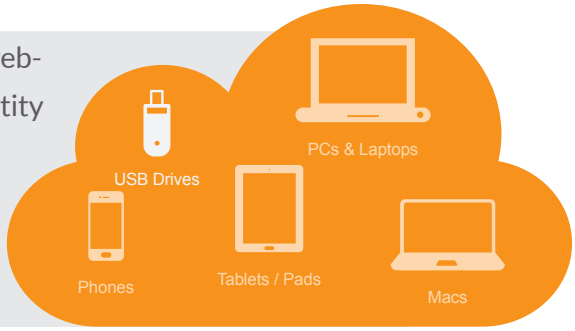
BeachheadSecure™ USB Storage

for USB storage devices

Encryption, authentication enforcement & remote access control

The BeachheadSecure™ Management System is a single, configurable, web-based console with device modules that can be added in any mix or quantity for iPhone & iPads, Android devices, Windows & Mac PCs and USB storage devices. This unique system allows you to remotely secure the vulnerable devices in your organization - including those owned by employees.



Quite possibly your largest data leakage vulnerability

Small, dense and portable storage devices that plug into PCs like flash, optical and external hard drives are ideal for transporting, backing up and sharing business data. These portable devices are so inexpensive and ubiquitous that employees often carry their own into the workplace. Unfortunately, without oversight these popular storage devices may very well represent your company's greatest threat for a catastrophic data breach. Fortunately, Beachhead offers BeachheadSecure™ USB a plug-in module to The BeachheadSecure™ Management System. From one centralized management console, administrators can enforce encryption and remotely change security policy not only on Mac and Windows Computers, Android and iOS phones and tablet, but now on all standard USB storage peripheral devices.

Encryption has been singled out as a compliance requirement by a growing array of new laws and industry mandates and while necessary, it is insufficient data protection by itself. Circumstances change and when a password is known or can be learned, encryption cannot protect your organization's data. You must have the ability to plan and respond to evolving security risk. BeachheadSecure™ USB provides cloud-managed tools that allow an administrator to determine who may write data to what device(s) & under what conditions ("data rights management") and to control who is permitted to read that data ("access control").

Like all Beachhead tools

BeachheadSecure USB is designed to provide organizational security and control of data while balancing usability and employee productivity. The BeachheadSecure console administrator can choose the level of security appropriate for their unique USB use conditions. For instance, a BeachheadSecure administrator in one company may choose a policy that mandates a username and password to authenticate (gain access) to their encrypted USB devices while an administrator in another company may opt for an even greater level of security. This administrator may mandate that USB devices first check-in via an Internet connection to essentially ask for approval to unencrypt it's contents. This way if the device has been reported lost or stolen, authentication privileges are essentially revoked - even with the right username & password - and no one will have access to its contents. This silent and automatic communications gives you essentially the final say on who and under what circumstances. who accesses your organization's data.

All things mobile. **BeachheadSecure™**

For more information call 408.496.6936 or email info@beachheadsolutions.com

BEACHHEAD