AirZip® FileSECURE™ Features

Communicate with Confidence™

AirZip FileSECURE offers a range of unparalleled advanced features that make it the most secure choice for securing your sensitive and confidential files and documents. FileSECURE is designed to provide a robust, easy to use and flexible solution that can meet the requirements of very small to very large organizations in an environment of constantly evolving threats.

Security Features

FileSECURE employs a range of security features to prevent unauthorized use of electronic files and documents. Each secured file will be protected by many or all of the following:

- Strong Encryption
  FileSECURE secures all files using AES256 encryption – strong enough to be authorized for securing Top Secret documents by the U.S. Government.

- Unique encryption keys
  Every file is secured using a unique encryption key limiting the damage should a key ever become compromised.

- Detects and blocks screen capture programs
  FileSECURE blocks literally thousands of screen capture and remote access applications to stop confidential information being compromised. In addition, you are able to explicitly whitelist (permit) and blacklist (block) specific screen grabbing applications.

- Prevents unauthorized printing
  A user must be granted specific print permission for a secured file before being able to print it.

- Printer whitelisting for location based printing (available on special request)
  Further restricts authorized printing to specific physical printers.

- On-screen and print watermarking
  Overlays information regarding the user (e.g. host name, IP address, mac address, Windows user name, FileSECURE User ID, date, etc.) accessing the document when displayed or printed. Primarily used for forensic analysis if someone has used a camera to take a picture of on-screen content or made unauthorized copies of printer output.

- Lock user access to physical workstations
  Users can be prevented from accessing secured content from anywhere other than specifically approved workstations (up to 8 per user can be registered)

- Encrypt temporary and recovery files
  FileSECURE secures the most common method used to hack into our competitor's products. Many products simply place a lock on these files which is easily defeated by people of average competence.

- User authentication
  User's must authenticate themselves each time they access a secured file. FileSECURE has its own user database, but can also be integrated with LDAP and Active Directory directory services or two factor authentication solutions such as RSA SecureID and Entrust PKI. When integrated with one of the external directory services, the user's userid and password for

accessing FileSECURE is the same as their Windows userid and password. When FileSECURE clients are deployed in a Citrix environment, there is an option to permit Single Sign-on (SSO) so that the user need not authenticate separately when opening a secured file.

- Separation of control
  The FileSECURE Authentication and Policy Server is usually deployed and physically managed by IT. However, security policy and control are under the control of the content owners themselves (or their management). This means that IT staff are prevented from accessing or viewing secured content unless they are explicitly authorized to do so. Files are secured on the content owner's workstation and are never sent to the Server thereby ensuring that an unsecure version can be intercepted. When deploying AutoSECURE, WebSECURE or Publisher it is recommended that these be deployed on dedicated workstations under the content owner's control.

- Audit trails and reporting
  From the moment a file is secured, all activity concerning that file is logged in FileSECURE's audit trail database. Comprehensive reporting is available for analyzing events and relationships between events, documents, permissions and users.

- Secure communications
  All communications between FileSECURE Clients and the Authentication & Policy server are conducted over Secure Socket Layer (SSL) channels using the same technology and security as is used when you conduct online banking.

- Distributed securing
  FileSECURE performs all securing activities (encryption and compression) on the securing user's workstation rather than sending files to be secured to a central location. This approach minimizes network traffic, distributes CPU cycles and enhances security.

- Dynamic rights
  A user's rights to a secured file can be changed or revoked at any time. If the user's employment is terminated, access to all their secured files can be revoked immediately. If the user's computer is stolen, access to secured files from that specific computer can be immediately revoked.

- Time based access
  Secured files can be set to expire at a predefined date and time. Users can also be restricted from accessing a secured file before a specific date and time. Both of these time parameters can be changed dynamically by the owner of the file.

- Offline control and tamper detection
  The only time FileSECURE user's are able to "lease" rights is when they enter offline mode, primarily used when traveling without internet access. An encrypted cache is populated with keys and rights for selected files. The maximum time that a user can cache keys and rights is determined by policy. Once that time expires, the user must connect to the Authentication & Policy Server and refresh the cache. Numerous tamper detection methods are deployed to detect attempts at compromising the cache. For example, if any attempt to set back the system clock us detected, the keys in the cache are destroyed.

- Communications interception prevention
  FileSECURE uses SSL encryption for all communication between Clients and the Server. The SSL libraries are statically linked into the Clients to prevent the easy and common attack of

replacing dynamic libraries (DLL's) with debug or otherwise compromised versions that permit the attacker to view the data stream and thus obtain the encryption key for a file.

- Designed specifically for multi-tenant environments

  FileSECURE was uniquely designed from the ground up to operate in an OnDemand or hosted environment where multiple different organizations are running under the same physical copy of FileSECURE. Each organization is cryptographically separated from each other, so that even if a user from one organization were able to obtain access to a secured file belonging to another organization hosted on the same server, they would be unable to do anything with it. In addition, no files – secure or unsecured - are ever sent to or stored on the Authentication & Policy Server thereby preventing the operators of the OnDemand service from even attempting to access content.

Operational Features

- Availability and Reliability

FileSECURE is designed to provide round the clock service. From robust code aimed to meet the stringent requirements of the largest organizations to AirZip's 7x24x365 worldwide support, FileSECURE is enterprise ready.

- Scalability

FileSECURE Authentication & Policy Server runs on all major operating systems and machine architectures. Designed to support tens of thousands of users on a single hardware platform, FileSECURE scales farther than any of its competitors - without the need for the cumbersome and hard to administer federated servers used by others.

- Constantly evolving technology

Unlike the relatively static functionality of competing products, AirZip has introduced substantial and unique features and functions over the past 4 years, and continues to invest heavily in ensuring that FileSECURE remains the leader in rights management technology. The majority of AirZip's customers are in China or doing business in China where intellectual property theft with impunity is rampant. FileSECURE is constantly being re-engineered to meet new threats of people determined to steal. Competitor products are simply not secure enough for the China market.

- Asia Support

FileSECURE offers both Simplified and Traditional as well as Japanese language Clients making it the only viable solution for deployment into the major Asian markets.

- Widest range of files that can be secured

FileSECURE can secure any file for secure end to end delivery and storage. For secure rendering, FileSECURE integrates directly with Microsoft Office and is a licensee of Adobe's PDF libraries, offering perfect rendering fidelity for these two environments. In addition, FileSECURE can secure and securely render the output of any application that can print, leading graphics image types, media files as well the engineering drawings produced by the major CAD applications.

- Designed to support internal and external users

FileSECURE allows you to seamlessly integrate your employees (who are usually integrated through LDAP/Active Directory) as well as suppliers, customers, consultants and others who are not part of the corporate network. Other solutions require that you forego LDAP integration entirely or add these non-employees to your directory service.

- Create users dynamically

FileSECURE Authors (those with securing privileges) can be permitted to create secure viewer accounts on-the-fly. During the securing process, an Author selects existing users (or groups) to

receive the secured file. If there are additional people, who not already existing users, that need to receive the file, the Author can simply provide their email addresses. FileSECURE then automatically creates a Reader account and sends an email to each individual notifying them of their new account information, as well as the public location from where the Reader client software can be downloaded. The file that the Author has secured is then distributed to the users. To view the document, each user simply clicks on it to launch the Reader. The user provides their credentials and can then view (or print, if permitted) the secured file under the control of FileSECURE.

- Auto-securing (patent pending)

FileSECURE offers several methods of automatically securing, and optionally distributing, files based on pre-defined criteria.

- Bulk securing

FileSECURE Publisher permits high volume securing of large archives of documents according to rules expressed in industry standard XML. This is an extremely useful feature for organizations that have recently acquired FileSECURE and wish to secure large quantities of existing files.

- Third party integration

AirZip, customers and partners can FileSECURE Publisher to integrate with third party applications. XML and COM API interfaces are available allowing users to integrate with FileSECURE from C, C++, VB, Java, Perl, Windows Powershell, etc.

- Ease of Use

For content owners, securing a file is as simple a right-clicking on it in Windows Explorer and selecting the FileSECURE menu option. Files can also be secured directly from inside many leading applications by clicking on the FileSECURE icon on the toolbar.
For those receiving a secured file, they just need to double click on that file. This will launch FileSECURE Reader and display the authentication dialog requiring the user to input their userid and password. (The appropriate FileSECURE Server connection information is carried in the secured file payload, so that information need not be manually entered).

AirZip, Inc,
961 Red Tail Lane
Bellingham, WA 98226
USA
tel：+1.360.922.0613
fax: +1.604.630.7101

email: info@airzip.com
http://www.airzip.com

AirZip Asia Ltd.
Level 30, Bank of China Tower,
1 Garden Road, Central,
Hong Kong, S.A.R.
tel：+852.2251.8466
fax：+852.2251.8467

email：info@airzipasia.com
http://www.airzipasia.com

People's Republic of China offices:

email：info@airzip.com.cn
http://www.airzip.com.cn

AirZip Beijing Co., Ltd.
Room 5609, 5th Floor, Chenchang Bldg., Zhichun Road
Haidian District
Beijing, 100080
Tel: +86.10.6262.1936-5034

AirZip Shanghai
Huangsheng Building, Room 1609, 399 Jiu Jiang Road
Shanghai 200003
tel：+86.21.6361.7286
fax：+86.21.6361.7285

AirZip Shenzhen
World Finance Center
Unit A, 31/F, Block A
4003 Shennan Road
Luohu District
Shenzhen 518001
tel: +86.755.2598.0171
fax: +86.755.8283.7487

