Photo courtesy of U.S. DoD, Samuel King. The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.

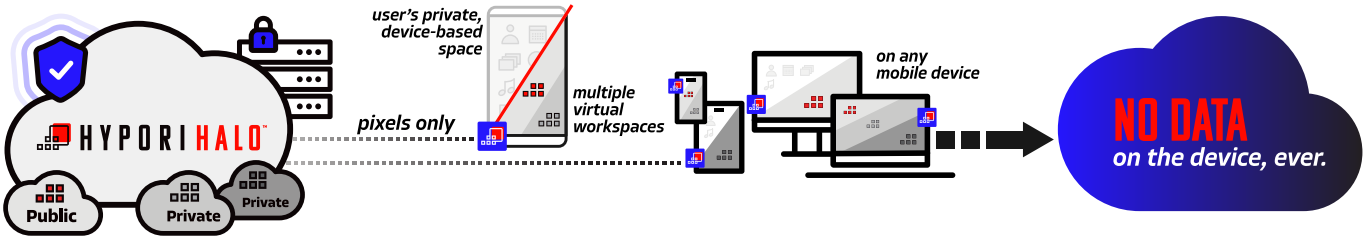
BYOD for U.S. DoD

Hypori Halo: the only tested and certified Bring Your Own Device (BYOD) platform used by the DoD.

Department of Defense (DoD) personnel need secure digital access to government data and applications from their personal devices easily, at scale, and without risk of data loss and privacy breach. Hypori Halo works on any device by eliminating the edge as an attack surface and preventing data at rest or in transit outside the enterprise, freeing the government from liability and security risks with 100% separation of data and preserving privacy for the end-user.

Rigorously tested and approved by the Department of Defense (DoD) Threat Systems Management Office (TSMO), the Director, Operational Test & Evaluation (DOT&E) Red Team validated Hypori Halo as the "most secure technology tested to date, with zero significant security findings."

Hypori Halo's zero-trust architecture enables secure user access to apps and data in the cloud or a customer data center from any Android, iOS, or Windows 10 device. The user accesses the apps and data through a separate, secure, virtual workspace streamed to the physical endpoint device. It is this separation and virtualization that is unique to Hypori's solution. There is 100% separation between the Hypori Halo virtual workspace and the user's personal workspace. There is no risk of data leakage or risk of data being stolen from the device because there is never any data at rest on the device. With zero data at rest and total separation, the user has complete privacy, and the organization is not liable for the user behavior.

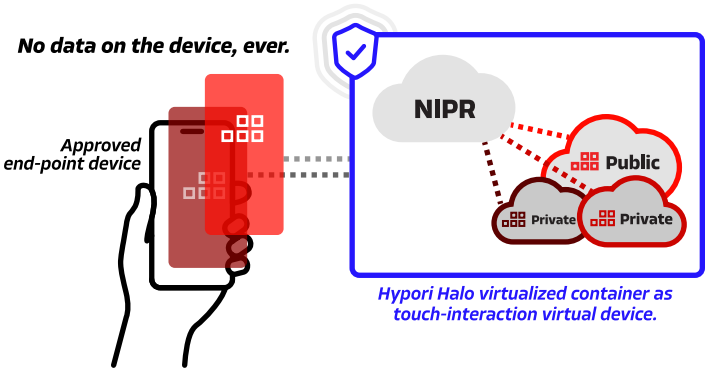


End users install the Hypori Halo App on their existing Android, iOS, or Windows 10 device, providing a secure and convenient method for accessing their Hypori virtual workspace. The Hypori Halo App leverages FIPS 140-2 crypto and TLS 1.2 encryption, supports PKI credential-based multi-factor authentication, and is NIAP Common Criteria certified.

Use Case

The National Guard trusts Hypori to provide secure access to NIPRNet from a personal device

Persistent threats against military networks are a key driver for cybersecurity and digital transformation. The Army's digital transformation plan will synchronize all its technology modernization efforts and better posture itself for multidomain operations.



The Army has nearly 500K National Guard and Reserve soldiers with regular day jobs, and many of them already have their primary employer mobile device management (MDM) on their device, therefore choosing an additional software management solution isn't an option for the Army since two MDM applications cannot run on a single device. Hypori Halo is the only secure option that enables the Army to maximize the use of their O365 Agreement without having to manage the Soldier's personal device. This eliminates the Soldiers' privacy concerns as well as the Army's liability risk of having access to personal Soldier information.

The National Guard chose Hypori Halo to enable secure BYOD access to CUI enterprise data and apps.

- Enhanced security as validated by the Army's TSMO Red Team.
- No data on the device, ever.
- Zero exposure from lost or stolen devices.
- Cost savings of 5x over Government Furnished Equipment (GFE).
- 100% separation of data means Army is not liable for the users' activities.
- Soldier's privacy is protected.

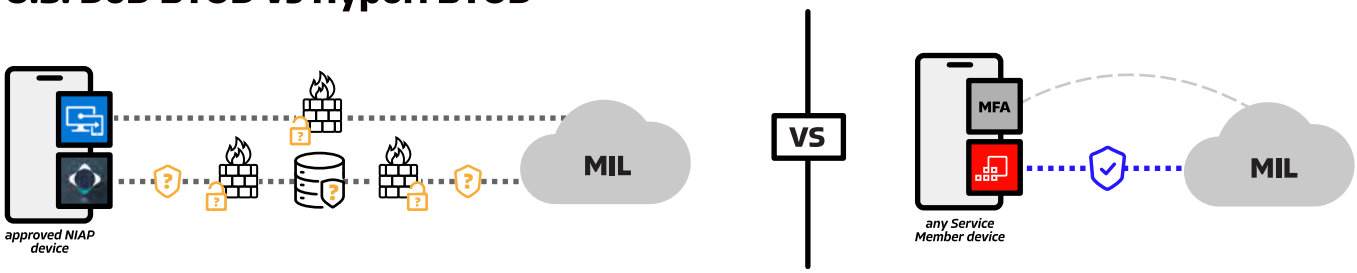
No data on the device, *ever*.

Speed to scale quickly empowers Soldiers on their personal devices while mitigating risk of data loss, privacy breach, and litigation.

The current DoD BYOD program requires security waivers to operate and makes the DoD liable for having access to personal information.

The DoD EULA for BYOD states, "The MDM and other applications are considered government-furnished equipment, and you are responsible for any malware from your device that penetrates the MDM and causes harm to any government information system."

U.S. DoD BYOD vs Hypori BYOD



Hypori Halo integrates with existing DoD software, Microsoft Intune, for enhanced O365 Identity Management options.

Advantages of Hypori Halo:

- Scale quickly with 1 click access to Hypori Halo on any endpoint.
- Does not require permissions on Soldiers' devices to ensure privacy.
- Eliminates spillages on physical edge devices.
- Removes DoD liability for Soldiers' mobile personal activity.
- One license for multiple devices, optimizes investment opportunity.
- Opportunity for laptop and desktop replacement where appropriate.
- Users can access any DoD-approved application from a list of hundreds of approved applications.

With Hypori Halo, DoD personnel can securely access government data and applications from their personal devices, they can operate confidently knowing their personal data remains private, and the DoD isn't liable for Soldier personal activity on the device.

Improve

- Soldier experience
- Soldier privacy
- Security for DoD data

Eliminate

- DoD liability on Soldiers' devices
- DoD responsibility for malware on Soldiers' devices
- Privacy concerns
- Data leaks

Reduce

- DoD investment in mobile administration
- Risk of data loss, privacy breach, litigation

Request a Demo:

Click for demo