# Achieve CMMC 2.0 Compliance with Hypori Halo
Safer. Faster. Better.

Hypori's secure mobility solution helps the DIB address CMMC 2.0 requirements by improving security efforts and reducing risk.

With cyberattacks on the rise, controlled unclassified information (CUI) among defense-related businesses is increasingly at risk. Therefore, the Department of Defense (DoD) is mandating the DIB to meet new security requirements in DoD contracts with a Cybersecurity Maturity Model Certification (CMMC) for better cybersecurity protection, awareness, controls, and hygiene.

Hypori is an NSA CSfC Compliant vendor under the Mobile Access Capabilities Package. We also meet the NIAP Common Criteria and are FIPS 140-2 Certified.
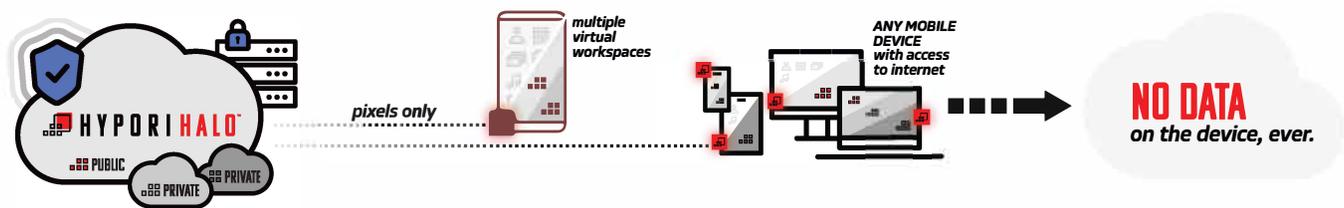
Compliance Challenges

- Lost/stolen devices create massive exposure risk (70M stolen/lost in the U.S. alone in 2020)

- Providing and maintaining corporate-owned devices is costly

- MDM is ineffective and risky

- Security & compliance restrictions impact mobile usability

- Breached mobile devices result in loss and/or damage to reputation

- Rigid mobile accessibility constraints in secured and unsecured environments

Hypori Solution

- **No data on the device, ever.** Zero exposure from lost/stolen devices.

- Enable BYOD (Bring Your Own Device) and access multiple environments from a single device

- No MDM required

- Easy path for regulatory compliance (CMMC, GDPR, CCPA, etc.)

- **Zero-trust architecture** ensures no data exposed, plus 100% isolation from personal data

- Access secure environments remotely from any device (cell, laptop, tablet)

> **Hypori Halo addresses the most challenging CMMC 2.0 requirements better than mobile data management (MDM) solutions.**

MDM is not as secure and presents a spectrum of liability and exposure.

| CMMC 2.0	CMMC 2.0 Req	Hypori	MDM
3.1.18	Control connection of mobile devices.	Hypori provides credentialed access that is fully managed, controlled and observed.	Restricted mobile device options; varied user acceptance; onerous on company IT to roll-out and enforce.
3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.	No data of any kind ever on the mobile device. Hypori encrypts the user 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 transmission unless otherwise protected by alternative physical safeguards.	Hypori uses an encrypted TLS tunnel to protect the data from the client to the virtual device.	Require 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 user data in the cloud – proven to be secure.	Uses FIPS-validated cryptography 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.	No data at rest on the device, EVER.	Cannot guarantee CUI protections on device.

Why Hypori?

Hypori enables secure access to classified networks via mobile devices while satisfying contractual requirements with the U.S. Military and Intel communities.

- **Secure** - Massive risk reduction from all edge devices down to single cloud instance
- **Separate** - 100% separation of personal and corporate data for complete privacy
- **Simple** - Scalable SaaS offering on cloud with simple, central administration
- **Cost effective** - Corporate-owned device programs are a cost and administrative burden
- **Proven** - Trusted by the most demanding military and national security organizations

Don't delay, your data is vulnerable.

Request a demo on our website to discover how Hypori Halo can secure your CUI to overcome CMMC challenges with a simple, cost effective, and better solution, or reach out to one of our team members below.
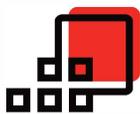
Hypori is the award-winning SaaS company transforming secure mobility for Federal and Commercial customers. Our innovative solution puts the power and speed of the cloud on any mobile device to enable remote users access to critical data and apps through a separate, secure virtual workspace. From commercial IP to national security level intel, Hypori Halo protects data from every type of threat with zero data at rest.