

# 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 license modules that can be added for iPhone & iPads, Android devices, Windows & Mac PCs, Window Servers and USB storage devices. This unique system allows you to remotely manage encryption and 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 – such as 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 of suffering a catastrophic data breach. Fortunately, Beachhead offers BeachheadSecure USB Storage, 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 and Android and iOS phones and tablets, but now also 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. However, while encryption is necessary, it is insufficient data protection by itself. Circumstances change, and when a password is known or can be exposed, encryption cannot protect your organization's data. You must have the ability to plan and respond to evolving security risks.

## Protection for USB Storage devices: extended encryption, authentication policy, visibility and access control

Intimately coupled with PC & Mac security is the ability to enforce security policy to USB devices plugged into PCs. BeachheadSecure USB Storage will enforce encryption and an authentication requirement for any storage device holding your sensitive data. An installed communications module provides you with visibility and complete access control over a USB device, including the ability to deny access or kill compromised data. Flexible authentication settings will allow local authentication (user name & password),

or require authentication to your administration console, giving you the ability to revoke authentication at any time. Flexible settings allow for credential caching, waiver of authentication requirements under certain circumstances, and much more. Backed by these features, BeachheadSecure USB Storage is the ultimate extension of data security on external devices.

## 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 organization's 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 its contents. This way, if the device has been reported lost or stolen, authentication privileges are revoked – even with the right username and password – and no one will have access to its contents. This silent and automatic communication gives you the final say on who accesses your organization's data, and under what circumstances.



For more information call  
408.496.6936 or email  
[info@beachheadsolutions.com](mailto:info@beachheadsolutions.com)

©2022 Beachhead Solutions Inc. All rights reserved. Beachhead Solutions and the design are trademarks of Beachhead Solutions Inc. All other trademarks and registered trademarks are the property of their respective owners. BHSUSB522