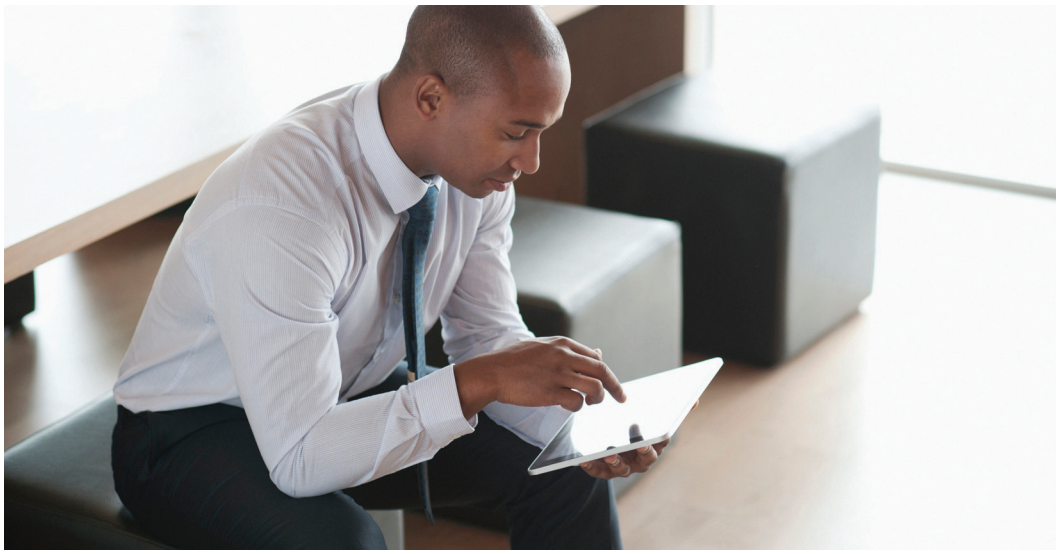
ZENPRISE
Protecting Mobile Enterprises
Everywhere

Zenprise Mobile DLP:
Liberate your users, not your data



Opportunities abound for your mobile enterprise. Employees are happier and more productive when they're given mobile email access. Meanwhile, companies running their businesses on mobile gain competitive advantage and even drive top-line growth. Tablets and smartphones change the way your users access information and collaborate to get their jobs done. Your challenge is moving beyond mobile email and enabling mobile access to business data in an easy, secure way.

Your enterprise is in their pocket

But giving users mobile access to sensitive business data is tantamount to letting them slip your enterprise into their pocket. What happens if they lose that device, along with your non-public financials, product design plans, or next week's press release? And what happens when they leave your company and take their device with your data to their next employer? With an increasing number of employee-owned devices on the corporate network, mobile data leakage is a growing concern for IT and security professionals.

According to CSO Magazine, 17 percent of organizations report having already experienced a mobile breach[1]. Zenprise MobileManager's core security and data loss protection features include passcode enforcement and full and selective device wipe. Most security conscious enterprises need a more granular way to prevent sensitive documents from leaving their organization.

Let users get their jobs done: Secure mobile access to files

Zenprise Mobile DLP lets your users access their data when and where they need to so they can get their jobs done. Zenprise Mobile DLP features a secure, data-agnostic document container that lets your users access presentations, documents, video, and other files from their mobile devices. Users can edit files and have these changes automatically synchronize across all mobile devices whose users have access to the file in their container. Similarly, organizations who want to distribute documents such as presentations, training videos, or service documents to groups of users can use this to manage, lock down, time expire, and ensure version control of these documents.

But protect your sensitive data

Zenprise Mobile DLP allows users to access files while allowing IT administrators to govern and protect corporate data from loss, leakage, or breach. The solution has the three critical components of DLP: protection of data-at-rest, data-in-use, and data-in-motion.

Protect data-at-rest—Zenprise Mobile DLP lets you protect your sensitive data-at-rest by encrypting files in the secure container. Moreover, the solution enables you to selectively wipe the contents of the secure container upon device loss or a user's departure from the company. Finally, you can set dynamic policies to wipe the container and data in the event of a device jailbreak, attempted unauthorized device access, or the device not re-authenticating after a certain period.

Protect data-in-use—Beyond protection of data-at-rest, Zenprise Mobile DLP lets you set content- and context-aware policies on the files (or in a more coarse-grained way on the folder or area in which the file resides) that prevent users from local saving, printing, emailing, and cutting and pasting data from sensitive files. You can further ensure file version control as well as set file time expiry.

Protect data-in-motion—Finally, the Zenprise Mobile DLP secure container uses an encrypted connection between the device and the enterprise to ensure end-to-end protection of data-in-motion.

Integrate with existing infrastructure
Zenprise Mobile DLP integrates with leading business applications, collaboration tools, and content repositories, starting with Microsoft SharePoint and Office 365. There is no need to stand up new infrastructure to allow users to access content from their mobile device. Zenprise just works with what you have.

Have your cake and eat it too
With Zenprise Mobile DLP, you can have your cake and eat it too. Users can get access to the data they need to get their jobs done, and you can protect your sensitive business data. Everybody wins.

Zenprise Mobile DLP[2] is available as an additional module to Zenprise MobileManager™ or Zencloud™, and offers the following capabilities:

FRAMEWORK	CAPABILITY
Enable	• Automatically synchronize data across devices and enterprise collaboration tool
	• Distribute documents to groups of users easily
	• Ensure version control
	• Save documents from device into secure container
Control	• Create rules on file access based on user roles
	• Integrate with Active Directory to auto-enable/disable file access
	• Map DLP policies on a file by file basis, across entire directory structures, and/or on a user by user basis
	• Integrate with enterprise collaboration tools and content repositories starting wtih Microsoft SharePoint and Office 365
Protect	• Protect data-at-rest, data-in-use, and data-in-motion
	• Secure data stored in secure Mobile DLP container via AES 256 bit encryption
	• Prevent leakage of sensitive data through context and content-aware security policies and secure data containers
	• Prevent users from opening certain files in third party applications (e.g., cloud based file sharing apps)
	• Stop users from sending sensitive documents via email, such as to a personal account
	• Block users from copying and pasting sensitive file data into emails or apps
	• Block users from printing sensitive documents
	• Prevent users from downloading confidential files locally to their mobile device
	• Enable controls to time-expire content on devices
	• Selectively wipe corporate data from the container
	• Enable automated wipe upon device jailbreak
	• Enable automated wipe upon failed user authentication
	• Disable data transfer when roaming

[2]2011 study of North American enterprises

[3]Today, Zenprise Mobile DLP is available for the iPad and integrates with Microsoft SharePoint and Office 365.