System Is Connected to a Domain**

- The user credentials are validated by Active Directory
- Windows boots normally.
- The *user profile* is loaded from Active Directory
- The *computer profile* is loaded from Active Directory.

### **Login If the System Is Not Connected to a Domain**

The process is the same as when the system is connected to a domain, except that:

- The user credentials are validated by using a cached copy of the Windows credential information stored in encrypted form on the hard disk.
- A different *user profile* is loaded. This profile is typically more restrictive than the one loaded when the system is connected to a Domain because of the risk that a user is no longer with the company, or has reported a lost system, which would be locked out with an online authentication, but not an offline login if the user were careless with his credentials.

## Normal system usage

Once logged in to Windows, the user can perform all normal job functions as permitted by the policies set for their work.

Data protection and data access control are completely transparent to the *authorized user*, who will have full use of all *authorized data*. They have no need to click on icons or select menu items to encrypt or decrypt a file. All file encryption and decryption is done on the fly, in the background, automatically. The user will be able to use all *authorized devices* to store and retrieve data and can run all *authorized applications*, enabling them to:

- create new files
- access and modify existing files
- delete files
- copy/move files to/from any partition on the local hard drive
- copy/move files to/from removable storage such as a CD-R or a USB flash memory drive
- copy/move files to/from a network folder

Employees using their system to perform assigned job functions will never encounter any restrictions on work activities. SSF will be 100% transparent to these users. Limits on actions will be encountered only if users attempt to access data for which authorization has not been granted, or use a device, or run an application which has not been authorized.

For example, as shown in Figure 8:

- A Finance Department employee will not have access to any Corporate HQ network folders, but will have access to selected Finance network folders. The Corporate HQ network folders and most of the Human Resources network folders and their contents will be visible in Windows Explorer to the Finance employee, but the files themselves will be unreadable.

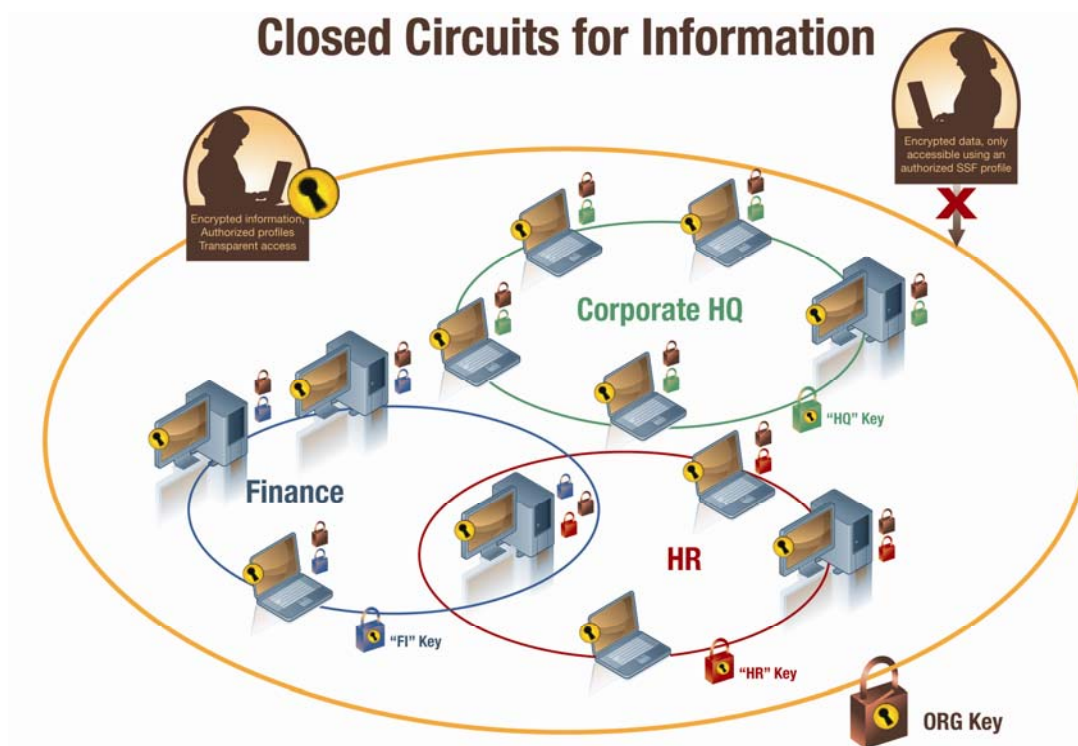


Figure 8: Users can only access data and applications only within their authorized closed circuit for information

- If an employee at corporate headquarters used a Flash Drive or CD to transfer a file to a Finance employee, the recipient would not be able to read, modify, or print that file. The same would hold true if that same employee used the Flash Drive or CD to transfer the file to anyone outside of the organization.
- If any user downloaded an application from a web site, that application could not be executed, even if the user were able to do a successful installation.

Authorization policy is completely outside users' control. The SSF client is *not user-configurable*, and SSF does not create any *ini* files or make any registry entries that could be modified by a technically-inclined user or attacked by malware.

Because SSF is so transparent to end users, training is usually not required either before or after deployment, except perhaps to reinforce the organization's security policies.

## Key Technologies

### Encryption Types

SSF uses two encryption types when building *Closed Circuits for Information* – physical encryption and logical encryption:

#### Physical encryption

##### Local hard disks

Local hard disks are encrypted at the sector level to provide a higher level of protection and prevent access to information on the disk if the system is booted by different means, such as a Flash drive or CD.

If all the information on the hard disk is encrypted, everything stored on that disk is protected, including temporary files and other trace information (swap files, etc.) that are not protected by traditional data protection processes and programs. This avoids the possibility of unauthorized exploitation and thus lowering risks.

Most encryption software uses the Windows Crypto API or a crypto toolkit, which consists of Dynamic Link Libraries (DLLs). Those DLLs load after Windows has started, and are vulnerable to attack.

##### Removable media

Full encryption of removable media at the sector level renders the media readable only on systems with SSF installed and for users with the proper *profile*. This design prevents information leakage, accidental or otherwise, to any entity outside the organization's authorized channels. This level of control is transparent to users during their normal course of business and the information is always protected, regardless of whether it is located inside or outside the company.

A common concern about full hard disk encryption is the impact on system performance. SSF uses symmetric block cipher algorithms (IDEA 128 bits or AES 256 bits), noted for their high performance and low resource usage, to avoid this issue. In practice, Secuware has determined that their implementation of symmetric encryption imposes only a 0.15% overhead in reading or writing protected files. The net result is that the performance difference between a system with encrypted hard disks and one without is minimal.

## Logical encryption (network-based files and folders)

Logical encryption is used to encrypt information at the file level, so the encrypted information can be stored on any media not formatted at the physical level, notably shared network folders.

Logical encryption is selected at the folder level, and all files stored in a given folder are encrypted with the same key. It is possible to protect multiple folders with the same encryption key, but only one encryption key can be used for any given folder.

Backup copies of files in network protected folders will remain encrypted, since they were encrypted when they were originally written to the network. Any administrator can be permitted to make backups, since the contents of protected files will be unreadable to unauthorized users.

## Pre-Boot Authentication

On installation, SSF modifies the Master Boot Record to start the system with the pre-boot authentication process instead of the boot record for the active partition.

The pre-boot authentication process uses its own TCP/IP network stack to communicate with Active Directory even before Windows is active. This approach eliminates hacker attacks based on modifying or replacing the key *dlls* used in normal Windows user authentication and prevents Windows-based keystroke loggers from capturing userIDs and passwords.

If a network is not available, or an AD node cannot be located, a locally-cached copy of the user credentials is used for authentication.

## Application Control

The Application Control module uses application signatures to verify that an application is authorized, has not been tampered with, and may be allowed to execute.

The *security* administrator uses the Application Control module to select and pre-approve the Windows OS and selected application folders. Alternatively, when dealing with a few standard system images that are used widely throughout the organization, all files on the hard disk can be selected.

The Application Control module then calculates 128-bit MD 5 hashes for all files inside the selected folders, which are packaged up as a *signature file*. The signature file is associated with an *application control profile*.

The *system* administrator assigns the application control profile to selected users. Every time a user attempts to start an application, or an application attempts to load a *dll*, the MD5 hash of that executable is calculated and compared against the hashes in the signature file. If a match is found, execution is permitted; otherwise, the file cannot be executed.

## Comparison with Market Alternatives

### Overall

SSF differs from other data protection solutions in several key ways:

- implementing data privacy protection and data access controls regardless of the location of that data
- providing data access controls on which USB and Firewire devices can be recognized by Windows
- controlling which applications can be executed on any given device

SSF's protection is active even when a system is turned off; users must go through a Pre-Boot Authentication process, integrated with Windows, to gain access to a system and its files. Similarly, SSF's protection is active even if the system or removable media is outside of the corporate network.

SSF's unified, data-centric approach means that only one administration console and three client modules are needed to create, set, and enforce policies for data protection and access for all classes of users and systems, USB and Firewire devices, and applications. The administration console is used to apply these policies to any user or system in the corporate network. Other solutions require many more modules to accomplish the same or less.

SSF is integrated tightly with Windows and LDAP services, resulting in a lightweight and scalable architecture that leverages, rather than duplicates, an organization's existing investments in security infrastructure.

### PKI-related issues

In a PKI, correct key lifecycle management is critical to the overall robustness of the security application. A PKI requires attention to the following issues, none of which are a concern for the SSF customer:

- Secure creation of a key pair
- Secure storage of the client (the Windows registry does not protect a private key adequately)
- Distribution of X.509 certificates with public keys.
- Backup or escrow of signing keys. (Authentication keys do not need to be escrowed.)
- Renewal/replacement of private keys and certificates on expiration of old certificates.

### Microsoft Vista BitLocker

**BitLocker** is a security feature introduced in Windows Vista that provides full disk encryption of local hard drives. However, as BitLocker doesn't support encryption of network folders, it does not support logical encryption.

BitLocker support is provided only in Windows *Vista Enterprise*, not for Windows *Vista Business*. Further, Microsoft recommends that the system has a Trusted Platform Module v1.2<sup>11</sup>, which is not yet available for many systems intended for the business market. For systems without a TPM, Microsoft has defined an alternate approach using BitLocker with a USB Flash Drive as part of the boot-up process. This approach has been – unsurprisingly – criticized by a noted security expert as “kludgy”<sup>12</sup>.

One key advantage that SSF offers over BitLocker is that BitLocker serves only to protect the local hard drive of a laptop or desktop system running Vista Enterprise from *offline* attacks. SSF can protect

data on any storage device across a broad range of Windows platforms and protects data even when it is located outside of the local system. In addition, SSF provides data access controls for USB or FireWire devices and implements controls on application usage, neither of which is supported by BitLocker.

Table 3 below summarizes these differences:

	<u>Secuware Security Framework</u>	<u>Windows Vista BitLocker</u>
<b>Platforms</b>		
Windows Endpoint Platform Support	Windows 2000 Professional Windows XP Vista (future announcements)	Windows Vista Enterprise
<b>Authentication</b>		
Authentication Methods	userID and password smartcard USB token	Trusted Platform Module v1.2 present in system USB Flash Drive
<b>Data Protection</b>		
Trust Relationships	Authenticates User	Authenticates System but not user (multiple users share same Trusted Platform Module PIN)
Protects System Hard Drive Data	All partitions All physical drives	Only C partition on primary physical drive
Protects Data on CD-R	Yes	No
Protects Data on USB Flash Drive	Yes	No
Protects Data in network folders	Yes	No
Permits Sharing Encrypted Data With Authorized Individuals	Yes	No
<b>Key Management</b>		
Recovery Key Required	No (see PKI-related issues section)	Yes
System Repair (e.g. motherboard replacement) makes data non-accessible for the user	Not an issue	Requires recovery key
User's Hard drive move to another system makes data non-accessible for the user	Not an issue	Requires recovery key
<b>Device Access Management</b>		
Only authorized USB and FireWire devices recognized by Windows	Yes	No
<b>Application Control</b>		
Only authorized applications can be run by the user	Yes	No

*Table 3: SSF offers comprehensive data protection and access control for all Windows 2000 and XP systems, whereas BitLocker offers protection only against system loss or theft and only for Vista Enterprise*

## Product Specifications

### ***Client***

#### **Platforms Supported:**

- Windows 2000 Professional SP 4
- Windows XP
- Windows Vista (during 2007)

#### **Hard Disk Space**

- 10 MB

### ***Administration Console***

#### **Platforms Supported:**

- Windows 2000 Professional SP 4
- Windows 2000 Server SP 4
- Windows XP
- Windows 2003 Server

The Administration Console may be co-resident on the same system as any of the SSF client modules.

#### **Hard Disk Space**

- Minimal

### ***Supported Servers***

- Windows 2000 Server SP 4
- Windows 2003 Server

### ***Supported Directories***

- Microsoft Active Directory
- Microsoft Active Directory Application Model
- Novell eDirectory

## Company History and Background

Secuware was founded in Madrid, Spain, in 1988 by Carlos Jimenez to provide proactive security for the Ministry of Defense in Spain. His goal was to create a “security grid” that could adapt and grow in response to changes in human behavior and evolving threats. Jimenez founded Secuware after selling his prior company, Anyware, which produced anti-virus products, to McAfee in 1988.

The Secuware Security Framework was launched in 1998. There are now more than 300 corporate and government customers in Europe and Latin America, protecting a total of 500,000 Windows desktops and laptops. The company has offices in Madrid, Spain, Dorfen, Germany, Mexico City, Mexico, Bogotá, Colombia, and now Sunnyvale, CA, USA.

---

<sup>1</sup> <http://www.gocsi.com/>. (Select hyperlink and complete questionnaire to enable download.)

<sup>2</sup> Knowledge Services Group, *Data Security Breaches: Context and Incident Summaries*, Updated September 28, 2006, p. 2, CRS Report for Congress, Congressional Research Service, The Library of Congress, Order Code RL 33199. [http://digital.library.unt.edu/govdocs/crs//data/2005/upl-meta-crs-8258/RL33199\\_2005Dec16.pdf](http://digital.library.unt.edu/govdocs/crs//data/2005/upl-meta-crs-8258/RL33199_2005Dec16.pdf)

<sup>3</sup> Ponemon Report Shows Sharp Rise in the Cost of Data Breaches, <http://complianceandprivacy.com/News-Ponemon-data-breach-cost-study.asp>

<sup>4</sup> Anne Saita, *Giving notice: Victims lashing out at compromised companies*, [http://searchcrm.techtargt.com/originalContent/0,289142,sid11\\_gci1131245,00.htmlm](http://searchcrm.techtargt.com/originalContent/0,289142,sid11_gci1131245,00.htmlm) Sept. 27, 2005

<sup>5</sup> Gartner Group, *Stolen Laptops Denote and Growing Data Security Breach for Higher Education*, 10 March 2006, ID number G00138273.

<sup>6</sup> Gartner Group, *Improvements in Security Will Encourage an Increase in Insider Collaboration of Cyberattacks*, 14 November 2006, ID number G00144683.

<sup>7</sup> *Introduction to Active Directory Application Mode*, Microsoft Corporation, August 2003. <http://www.microsoft.com/windowsserver2003/techinfo/overview/adam.msp>.

<sup>8</sup> Microsoft Corp., <http://support.microsoft.com/kb/314079/en-us>. *How to use System files to create a boot disk to guard against being unable to start Windows XP*

<sup>9</sup> Brian M. Posey MCSE, <http://articles.techrepublic.com.com/5100-6346-5928902.html>. *Boot Windows XP from a USB flash drive*

<sup>10</sup> <http://www.knoppix.net/>.

<sup>11</sup> Microsoft Corp., <http://technet.microsoft.com/en-us/windowsvista/aa906017.aspx>. BitLocker Drive Encryption: Technical Overview, Version 1.02, April 4, 2006

<sup>12</sup> [www.schneier.com/blog/archives/2006/05/BitLocker.html](http://www.schneier.com/blog/archives/2006/05/BitLocker.html).



**Secuware, Inc**  
440 North Wolfe Road  
Sunnyvale, CA 94085  
Phone: 1-800 720 0734  
Email: [sales@secuware.com](mailto:sales@secuware.com)  
[www.secureware.com](http://www.secureware.com)