MIRRORMAZE COMMUNICATIONS
1 London Road Ipswich IP1 2HA UK
www.mirrormaze.io

# Introduction

The purpose of this document is to provide the reader with an overview of NimbusMobile, the Smartphone as a Service Platform. This document will describe the key capabilities of the Platform and services provided by Mirrormaze Communications Ltd.
This document is intended for potential buyers and procurement leads. If you have any questions regarding the content of this document, then please contact us at sales@mirrormaze.io

# Who is Mirrormaze Communications?

Mirrormaze Communications, founded by former National Security officers, specialises in enabling mission-critical communications and covert operations within secure, regulated, and high-trust sectors. We provide a suite of ESG-aligned, software-defined capabilities, including a Mobile Smartphone as a Service, Virtual Desktops for unattributable Internet access and disposable internet proxy infrastructure designed to overcome the unique operational, compliance, and security challenges of conventional systems. Our solutions deliver scalable, reliable, and confidential capabilities that empower organisations to maintain operational integrity and regulatory assurance in even the most demanding environments.

# What is NimbusMobile

NimbusMobile is a secure, cloud Smartphone as a Service platform that solves the "multi-phone problem" for UK public sector organisations. It eliminates the operational risk and logistical burden of procuring, maintaining, and carrying multiple physical "burner" handsets and SIM cards.

Traditionally, teams have had to manage a complex inventory of physical mobile phones to maintain different legends or access mobile-only apps. NimbusMobile consolidates this entire physical inventory into a single, secure dashboard accessible via a standard web browser or the NimbusMobile app on a mobile device.

**Replacing the "Box of Phones"**
NimbusMobile virtualises the experience of holding a physical device, moving the hardware from the user's pocket to a secure, remote data centre.

Remote Access to Real Hardware: Users can access Physical Android Devices (such as Samsung and Nokia) and Virtual Android Devices (such as Graphene, Cuttlefish, Pixel or custom images) directly through their browser or the NimbusMobile App. This allows for genuine interaction with mobile-first platforms (like TikTok, Snapchat, or WhatsApp) that

often block standard emulators, without the user ever needing to touch the physical equipment.

Integrated Mobile Numbers & Telephony: The platform removes the need to physically swap SIM cards or manage top-ups. Real UK and International Mobile Numbers are integrated directly into the dashboard, enabling operators to receive SMS One-Time Passwords (OTPs), handle verification codes, and conduct VoIP calls instantly. This streamlines the creation and maintenance of social media accounts that require mobile verification.

Centralised Command & Control: Instead of managing evidence across ten different physical phones, all data is handled within one secure environment. A unified dashboard provides centralised access control, ensuring that device allocation can be managed instantly (e.g., reassigning a "phone" from one user to another) without physically handing over a device..

# How does it work?

The Platform is hosted within AWS London. This ensures that all customer data, user management logs, and virtualised infrastructure remain within UK legal jurisdiction, meeting data sovereignty requirements for UK public sector organisations. NimbusMobile manages the availability, security updates, and device farm maintenance, allowing customers to focus purely on investigations.

To support physical device integration, NimbusMobile provides proprietary Device Hubs. These hubs act as the bridge between the customer's local physical devices (e.g., specific handsets procured by the customer) and the NimbusMobile software stack, enabling secure remote orchestration of local hardware.

NimbusMobile can be accessed from any mobile device using the NimbusMobile App. It is securely available for download from both the Apple App Store (iOS) and Google Play Store (Android).

**Configurable Attributes include:**

- Network & Location: Public/Private IP addresses and Mobile GPS coordinates.
- Device Fingerprint: Operating System and browser configurations.
- Environment: Pre-installed applications and extensions tailored to the persona.
- Connectivity: Disposable mobile phone numbers and local exit points.

# What can it be used for?

NimbusMobile is designed to support a wide spectrum of digital investigations, from passive intelligence gathering to active undercover engagement. It allows operators to apply professional tradecraft in a secure, audited environment.

**False Online Persona Management**
Solve the logistical challenge of maintaining multiple online identities. Users can create and sustain credible False Online Persona accounts on major social media platforms.. The integration of real Mobile Numbers enables the immediate verification of these accounts via SMS/OTP, while the Physical Device Farm ensures the "device fingerprint" matches a real device, preventing accounts from being flagged as bots or banned.

**Investigations on "Mobile-First" Platforms**
Target platforms that are not accessible via desktop browsers. NimbusMobile provides access to these platforms from the user's desktop browser. This allows users to view content and interact with platforms that would otherwise be inaccessible.

**Information Capture & Audit**
NimbusMobile allows users to securely capture information from Mobile-First Platforms. This enables users to capture transient or view-once data that would ordinarily have been lost using traditional emulators or handsets.

**Geographically Specific Investigations**
NimbusMobile enables users to conduct investigations that require a specific geographic presence. Using the Unattributable Proxy Infrastructure and location spoofing, users can appear to be browsing from specific countries or regions, allowing them to bypass geo-blocking, view localised content.

MIRRORMAZE COMMUNICATIONS
1 London Road Ipswich IP1 2HA UK
www.mirrormaze.io

# Service Benefits

**Force Multiplier for False Online Personas**
As with all our platforms, NimbusMobile decouples the digital identity from physical hardware, allowing a single investigator to build, maintain, and operate multiple distinct personas simultaneously with significantly reduced effort.

**Cognitive Efficiency**
Remove the mental burden of "technical tradecraft." NimbusMobile handles complex device fingerprinting and network miss-attribution. This allows the user to focus entirely on engagement and intelligence gathering without worrying about technical operational security issues that can undermine operational outcomes.

**Operational Velocity**
Switch between isolated FOPs in seconds via a single intuitive dashboard. Unlike other solutions, there is no need to log into other profiles, physically swap devices, reboot, or manage a drawer full of phones. A single user can now effectively manage the "Pattern of Life" for multiple active personas in the time it takes a competitor to boot up two.

**Persistent State Management for Social Media Credibility**
Social media platforms, especially mobile-first ones, aggressively flag accounts that use IPs with a low reputation or emulators. NimbusMobile's infrastructure is specifically designed to enhance the credibility of online accounts.

**Collaborative Investigations**
NimbusMobile enables efficient and easy online account management across multiple platforms by giving users a single dashboard. Multiple authorised users can be granted access to online accounts and profiles. If a primary user needs to hand over an investigation, a colleague can seamlessly use active accounts and profiles immediately.

This capability allows a small team to project and maintain the operational capacity and velocity of a much larger team, delivering more outcomes with less time and resources..

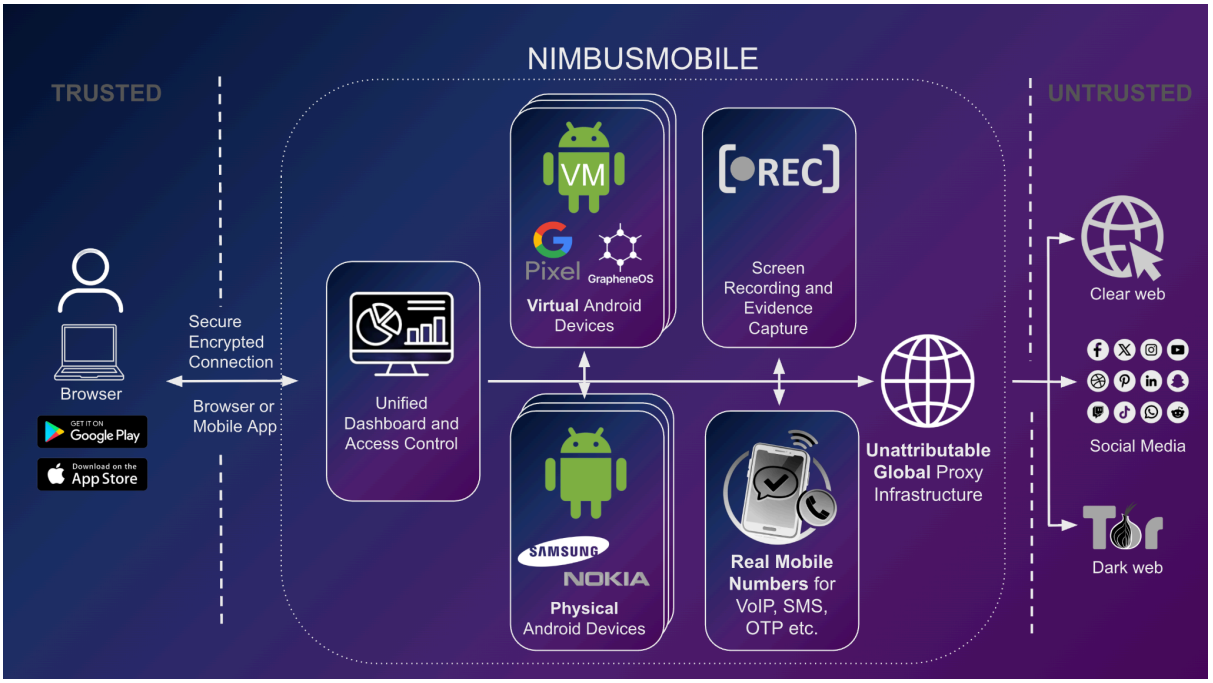
**Financial & logistical Efficiency**
Replace the expensive, slow logistics of physical procurement with instant software provisioning. Eliminate operational inefficiency of using multiple platforms that lack flexibility and have concurrency restraints. NimbusMobile allows customers to spin up a new, fully non-attributable desktop environment from trusted templates in minutes. Each Desktop Environment is preloaded with customer specific tools and users can install their own additional tools.

By consolidating multiple investigation tools onto a flexible single cloud platform, customers can reduce the procurement budget by up to 70%, reallocating those funds to frontline resources.

**Automated Evidence & Compliance**
NimbusMobile makes the administrative side of investigations much easier for users, ensuring they spend less time managing separate physical devices and more time investigating. The platform automatically records video and logs of all activity. This ensures that even fleeing evidence (like disappearing messages or live streams) is captured without the user needing to remember to press "record" or manually take screenshots.

# NimbusMobile Service Definition

## Design overview




The NimbusMobile architecture is engineered using the principles of Zero-Trust, Assume Compromise and Secure by Design. It physically and logically separates the user's local environment (trusted) from the target environment (untrusted), ensuring that no direct connection ever exists between the customer's infrastructure and the public internet.

The platform is composed of three distinct architectural layers:

**The Trusted Access Layer (User Interface for browser and app access)**
This is the only entry point for users. It is a secure, authenticated environment that provides command and control without processing any target data locally. A browser based interface

renders the visual output of the remote devices. It uses encrypted WebRTC streams to provide low-latency control. A native application (iOS/Android) that replicates the dashboard functionality for secure access on mobile devices. Role-Based Access Control (RBAC) ensures users only see devices and data relevant to their account. Collaboration can be configured which would allow multiple users access to the same devices.

**The Core Orchestration Layer**
Hosted in AWS London (for the SaaS model) or on private infrastructure, this layer manages the logic of the system. The Core Layer is also responsible for SMS and voice traffic from the telco provider's network. For physical device integration, proprietary Controller Boxes act as secure gateways. These hubs physically connect to racks of smartphones and provide seamless remote access.

**The Device Farm**
It is completely isolated from the Trusted Access Layer. Containerised Android environments (e.g. Google Pixel, GrapheneOS etc) running on high-performance servers. These are ephemeral and can be destroyed instantly. Real commercial smartphones (e.g. Samsung, Nokia, etc.) can be connected using Controller Hubs. These can be hosted securely on-prem or in a remote secure customer location.

**The Egress Layer**
A distributed network of exit nodes that anonymises the traffic and makes it appear to be genuine mobile phone traffic. It ensures that the IP address visible to the target website or app belongs to a generic ISP or mobile carrier in a specific geographic location, rather than a data centre or the customer's own infrastructure.

## Access control

Access to NimbusMobile can be configured in several different ways depending on customer requirements. It supports the following authentication mechanisms:

- Basic username and password
- Multi Factor Authentication
- Single Sign On using SAML2

Within the Platform access control is role based (RBAC). There are two levels of privilege within the Platform:

- Admin – This role has access to all the data produced by users that are assigned to them.
- User – This role is used by investigators and researchers.

## Auditing

Auditing user activity is one of the core capabilities of NimbusMobile. User activity within the Platform are captured and logged. All actions triggered by a user from the moment they log in to the moment they disconnect from devices are recorded in a secured audit database.

## Information Assurance

NimbusMobile is developed according to "Secure by Design" principles, leveraging the expertise of NCSC-certified security architects to ensure a robust and defensible architecture.
Mirrormaze Communications adheres to a rigorous Software Development Lifecycle that is based on NCSC secure development guidance[1] and the Microsoft Secure Development Lifecycle (SDL)[2]. As part of our development lifecycle, we conduct a range of security activities, including but not limited to attack vector analysis, dynamic security testing and regular developer security training.

[1] https://www.ncsc.gov.uk/collection/developers-collection
[2] https://www.microsoft.com/en-us/securityengineering/sdl

MIRRORMAZE COMMUNICATIONS
1 London Road Ipswich IP1 2HA UK
www.mirrormaze.io

# Service and Support

We provide **second and third-line support**, complementing your own first-line capability. Support Details:

- **Personnel & Location:** Our support service is UK-based, and some staff hold DV clearances.
- **Standard Service Hours:** Available Monday to Friday, from 09:00 to 17:00 (excluding UK Bank Holidays).
- **Standard Contact Methods:** Support is delivered via email
- **Enhanced Support:** An upgraded service is available for customers who require extended support hours and access to on-site and telephone-based support.

The standard service response times for incidents are detailed in the table below.

| Severity | Description | Response Time | Resolution Time | Response Updates |
|---|---|---|---|---|
| P1 | NimbusMobile is unavailable | 1 business hour | 24 hours | Every 2 hours within business hours |
| P2 | NimbusMobile performance is severely degraded | 2 business hours | 48 hours | Every 4 hours within business hours |
| P3 | NimbusMobile performance is degraded | 4 business hours | 72 hours | Daily (Business days) |
| P4 | Standard Support Request | 24 business hours | 5 working days | As required |