Secure.	Private.	Cost-Effective.	Convenient.	Compliant.

Proven Security AND Total Personal Privacy.	Hypori enables secure virtual access from any mobile device to enterprise apps and data (e.g., CUI or FCI). Trusted by the DoD and Intelligence Communities, Hypori is built on a zero-trust architecture and is certified at the highest levels of security. Hypori's commitment to security and privacy using virtualization technology enables easy onboarding at-scale and improves bring-your-own-device (BYOD) user adoption.

Out of Scope, Out of Mind.

Cybersecurity is a priority for the U.S. Department of Defense (DoD). It is also increasingly top of mind for the ~220,000 contractors and subcontractors that comprise the DoD's multi-tier supply chain – also known as the defense industrial base (DIB). These entities are actively being targeted with cyber-attacks from nation-states and other malicious actors whose goal is to steal intellectual property, Federal Contract Information (FCI), and Controlled Unclassified Information (CUI) shared with DIBs. Given this growing reality, the DoD developed 32 CFR Part 170, or the Cybersecurity Maturity Model Certification (CMMC) Program. It will be used to assess existing DoD cybersecurity requirements, with the goal of strengthening DIB cybersecurity and better safeguarding DoD information.

Published on 15-OCT-2024, and effective 16-DEC-2024, CMMC language is expected in contracts as of 1Q2025. The 48 CFR part 204 CMMC Acquisition rule (updated 11-OCT-2024 – Section 204.7500) will allow the DoD to require adherence to a specific CMMC certification level in a solicitation or contract.

When CMMC requirements are applied to a solicitation, contracting officers ***will not*** 1) make an award, 2) exercise an option, or 3) extend the period of performance on a contract, unless the offeror or contractor has passing results from a current certification assessment or self-assessment for the CMMC level.

An affirmation of continuous compliance with the security requirements in the **Supplier Performance Risk System** (SPRS) for all information systems that process, store, or transmit FCI or CUI during contract performance is also required. Furthermore, the appropriate CMMC certification requirements **will flow down to subcontractors** at all tiers when the subcontractor processes, stores, or transmits FCI or CUI.

Where Does Hypori Fit In?

The **Hypori CMMC Cloud** within AWS protects customers from data loss due to system compromise at the edge. It is delivered under the exact specifications of our **Hypori IL5 SaaS Platform**. This platform has successfully passed numerous DoD, Commercial, Intelligence Community, and internal security reviews of our component architecture, which continue on a regular basis.

NOTE: You can find resources in the Hypori Trust Center that validate Hypori's commitment to security and compliance.

The **Hypori App** is a Virtual Mobile Infrastructure (VMI) client, where VMI is technically equivalent to a Virtual Desktop Infrastructure (VDI). The Hypori **(VMI)** App, **which the endpoint is hosting, is designed/configured to not allow any processing, storage, or transmission of CUI or FCI beyond the keyboard, video, or mouse sent to the VMI client.**

As such, and per Table 3 §170.19(c)(1) [**Level 2**], and Table 5 §170.19(d)(1) [**Level 3**] in 32 CFR Part 170 published 15-Oct-2024 in the Federal Register, **the edge device that the Hypori App is installed on is considered out-of-scope**, and there are no documentation requirements.

Thus, the Hypori App enables you to access CUI and FCI from your edge device as part of your BYOD program, while eliminating any concerns that your edge device is classified as a **contractor risk managed asset** (CRMA).

In contrast, edge devices that run **MDM/MAM solutions** and access CUI or FCI are considered **in-scope**. They classify as **Security Protection Assets** and require the implementation of all relevant **Level 2 practices**. The edge devices are likely to be considered a **contractor risk managed asset** (CRMA) which could trigger a CMMC assessment. MDM also presents a spectrum of liability and exposure issues and invades user privacy. These details were previously explored in the Hypori blog post entitled "SMB DIBS Guide to CMMC Compliance: Essential Checklist for Cybersecurity".

For more detailed technical information, including the **Hypori CMMC Cloud Shared Responsibility Model** that provides customers with the specific controls they inherit from the Hypori CMMC Cloud to comply with CMMC requirements, contact info@hypori.com.