

Streamline Mobile CMMC Compliance

Quickly meet CMMC requirements, preserve remote workforce privacy, and increase productivity by enabling access to secure environments and protecting CUI on any mobile device, anywhere.

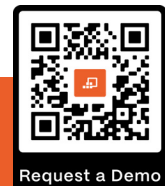
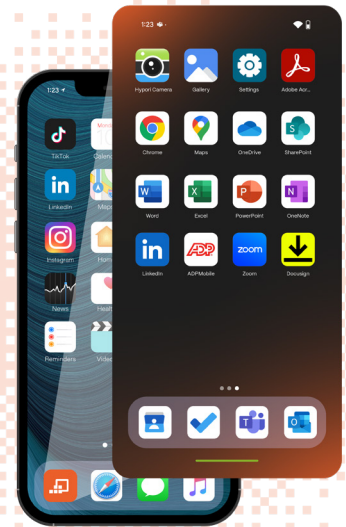


Increase Security and Protect Privacy while Reducing Risk and Cost Hypori for Defense Industrial Base Contractors


As the largest classified mobility provider in the Department of Defense, Hypori is enabling bring-your-own-device (BYOD) programs across regulated industries and the defense industrial base (DIB) through our secure workspace solution. Hypori is an app-accessible, separate, secure mobile workspace delivering encrypted access to enterprise apps and data from any smartphone or tablet.

Hypori accelerates Cybersecurity Maturity Model Certification (CMMC) compliance and reduces cybersecurity risks by transmitting only encrypted pixels and never storing, transmitting, or processing data of any kind on the physical device hosting the virtual workspace. This ensures 100% separation of corporate, government, and personal data while preserving end-user privacy.

- Access corporate, IL4, IL5, Microsoft GCC-High, PreVeil, and Google Workspace environments from a single smartphone or tablet.
- Prevent data spillages and exposure from lost/stolen devices with no data – CUI or FCI – at rest.
- Reduce hardware spending and attack surfaces while empowering hyper-mobile workforces on their personal devices.
- Zero-trust mobile workspace operates in AWS GovCloud, 100% separate from the user's personal data preserving total user privacy.




Future-proof your CMMC mobile strategy with Hypori




Enable BYOD for remote access to multiple secure environments from employee personal mobile devices.



Reduce the attack surface from 1000s of devices to a single cloud instance.



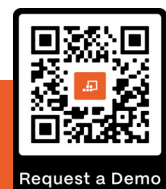
Accelerate CMMC compliance with FedRAMP High (in process), NIAP Common Criteria certified, zero-trust technology that adheres to DFARS for protecting CUI based on NIST 800-171.



Empower global workers on personal devices with 100% user privacy. No need for corporate-issued mobile devices or managing fleets of phones.

No data at rest means no data at risk and swift CMMC compliance using Hypori to secure CUI. **No MDM can do that.**

CMMC 2.0	CMMC 2.0 Req	Hypori	MDM
3.118	Control connection of mobile devices.	Hypori provides credentialed access that is fully managed, controlled, and observed.	Restricted mobile device options; varied use acceptance; onerous on company IT to roll-out and enforce.
3.119	Encrypt CUI on mobile devices and mobile computing platforms.	No data of any kind ever on the mobile device. Hypori encrypts the enterprise data in the cloud file storage.	Vulnerable to root kits to bypass security controls on device.
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmissions unless otherwise protected by alternative physical safeguards.	Hypori uses an encrypted TLS tunnel to protect accessed enterprise data from the virtual device to the cloud.	Requires VPN apps to protect the communications in transmission.
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Hypori uses FIPS-validated cryptography to protect all CUI in the cloud - proven to be secure.	Uses FIPS-validated cryptograpy on the device subject to device-level unauthorized access.
3.13.15	Protect the authenticity of communications sessions.	Hypori uses a variety of security controls to validate the user and device access to the cloud.	Subject to maintaining the security of the device, user data, and CUI storage.
3.13.16	Protect the confidentiality of CUI at rest.	Hypori never transmits, processes, or stores data of any kind on the physical device hosting the virtual workspace.	Cannot guarantee CUI protections on device.



Hypori enables BYOD programs that meet CMMC "data at rest" requirements on any smartphone or tablet, eliminating the need to purchase, distribute, and manage corporate devices while protecting government data from malware and data-harvesting apps like TikTok.

Reduce IT administration, capital expense, liability, and risk with the only DOD CIO-approved BYOD program in use by the DOD.

Trusted By:



U.S. ARMY



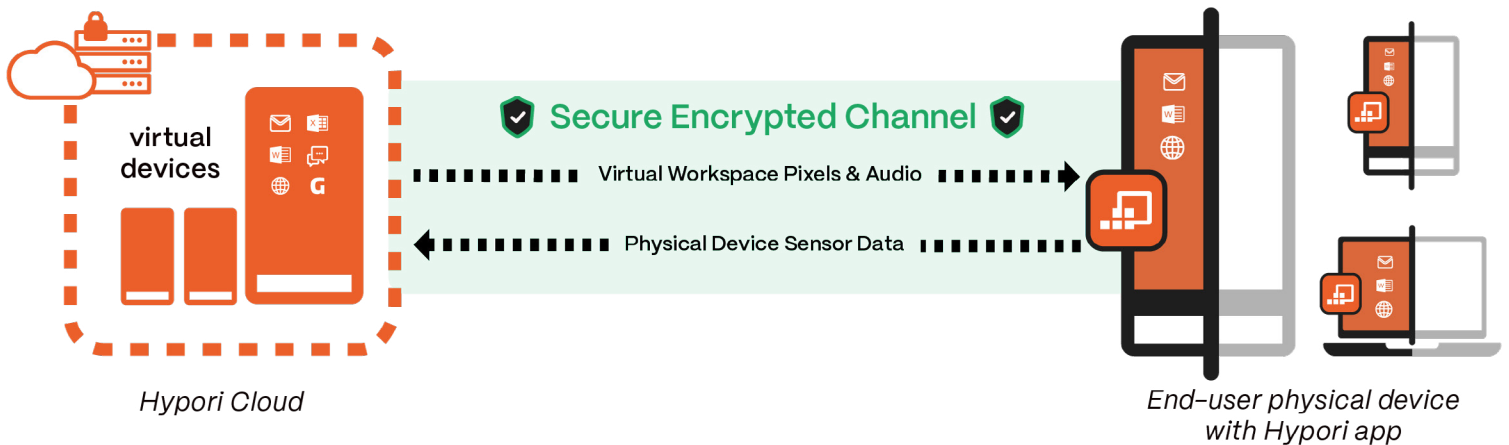
U.S. AIR FORCE



UNITED STATES
SPACE FORCE

Hypori is a U.S. Army, Air Force, and Space Force enterprise-approved solution providing BYOD access for service members, civilians, and contractors worldwide.

Reduce IT admin and eliminate hardware and device management.



Protecting everything that's important
—your enterprise and your people.

How can Hypori accelerate your CMMC
compliance journey? **Let's talk.**



80 Sec Demo



Email Us