

SecureZIP	Standard	Enterprise
<b>Application Integration</b> Stream data directly to/from applications without staging data to disk.		
<b>Encryption via passphrases and/or digital certificates</b> SecureZIP® complements environments using PKI and those that don't by enabling encryption and decryption via passphrases, public key/private key pairs, or both at the same time, depending on the requirements of each intended recipient. SecureZIP supports X.509 RSA v3 certificates issued from recognized certificate authorities such as VeriSign®, Entrust®, Comodo®, and Microsoft®.		
<b>Digital signatures to verify documents have not been altered</b> SecureZIP enables users to sign files with their unique digital certificates. Recipients of signed files can validate the signature to ensure the sender is who they claim to be and verify that the document has not been altered or tampered with since signing. In addition, digital signatures offer non-repudiation - the signer cannot later claim that the signature is invalid.		
<b>Contingency key access to protected files</b> SecureZIP's contingency key provides administrative capabilities to ensure that anything secured will be accessible in the event of an audit or for data recovery purposes.		
<b>File name encryption</b> File name encryption masks file name, file size, and other information to further protect data if it is intercepted in transit or improperly accessed.		
<b>Error reporting for both attended and unattended operations</b> SecureZIP reports errors either to the standard Syslog (UNIX), or through SNMP (Simplified Network Message Protocol) integration with leading data center management applications.		
<b>Email (SMTP) integration</b> Distribution of encrypted files to end-users simply requires adding a switch and the destination email addresses for the recipients, saving processing time and development effort either inside or outside the enterprise.		
<b>FTP integration</b> FTP integration enables automated delivery of files.		
<b>Support for smart cards and smart tokens (Windows® only)</b> SecureZIP's support for smart cards and smart tokens enables security professionals to apply an added layer of data protection by storing the user's private decryption key on a small portable device. Smart cards and smart tokens also enable two-factor authentication, requiring the user to present two credentials before he can access protected data - something known and in the user's possession, such as a password and a private key stored on a portable device.		
<b>Automatic file wiping</b> SecureZIP can be configured to overwrite deleted files - up to seven times in accordance with NSA specifications - to ensure deleted information cannot later be recovered.		
<b>Automatic access to public keys in directories</b> SecureZIP offers an optional interface that integrates with Lightweight Directory Access Protocol (LDAP) compliant directories, such as Sun® iPlanet, Novell NetWare®, and Microsoft Active Directory®. LDAP integration makes it easy to locate, retrieve, and apply the public keys for certificate-based encryption and decryption.		