CipherShare
Features and Benefits

CipherShare Features and Benefits

Feature	Benefits
Security	
End-to-end Encryption	**Everywhere, "Always On" Security**: CipherShare provides completely transparent encryption of all data at rest and in-flight - at the level of the individual user - throughout the data lifecycle. As well, all document/file/message/chat data are encrypted at rest both centrally and locally and during transmission.
Need-to-Know:	**File/Object Level Permissioning**: CipherShare uses individually targeted PKI based asymmetric encryption to provide fully granular disclosure (sharing) at both the object (file/chat/message) and user levels. This allows CipherShare to operate on a complete "kneed to know" basis. A user sees ONLY the data that has been explicitly shared with him/her. Without that access privilege, the user will have no access or knowledge of the data.
Challenge / Response Authentication	**Strong Authentication**: CipherShare utilizes obfuscated password memory and edit boxes, hashed passphrases, authenticated Diffie Helman and a robust challenge response protocol to provide for secure, strong authentication. Once logged in, digital signatures are used to sign all actions, providing non-repudiation.
Transitive Trust	**Delegated Trust Verification**: CipherShare uses transitive trust to enable rapid and secure authentication and trust relationship development. In CipherShare, a single Security Officer can verify the authenticity of each member of the workgroup, and pass the authentication status through transitive trust to each member.
Consistent Security	**Asymmetric Encryption**: CipherShare treats the security for all objects consistently with a single security / encryption protocol based on transparent PKI and asymmetric encryption.
Password and Key Recovery	**No Recovery by Single Administrator**: Currently, CipherShare does not allow for arbitrary password recovery by an administrator. Version 3.0 will use a sophisticated key recovery system based on split keys and multiple administrative consent, which does not allow for the possibility of a rogue administrator acting alone to gain access to data.
Temporary Application File Protection	**EFS and Secure Delete**: CipherShare uses the following mechanisms to secure application temp files: 1) Optionally use of Microsoft's "Encrypted File Service" or EFS. 2) Secure delete (zeroing) of all temp files between sessions. Additionally, future releases will include: 3) NTFS permission restriction based on Windows access permission. 4) Share permission override monitoring to check for rogue administration access.
Symmetric and Asymmetric Algorithm matching	**NIST Compliance**: With Version 2.2, CipherShare will offer full compliance with NIST guidelines for asymmetric and symmetric key algorithm matching (for example, NIST calls for the use of SHA-512 as a hashing algorithm for AES 256). CipherShare will utilize high performance elliptic curve (EC) algorithms to provide asymmetric encryption for all shared data throughout the data lifecycle.
No "Super User"	**Prevention of Insider Threat**: CipherShare's transparent integration of PKI and encryption completely separates administrative functions from content, preventing the possibility of "rogue" administrators having the ability to access and exploit data within the CipherShare system.

CipherShare Features and Benefits

Feature	Benefits
Document Management	
Versioning	**Non-Repudiable Version History**: CipherShare offers full delta versioning at the binary level, regardless of format or type. Each delta is digitally signed. CipherShare maintains an auditable version history of any file or document enabling non-repudiation at the version/modification level.
Check-in/Check-out	**Editorial Control**: CipherShare offers check-in/check-out and document/file locking to ensure that editorial conflicts do not occur, and that version histories can be fully tracked and audited.
Auto-Notification	**Real-time Interaction**: CipherShare immediately broadcasts encrypted metadata to authorized members of the share list, and so offers better "real-time" interaction among share members.
Document/File Meta-data	**Data on Demand**: CipherShare tightly couples meta data with each file/document. CipherShare allows users to view meta-data independently of the associated object, and download object (file/document) data on demand.
Search	**Rapid Access to Documents**: CipherShare's meta data handling allows complex search and filtering functions to be offered. As well, CipherShare offers full content search for both documents and messages.
Integrated Spell-checking	**"On-the-fly" Spell Checking**: CipherShare has integrated spell checking for all message and chat data which offers users the ability immediately correct spelling.
n-Tier Folder Structure	**Customized Content Structure**: CipherShare offers a fully customizable n-tier document/file structure, allowing an organization to develop a content structure that reflects their operational and knowledge management practices.
Digital Signatures	**Strong Identification and Non-repudiation**: CipherShare offers digital signatures for all data and objects including documents, files, versions, messages, chat sessions, share lists, etc. This feature, coupled with CipherShare's strong authentication, ensures that actions performed by users are tracked at the level of their digital signature, providing non-repudiation.
Chat	
Selective Chat Participation	**Privacy**: CipherShare enables fully private and encrypted chat sessions between specific members of a workgroup. As well, CipherShare has no limit - outside of system resources - on the number of chat instances to be run simultaneously. Each chat session is a fully private channel between participants
Messaging	
Securely Encrypted Messages	**Privacy and Non-Repudiation**: All CipherShare messages, chats and data are contained in encrypted form within the CipherShare environment. All messages are digitally signed.

Feature	Benefits
Bandwidth Optimization	
File / Data Transfer Optimization	**Streaming Encryption of all File Types**: CipherShare utilizes high efficiency streaming encryption and "smart" upload / download managers to offer full resumability for arbitrary file sizes and formats including document, movie, audio and CAD/CAM.
Delta Versioning	**Minimal Data Transfer**: CipherShare uses source file (binary level) delta-versioning to provide highly efficient data transfer for all file types and formats, versioning control, auditing and high efficiency bandwidth usage.
File Compression	**Minimal Storage Impact**: All data stored and transferred through CipherShare is compressed prior to encryption, allowing for storage gains of up to 15:1, depending on file format.
Granular Access	**Minimal Data Replication**: Because of CipherShare's granular disclosure and workgroup creation abilities, sharing data between workgroup members does not require the creation of a new workspace area, but can be easily supported within a larger community of users. This minimizes confusion and data replication.
Client / User Mobility	
Roaming Secure Workspace	**Rapid Mobility:** Roaming with CipherShare is very simple, requiring only a TCP/IP connection to connect to a CipherShare server from anywhere.
Loss Recovery and Theft Prevention	**Local Data Protection**: CipherShare's fully encrypted local cache prevents theft of data through strong encryption. As well, a CipherShare user can easily recover his/her data by installing a new CipherShare client and connecting to the CipherShare server.
Usability	
Intuitive Collaborative Features	**High Performance**: CipherShare's user interface is high performance and "clean", offering intuitive collaborative and file sharing services.
Well Structured Interface	**Low Learning Curve**: CipherShare's functions are consistent and easy to learn.
Standard Models	**Accepted Document Management Models**: CipherShare uses generally accepted editing and document management models including "Check-in/Check-out", document locking, auto-versioning and auto-notification.
Simple Administration	**Rapid Deployment**: CipherShare's administration functions are simple and function autonomously. No specific technical expertise is required and CipherShare's PKI infrastructure is transparently created without the need for additional software.

CipherShare Features and Benefits

Feature	Benefits
Architecture	
Client-Server	**Synchronization:** CipherShare's client / server architecture ensures that everyone sees the same server state, enables synchronized operations such as locking, and supports more efficient network transmissions;
Centralized Repository	**Data Centralization**: CipherShare's client / server architecture allows for true store and forward, centralized master database repository and backup.
Server-based Store and Forward	**Bandwidth Efficiency**: The CipherShare server offers download on demand with source transfer rates independent of peer connection speeds.
Secure Local Repository	**Secure Off-line Access**: CipherShare's client/server framework offers fully encrypted local caching of synchronized content, enabling secure off-line access and editing and theft prevention.
TCP/IP	**Accessibility**: CipherShare can be used with any standard Internet or dial-up connection. No additional specialized hardware or software is needed.
C++	**Performance**: As a C++ application, CipherShare's application performance is very high for both the client and server.
Installation & Configuration	
Broad Platform Support	**Inclusivity**: Client is supported on all 98+ Windows platforms (98 / Me / 2000 / XP) extending CipherShare's end-to-end security and encryption to older computers.
Simple Installation and Low Installed Footprint	**No Specialized Expertise**: CipherShare's client / server application is simple to install and - at 3.5 megabytes fully installed - has a very low footprint. Deployment is straightforward and requires no specialized expertise. Because of its small size and highly efficient memory usage, CipherShare has a very limited impact on client machines. Generally, no additional RAM or hard drive space is needed.
Configurable Ports	**Granular Control**: CipherShare Server ports can be easily customized and pre-configured for any collaborative group or context, enabling very granular firewall configuration and control over CipherShare related traffic.
Auto-upgrade Detection	**Ease of Deployment**: CipherShare's auto upgrade detection services enables rapid distribution of new client upgrades without the need for intervention by MIS staff.

About Proven Security Solutions

Proven Security Solutions is a software development and consulting company specializing in highly secure and completely transparent applications of encryption and key management.

Proven Security's mission is simple - making state-of-the-art cryptographic security an invisible component of high value software applications.

For more information on, please visit www.provensecuritysolutions.com or e-mail us at info@provensecuritysolutions.com.