WinZip® ENTERPRISE

SOLUTION DATASHEET

How to prevent the top 10 data security threats

Companies face various cyber threats, including those that originate both inside and outside of the organization. WinZip® Enterprise offers a range of features to enable secure document storage and sharing, painless backups, and intuitive cloud management. Learn how WinZip Enterprise can help to manage your organization's exposure to cyberattacks.

Data security threat	WinZip solution
Malware infections Malware can steal sensitive information or encrypt it as part of a ransomware attack.	**WinZip Enterprise** WinZip Enterprise protects sensitive data against theft or encryption by ransomware. Features: • At-rest data encryption with AES-256. • Automated backups to local device or cloud storage. • File-specific passwords limit attackers' access to sensitive data.
Social engineering Phishing attacks attempt to trick users into clicking links or opening malicious attachments.	**Cloud storage** Integrated cloud storage reduces the need for insecure document sharing. Features: • Single-pane-of-glass cloud management. • Only show supported cloud environments. • Integrated backup and encryption support.
Compromised credentials Stolen credentials can be used to access corporate accounts, data, and resources.	**Resource-level data encryption** WinZip Enterprise can encrypt individual files or directories with a unique password, limiting the impact of compromised user credentials Features: • Gold-standard AES-256 encryption. • Configurable password policies. • "Break the glass" recovery if password is lost.
Vulnerable third-party software Third-party software may contain exploitable vulnerabilities or malicious code.	**Granular data encryption** Encrypting individual files and folders with unique passwords limits third-party software's access to potentially sensitive data. Features: • Gold-standard AES-256 encryption. • Support for local devices and cloud environments. • Compliance with FIPS and other regulatory requirements.
Accidental email leaks Insecure emails and attachments may leak sensitive data to unauthorized users.	**WinZip Courier** WinZip Courier enables painless encryption of files shared as email attachments. Features: • Gold-standard AES-256 encryption. • Security policies enforce email attachment encryption. • Built-in support for secure cloud sharing.

Weak passwords

Employees set weak passwords or use them across multiple online accounts.

Password settings

WinZip Enterprise admins can specify rules for passwords used to encrypt files with WinZip.

Features:

- Set length and character requirements for WinZip passwords.
- Rules are encoded into the WinZip Enterprise installer.
- Consistent password policies for files on local devices and in the cloud.

Inadequate data protection

Data lacks proper access controls or encryption at rest and in transit.

At-rest data encryption

WinZip Enterprise offers built-in support for data encryption as well as compression for data at rest or transferred via email attachments.

Features:

- Gold-standard AES-256 encryption.
- Company-configurable password policies.
- Secure file sharing via attachments or the cloud.

Weak backup and recovery

Backups are not created regularly, are inaccessible, or are vulnerable to tampering.

Automatic backups

WinZip Enterprise offers automatic backups of files to a user or enterprise-specific location.

Features:

- Automated, encrypted backups.
- On-device or cloud backups.
- Support for differential-incremental backups.

Configuration mistakes

Security settings are misconfigured or disabled, leaving systems insecure.

Custom WinZip Enterprise installation

WinZip Enterprise enables admins to configure it at installation, preventing costly configuration errors.

Features:

- Enable or disable individual features.
- Customized installer for mass deployment.
- Integration with Microsoft Intune.

Removable media

Lost or stolen USB drives or other removable media expose sensitive data.

WinZip SafeMedia

WinZip SafeMedia* enables painless full-disk encryption of removable media

Features:

- Gold-standard AES-256 encryption.
- Support for drag-and-drop file transfer to or from removable media.
- Compliance with FIPS, HIPAA, and other regulations for securing removable media.

*Available for purchase as a separate product.