U.S. ARMY

ARMY BYOD with Hypori

An enterprise capability now offering secure virtual mobility

Secure access to NIPRNet, MS Teams, email, CAC-enabled websites, and more from your personal mobile device.

Enroll Now





Private

- Total user privacy
- The Army NEVER has access or visibility into your personal device or personal data

Secure

- Authorized to process CUI securely & conduct official business from your personal device
- No data in transit, no data at rest – your personal device presents no risk to government network
- Send and receive encrypted emails

Simple

- Only carry one device
- No CAC needed to login



Army BYOD with Hypori

No data to lose. No data to leak. No data to wipe.
No need to seize the user's device.

Act Now

Access the BYOD Hypori Hub from a CAC-enabled device to learn more and enroll at armyeitaas.sharepoint-mil.us/sites/hypori

Learn more:
hypori.com/army-byod

LEARN MORE

ARMY BYOD with Hypori

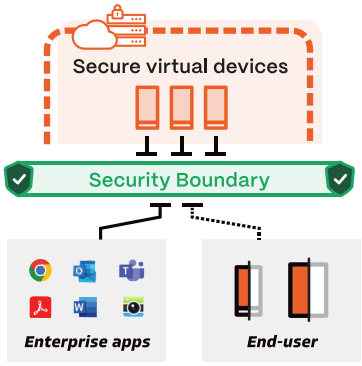
U.S. ARMY

Maintains Total Privacy for the End User

Hypori security boundary protects Army data and user privacy.

Army BYOD using Hypori delivers secure access to Army 365, Teams, MyPay, CAC-enabled websites, and more via a separate, secure virtual device from any smartphone or tablet.

Army BYOD with Hypori



- **Encrypted pixel transmission to/from the end-user device**
- **The virtual device is 100% separate prohibiting the Army from accessing the users personal data on the physical device**
- **Army data never leaves the IL5 cloud, therefore it is never stored on the end-user device**
- **No data on the device means NO NEED TO SEIZE THE USER'S DEVICE**

How does Hypori ensure user privacy?

Does the Army have access to my personal data and activities?
(i.e., browsing history, downloads, photos, calls, texts, etc.)

No! The Army NEVER has access to the user's physical device. Unlike DMUC devices or organizations that use mobile device management apps on employee phones, Hypori does not have the ability to view or access the user's personal information on the physical device.

Will the Army need to seize my phone?

No! No data transmitted to and no data stored on the device means there is no data to lose, no data to leak, no data to wipe – no need to seize the user's device.

Do the files I access from the IL5 cloud get stored on my device?

No! Only encrypted pixels travel to and from the physical device. No data is stored on the user's device.

What permissions will Hypori need on a user's smartphone?

The user controls Hypori access to the physical device sensors (i.e., microphone, camera, location, etc.) Hypori is NOT mobile device management (MDM) or mobile application management (MAM) software. It does not require root access to the physical device. Any permissions granted within the Hypori virtual workspace are limited to that virtual workspace (residing in the IL5 cloud) and have no bearing or impact on the physical device.

Enroll today from a CAC-enabled device at armyeitaas.sharepoint-mil.us/sites/hypori

Learn more: hypori.com/army-byod