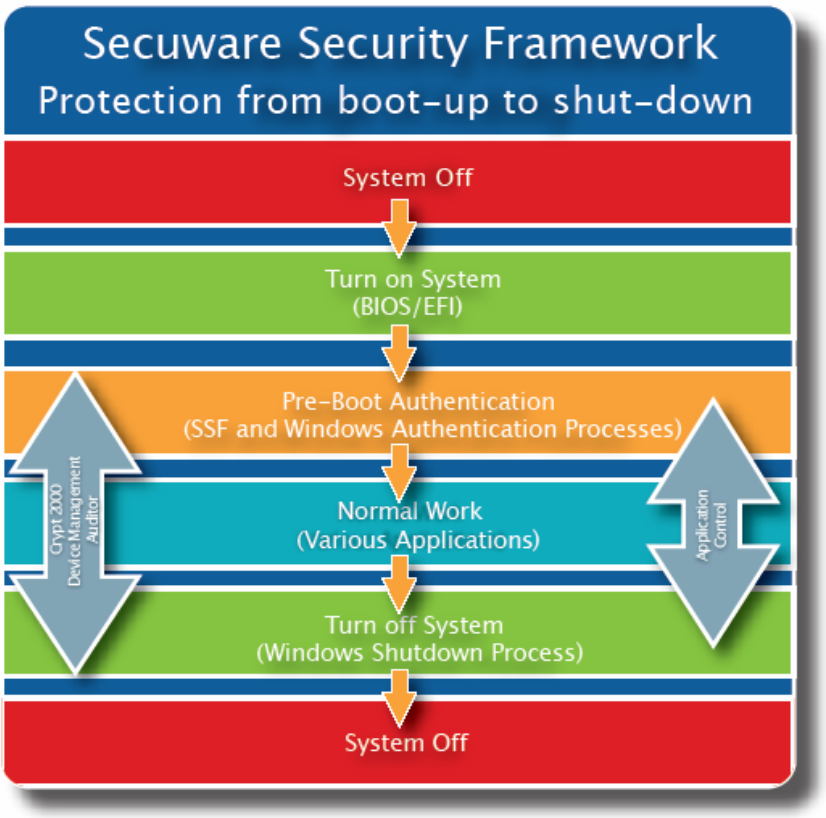
Secuware™ Security Framework

Secuware Security Framework (SSF™) makes it easy for enterprises to protect data against unauthorized use or access, regardless of user role, location, or storage medium. SSF's *Closed Circuits for Information*™ ensures that only **authorized** individuals using **authorized** applications on **authorized** devices can access **authorized** data.

SSF prevents information leakage and blocks malware with policy-based, centrally managed controls over data, devices, removable media, and applications that are enforced inside and outside the enterprise. These controls are tightly integrated with Windows® Active Directory® and other LDAP environments, and are in place from client boot-up to system shutdown while remaining completely transparent to end users.



SSF is used by more than 500 enterprises and government departments throughout Europe and the Americas, protecting over 800,000 systems. SSF protects against internal and external misuse of data:

- Lost or stolen laptops.
- Systems discarded without the hard drives being wiped.
- Users misappropriating confidential information.
- Users copying information without authorization to portable storage media (USB, FireWire®, CD/DVD, floppy disks, removable hard drives).
- Users running unauthorized downloads that may contain malware.
- Cyber criminals infiltrating networks to steal data.

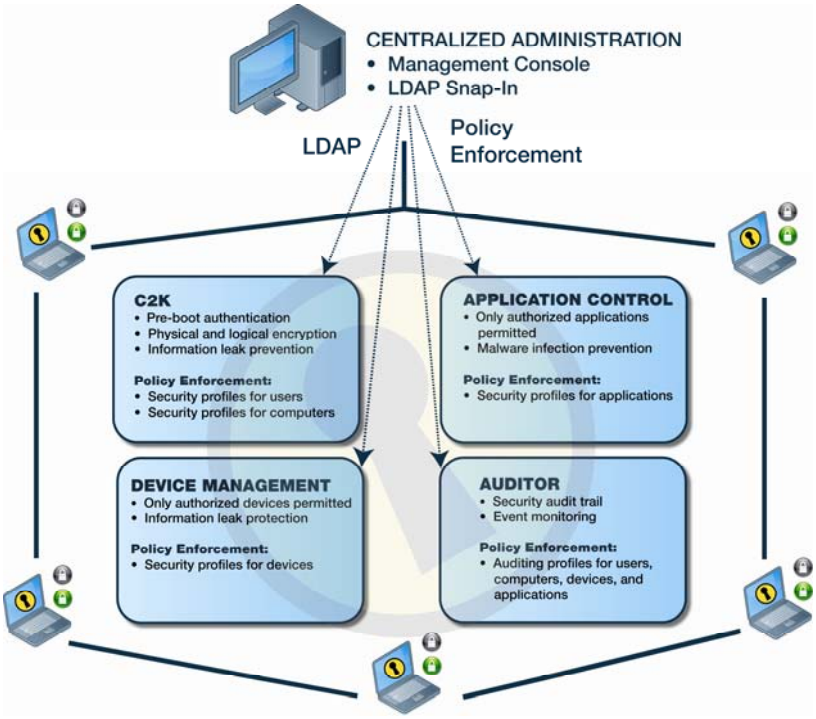
SSF protects corporate data from unauthorized use or access inside and outside the enterprise.

- Scalable, centrally-managed, highly granular policies protect data stored on local hard disks, network folders, and removable /portable storage media.
- Every user, every computer, and every device can be governed by specific policies according to role and location.
- Protection easily evolves with the needs of the enterprise.

"Data protection is not just a 'lost laptop' problem. Organizations need a data protection solution that covers a range of devices, applications, hard drives and network folders with a single, consistent approach to setting policy. Rather than reinventing policy management systems and creating yet another management console, leading data protection solutions will integrate with existing policy information stores and other LDAP-enabled directories."
— Neil MacDonald, Vice President and Distinguished Analyst, Information Security, Privacy and Risk, Gartner.

SSF is easy to administer.

- Highly scalable architecture uses lightweight client and snap-in Management Console.
- No server or policy database needed, reducing costs and administrative complexity.
- Policies and device keys stored securely in Active Directory as schema extensions.
- Symmetric keys eliminate PKI key management issues.
- Separate roles for security administrator and IT administrator ensure maximum security.



The SSF suite comprises four client modules and an Administration Module in the form of an Active Directory snap-in.

Product Specifications

Clients

- Windows 2000 Professional SP4
- Windows XP

Administration Console

- Windows 2000 Professional SP4
- Windows 2000 Server SP4
- Windows XP
- Windows 2003 Server

The Administration Console can reside on the same system as any of the SSF client modules.

Servers

- Windows 2000 Server SP4
- Windows 2003 Server

Directories

- Microsoft Active Directory
- Microsoft Active Directory Application Mode
- Novell® eDirectory™

- **C2K** enforces strong user authentication through Pre-Boot Authentication that's tightly integrated with Windows, leveraging existing investments in user authentication and identity management. Systems cannot be booted with system rescue tools that bypass the hard disk. C2K enables *whole disk encryption* on local hard disks and removable media, and *logical encryption* on network folders. Files are always encrypted on the media, and decrypted only as needed. Files on an encrypted hard disk cannot be decrypted if the hard disk is placed in a different system, even one with C2K installed.
- **Device Management** ensures only authorized USB and FireWire devices can be used by employing a whitelist approach based on the serial numbers of individual devices. Different whitelists can be assigned to different classes of users, enabling more granular control of device use.
- **Application Control** ensures users can run only those applications authorized by the security administrator, blocking the use of programs that enable access to restricted data, preventing non-business use of systems and stopping malware from executing. Different application profiles can be assigned to different classes of users, so that execution privileges can be controlled based on roles or other user characteristics.
- **Auditor** maintains records of all relevant events for analysis and to assist in compliance and forensic reporting.
- **Centralized Administration.** The Administration Console is used by the security administrator to create security policies. The policies are stored in Active Directory as user and system profiles and device keys. IT administrators can then assign policies to specific users and systems, using Active Directory schema extensions. Active Directory is also used to automatically distribute policies to clients at the next login or Group Policy Object update, simplifying day-to-day administration and scaling easily to large user and system populations.

SECUWARE

440 North Wolfe Road, Sunnyvale, CA 94085 Phone: 1 800 720 0734 / 1 408 524 3070 Fax: 1 408 524 3072
info@secuware.com www.secuware.com