QuantumGate

SECURE VMI

Secure Virtual Mobile Infrastructure (VMI) for Government and Enterprise Security

DATA SHEET

quantumgate.ae

Overview

Our Secure Virtual Mobile Infrastructure is a solution that enables users to remotely access a secure virtual mobile environment using a personal or company-issued device. The environment, which can be hosted in the cloud or on-premises, provides secure access to a virtual mobile through a lightweight client application while maintaining centralized control and user isolation. It eliminates the need for sensitive data to reside directly on user devices, reducing risks associated with loss, theft, or compromise. It also eliminates the need for users to carry two phones.

Key Features

VIRTUAL ANDROID INSTANCES

Runs Android Open-Source Project instances on isolated virtual machines or containers.

TAILOR-MADE CLIENT

Lightweight application available on iOS, Android, Windows, Linux, and browser platforms to access remote Android instances.

SECURE MEDIA BRIDGE

Connects device peripherals, including the camera, audio, and Bluetooth, securely to the virtual Android instance, and supports multimedia applications such as Microsoft Teams.

END-TO-END DATA SECURITY

Implements a novel architecture in which user data is stored in separate, confidential computing nodes, enhancing data confidentiality.

SECURE BOOT AND HARDENED AOSP

Supports secure boot configurations and runs on a hardened Android Open-Source Project image for increased system integrity.

ATTESTATION AND TRUST MECHANISMS

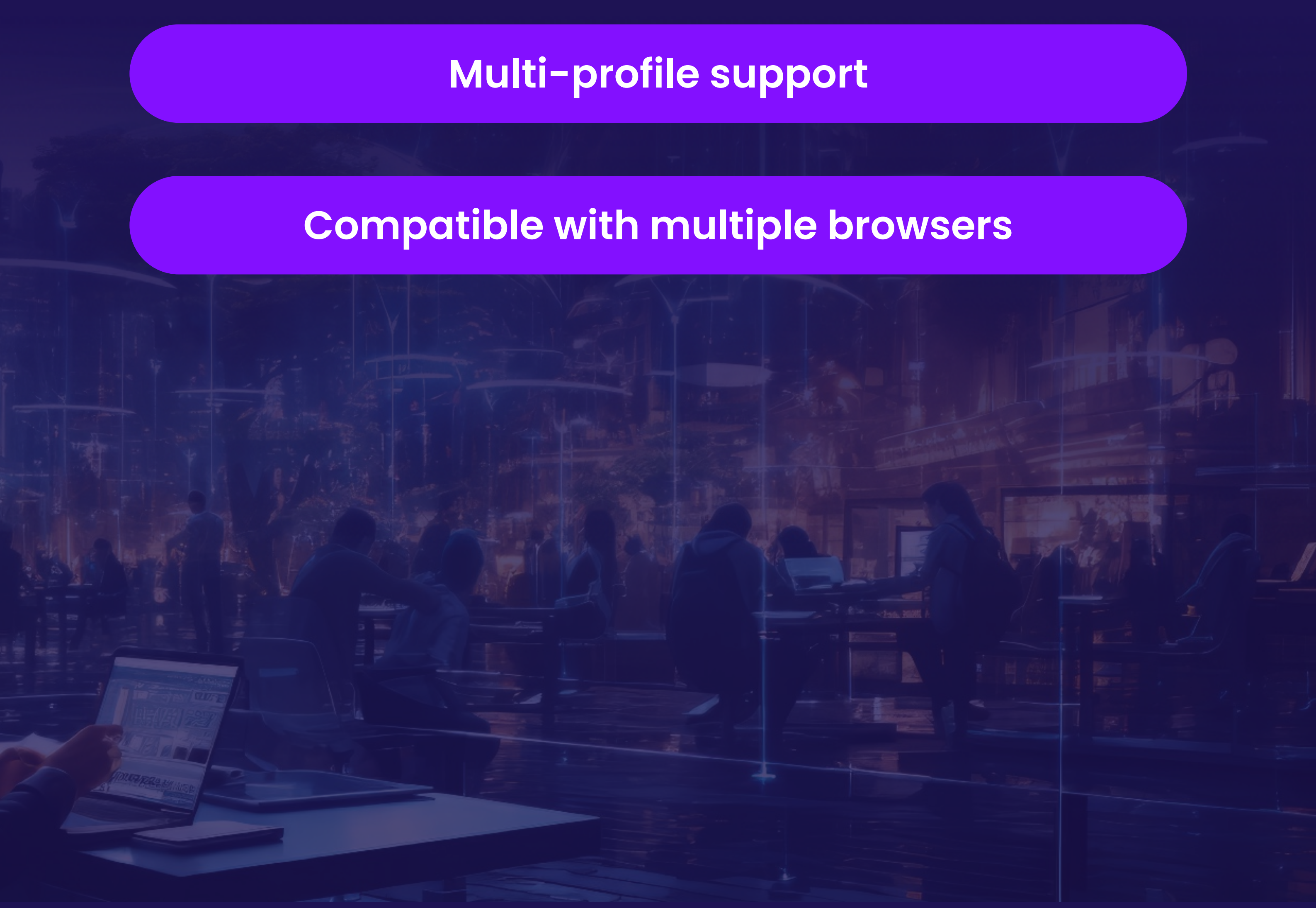
Leverages attestation within the cloud service infrastructure to verify the integrity of the backend environment.

SESSION-SPECIFIC CERTIFICATES

Uses unique credentials per session to ensure secure authentication and reduce long-term key exposure.

Other Capabilities:

- Integrated with third-party telephone capabilities
- Support for geolocation features
- Data sharing between cloud instance to physical device and vice versa
- One-time link sharing for live support use cases
- Multi-profile support
- Compatible with multiple browsers



Benefits:

DATA NEVER STORED ON DEVICE

No sensitive data resides on the user’s device. All interactions are streamed from isolated virtual Android instances hosted remotely.

MULTI-DEVICE ACCESS, INCLUDING BRING YOUR OWN DEVICE

Supports both personal and enterprise devices without compromising security. Accessible from various user devices. No need for users to carry multiple phones.

SCALABLE MANAGEMENT

Supports scaling to over 10,000 concurrent virtual Android instances with administrative orchestration for creation, revocation, and diagnostics.

HARDWARE ISOLATION BENEFITS

Protects against threats such as SIM card exploits, USB-based malware, and memory and baseband vulnerabilities by isolating the virtual instance from device hardware.

APPLICATION COMPATIBILITY

Validated compatibility with standard enterprise applications such as Outlook, Slack, and OneDrive through structured user testing programs.

Technical Specifications:

DEDICATED CLIENT APPLICATION

Required for secure session access. Available for iOS, Android, and browsers.

CLOUD BACKEND

Runs virtualized and isolated AOSP instances in containers or virtual machines. Supports attestation and secure boot.

MANAGEMENT FUNCTIONS

Tools for provisioning, diagnostics, user session recovery, and instance revocation.

SECURE MEDIA BRIDGE

Connects device peripherals to the virtual Android instance for secure multimedia use cases.

Supported Mobile Platforms:

iOS 16
and above

Android 12
and above

Supported Cloud Environments

GCP

Azure

Deployment Model

- Deployable on public cloud, private cloud, or on-premises infrastructure.
- Supports containerized or virtualized secure Android sessions.