

# BeachheadSecure™

## PC and mobile device security for Service Providers

Finally. An insanely easy approach to safeguard confidential, sensitive and personal data on PCs and mobile devices including USB storage drives. BeachheadSecure is an affordable managed service that gives you the ability to enforce encryption and security policies for your organisations' devices in a framework that makes risk mitigation and proving compliance an absolute breeze.



### Who needs this? Your practice does!

And if you haven't already asked why, you must. Nearly every organisation is affected by a growing list of data protection requirements where encryption is recommended or specifically mandated (e.g. POPIA, GDPR and PCI/DSS) that call for the protection of personal, consumer and sensitive data. What about client-confidential data and emails entrusted in your custody! Today this sensitive data is widely proliferated on Windows and Mac PCs, Android and iOS phones and tablets and USB storage devices - all of which are highly vulnerable to loss or theft. Information security guidelines typically stipulate the use of encryption as a vital technical control by all Service Providers to safeguard data on both company and employee-owned devices!

### As the name implies,

BeachheadSecure is an innovative tool designed to be transparent enough for users to ensure maximum productivity and is easy enough for any Service Provider to deploy and use either as a self-managed subscription or a monthly managed service without the requirement of hosting any hardware or supporting software — a Beachhead partner will get you sorted to simply secure your devices!

### Confidential data security your clients will appreciate.

Encryption is just the beginning and is required to ensure compliance to POPIA, GDPR and the Professional Body mandates. But encryption alone cannot protect your data if the password is compromised or if the device is already authenticated. BeachheadSecure gives Service Providers the patented ability to deny and restore access to data remotely ("data quarantine"), destroy at-risk data or to perform a number of other remote protections to ensure your (and your stakeholders) data is safe from compromise, even for your USB drives (inc. memory sticks) not in your possession.

Smartphones have become the single most carried, most valuable life tool with access to wads of sensitive & confidential data. What happens to that data if the phone is lost or stolen? Beachhead Phones and Tablets to the rescue! Encryption, application management, password enforcement and data elimination are just some of the capabilities that are at your disposal.



### Benefits

<b>Enforced Encryption</b>	Ensures compliance to legal obligations & stakeholder mandated information security guidelines
<b>Quarantine &amp; Data Lock</b>	Mitigate the risk of data exposure to any unauthorized user or thief when a device is lost, stolen or impounded or kept off the internet
<b>Remote Wipe</b>	Kill access to sensitive or confidential data when a device is reported stolen or as needed. <i>Mission Impossible</i> , made possible!
<b>Instant Lock</b>	Immediately eliminate access to phone and tablet devices if lost, stolen or impounded
<b>Data Isolation</b>	Securely shield data between users on Windows PCs so when you need to give your PC to the "IT Guy" to fix, be assured your data remains inaccessible to them - unless you choose to provide access!
<b>Mobile Wi-Fi Provisioning</b>	Automatically and simply set up access to your organizational wifi connections on phones and tablets without users ever knowing the password. Also remotely decommission wifi access to prevent employees, volunteers & contractors leaving the organization with continued access to the network without disruption caused to current wifi users
<b>Device Auditing &amp; Compliance Reporting</b>	Leverage device telemetry for forensic, auditing or reporting purposes for any of your secured devices, be it Windows or Mac PCs & laptops, encrypted USB storage, and Android and iOS phones and tablets. One-button "Compliance Report" to demonstrate security and compliance for client custodial data.

### What customers have to say:

*"[Beachhead] incorporates valuable functions deeply appreciated by [ ] wanting to protect the data on their devices and needing evidence of these controls and measure. It is also great that the vendor is backed by good technical support and great service from its regional distributor. This was all experienced with a deployment at a corporate bank in Harare desiring a co-managed IT (CoMIT) service. We evaluated and proposed the solution to our client since learning that BeachheadSecure is now available - and affordable - to African MSPs like us."*

**John Tseriwa, Director,**  
Sagehill Business Solutions.



**BEACHHEAD**

All things mobile. BeachheadSecure™

For more information about BeachheadSecure please contact:

**Amit Parbhucharan**  
amitp@beachheadsolutions.com