

BeachheadSecure™

PC and mobile device security for
Financial Advisors, Brokers & Underwriters

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 firm's 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 and the Financial Sector Conduct Authority (FSCA) stipulate the use of encryption as a vital security control by all Financial Advisors, Brokers & Underwriters to safeguard data on both entity 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 entity 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 entities 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 clients) 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? BeachheadSecure Phones & Tablets to the rescue! Encryption, application management, password enforcement and data elimination are just some of the capabilities that are at your disposal.

Financial Advisor, Broker & Underwriter

Benefits

Enforced Encryption	Ensures compliance to legal obligations, Financial Sector Conduct Authority (FSCA) & industry body information security guidelines
Quarantine & Data Lock	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
Remote Wipe	Kill access to sensitive or confidential data when a device is reported stolen or as needed. <i>Mission Impossible</i> , made possible!
Instant Lock	Immediately eliminate access to phone and tablet devices if lost, stolen or impounded
Data Isolation	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!
Mobile Wi-Fi Provisioning	Automatically and simply set up access to your entity wifi connections on phones and tablets without users ever knowing the password. Also remotely decommission wifi access to prevent employees, associates & contractors leaving the firm with continued access to the network without disruption caused to current wifi users
Device Auditing & Compliance Reporting	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 Beachhead customers have to say:

"Part of our decision to select BeachheadSecure for our mobile and workstation data encryption – and to assist us in our POPIA compliance strategy – was due to its implementation simplicity and user experience. Other data encryption solutions we looked at were difficult to set up and even harder to manage. We desired a solution that would not interfere with our users and their productivity in any way, but that would still give us the high level of security and audit reporting we require. Beachhead's technology has helped us greatly in our security and POPIA compliance efforts."

Ralph Hopkins, Head of Information Technology,
Cliffe Dekker Hofmeyr Inc.

All things mobile. BeachheadSecure™

For more information about BeachheadSecure please contact: