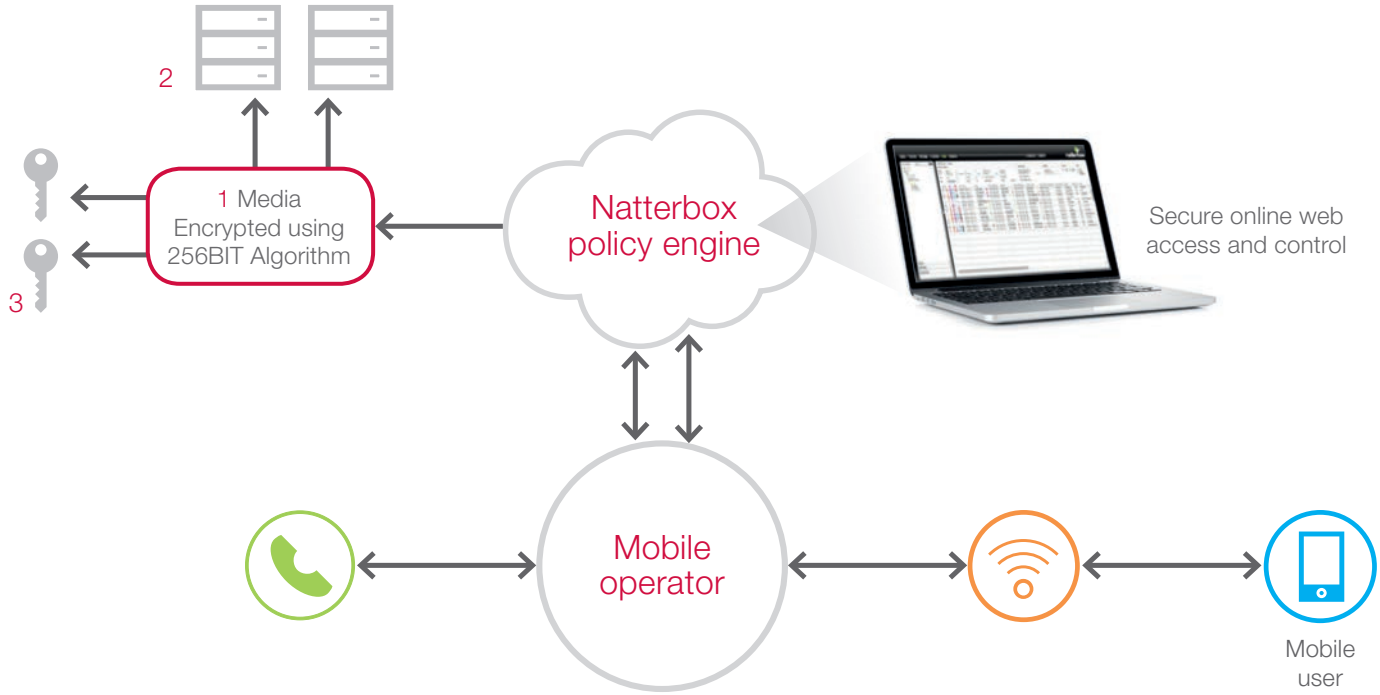
Mobile Voice Recording: Security Overview

Call Capture & Storage

1. All calls captured are encrypted with a 256bit encryption key unique to your organisation.
2. The encrypted media is sent for storage via secure and dedicated links to dual, geographically separated data centres - and replicated to multiple storage devices, ensuring complete data redundancy.
3. Encryption keys are stored in separate data centres to the encrypted recordings. Separate encryption keys are allocated for each organisation or group.



Data Access

Data is separated logically for each organisation or group, ensuring that an authorised administrator for one user group cannot access the recordings of another user group.

Access to your organisation's call recordings can be restricted to defined IP addresses (therefore specified, approved locations) - and password complexity is enforced.

Adam Phones
Intelligent Integrated Communications

Multi-Factor Authentication

Multi-factor authentication provides a method to harden the authentication process, which identifies a user. In addition to the typical single-factor authentication (usernames and passwords), multi-factor security adds a further layer of required information that must be provided in conjunction with the username and password.

Rather than the additional piece of information being something the user also knows (such as a memorable word)
it derives from something the user owns (their mobile device), and is dynamic in nature (updates at regular intervals).

Natterbox's multi-factor authentication uses a dynamic key generator app, compatible with iOS, Android and BlackBerry. Each portal administrator must have their device with them in order that a code generated by the application (which updates every 30 seconds) can be entered, along with the username and password.

The organisation can choose that all users must use multi-factor authentication to access the portal, with configuration and setup of the key generator taking place the first time a user logs in.

Call Recording Playback

The requesting administrator / compliance officer can review call recordings using two methods, as below. When a call recording is captured, the playback method is defined within the policy - allowing ultimate control, protection and flexibility.

1. Media download - all recordings can be downloaded and played in local media applications on the desktop.
2. Streamed media - all recordings will be streamed through a dedicated player embedded into the Natterbox portal. This player does not allow the recording to be saved locally, and no temporary copies of the file are made either.

Inactivity Timeout

The portal screen times out automatically after a period of 15 minutes inactivity, to prevent accidental exposure to the system. The username and password must be re-entered to gain access to the portal, where all existing session settings are retained.