Hypori
One Device, Zero Worries™

Physical devices vs. Hypori Virtual Workspace

A game-changer for security and management

Not a one-for-one swap

Managing mobile access to enterprise data is more complex and riskier than ever. Devices get lost, stolen, or compromised. Hypori offers a secure virtual workspace accessible from your personal phone or tablet, with no enterprise data stored on the device and total personal privacy.

This isn't a one-to-one replacement for a physical device. It's a smarter, more strategic model for mobile access. Hypori delivers zero-trust security, centralized control, and the flexibility today's fast-moving leaders demand.

Capability comparison

A side-by-side look at what you gain—and what shifts—when you move to Hypori.

Capability	Physical device	Hypori Virtual Workspace
Hardware/device ownership	User or organization-owned physical device with its own CPU, memory, and storage	Virtual devices hosted in the cloud/data center and defined by the enterprise. Role of physical devices is limited to functioning as a display mechanism
OS and app installation	OS & apps installed directly on physical device. OS and apps execute on physical device	OS and apps execute in a secure cloud; OS and apps are virtualized on physical device
Data processing and storage	Data is processed and often stored on physical devices. High risk of data loss if device is lost, stolen, or hacked	No data is processed or stored on the physical device. All processing and storage are done in a secure cloud
Security model	Device and apps are vulnerable to malware, theft, or unauthorized access; Security relies on physical device policies using 3rd-party software	Built on a "zero trust" approach —meaning it doesn't assume your physical phone is safe or secure. The use of virtualization technology ensures no data is ever processed or stored on your physical device. Even if bad things are happening on your physical device, your virtual workspace is protected and everything stays secure
Access and connectivity	Full offline functionality for apps and data that are not reliant on the web or cloud	Hypori requires network connectivity (Wi-Fi or cellular). It cannot be used offline
Calls and SMS	Make/receive calls, SMS/RCS, and MMS directly through their mobile carriers	Supports VoIP/softphone and messaging apps; traditional cellular calling or SMS/RCS is not stored locally
Hardware use	Direct use of GPS, camera, microphone, accelerometer, and other built-in sensors	Limited or indirect access to native hardware (e.g., camera, mic) via pixel streaming; GPS or sensors can be virtualized if needed

Hypori®

One Device, Zero Worries™

Physical devices vs. Hypori Virtual Workspace

A game-changer for security and management

Capability	Physical device	Hypori Virtual Workspace
User experience	Instant, responsive interaction	Rendering (i.e., display) of virtualized apps and data is network dependent; Actual apps and data processed at "cloud resource speed"
IT control and management	IT can deploy MAM/MDM solutions, user can install personal apps unless prevented by policy; difficult to enforce restrictions on unmanaged device	Virtual workspace protected by centralized provisioning, security policies, and app deployments; simplified compliance auditing; minimal exposure on devices
Scalability and deployment	You must physically acquire and provide each device	Instant provisioning of virtual devices; minimal new hardware is needed for the user
Compliance and audit	Logs and usage remain local; difficult to ensure compliance on personal devices	All logs and data can be centrally stored, tracked, and audited; easy to revoke/adjust user access from a single console
Device loss or theft	Risk of data compromise; need mobile device management in order to wipe apps/data	No apps or data on the endpoint; strong user authentication; revoking the virtual workspace instantly blocks access

Key Takeaways

Security

- Physical devices store data locally, creating risk if the device is lost, stolen, or compromised.
- Hypori keeps all enterprise data in a secure cloud or data center, with nothing stored on the device.

Connectivity

- Physical phones can work offline—supporting calls, texts, and local apps without a connection.
- Hypori requires internet access, as it streams a secure virtual device from the cloud.

Hardware Integration

- Physical phones rely on MDM or company policy to control usage and data security.
- Hypori can virtualize these capabilities or sensors, but performance and access may be subject to network or policy constraints.

IT Control

- Physical phones rely on MDM or company policy to control usage and data security, often with limited visibility.
- Hypori centralizes app deployment and data storage for stronger compliance, easy revocation, and reduced endpoint risk.

Physical devices offer local storage, full hardware access, and offline capability but at a cost. Data is exposed. IT control is limited. And scaling across users requires hardware, logistics, and risk.

Hypori Virtual Workspace delivers a "no data at rest" solution, centralized IT oversight, and scalable deployment, eliminating the need to issue or carry multiple devices. While Hypori requires reliable connectivity and may limit direct access to some hardware features, Hypori offers a more secure, flexible, and modern approach to mobile access.