

M&A Voided Their CMMC Compliance. Hypori Restored It in Weeks.

Without MDM/MAM or New Devices.

A mid-size defense contractor inherited thousands of personnel following a major acquisition—and needed a compliant BYOD model before a compliance audit. They had one within weeks.

THE CHALLENGES

A Compliance Crisis Born from Growth

When a defense contractor acquires another company, the compliance clock restarts. Cybersecurity Maturity Model Certification (CMMC) assessments don't transfer to acquired entities. For one mid-size GovCon firm, a high-profile acquisition meant thousands of inherited personnel, a voided assessment scope, and an immovable deadline.

MAM on Personal Devices

The security team's first approach was deploying Mobile Application Management (MAM) across employees' personal phones. To meet CMMC Level 2 requirements, MAM deployments must exert control over components of an employee's phone, creating an adoption barrier unscalable across thousands of bring-your-own-device (BYOD) users.

Corporate Device Issuance

The fallback—issuing corporate devices with Mobile Device Management (MDM) installed—carried a price tag three times their available budget. With a hard audit deadline and no compliant model in sight, neither path was viable.

ABOUT THE CUSTOMER



INDUSTRY

Defense & GovCon



REQUIREMENT

CMMC Level 2



WORKFORCE

Thousands post-acquisition



CHALLENGE

BYOD compliance without MAM

HOW MOBILE GETS OUT OF SCOPE

The CMMC Scoping Guide explicitly excludes Virtual Desktop Infrastructure (VDI) from the assessment boundary. The DoD CIO Office has confirmed that Virtual Mobile Infrastructure (VMI) is treated equivalently—meaning mobile devices running Hypori fall outside scope by regulatory guidance, not just architectural design.

Three conditions:

1. CUI is fully **protected** within the Hypori Government Cloud and controlled by the customer's enterprise.
2. The device renders **pixels** and relays **input only**.
3. The **SSP documents** the boundary for assessors.

Hypori enforces all three by design.

THE SOLUTION

CMMC Scope Reduction Without Managing the Personal Device

Following guidance from a trusted technology partner, the defense contractor evaluated Hypori—a Virtual Mobile Infrastructure (VMI) platform that streams a fully isolated virtual workspace to any personal phone. CUI stays inside a controlled environment. No customer data ever resides on the end user device.

Hypori removes that condition at the infrastructure level—so BYOD users fall outside the boundary by architecture, not policy. Under CMMC, a device enters assessment scope only when it stores, processes, or transmits controlled information. Hypori removes that condition at the infrastructure level—so BYOD users fall outside the boundary by architecture, not policy. The defense contractor documented the posture in its System Security Plan (SSP) and entered the audit cycle with a defensible scope reduction position.



CMMC SCOPE REDUCTION

CUI never resides on the personal device. BYOD users fall outside the CMMC audit boundary by architecture—not policy workaround.



ZERO MDM/MAM. FULL PRIVACY.

No MDM/MAM profile required on the host phone. Employees keep full privacy, eliminating the #1 adoption barrier in GovCon BYOD programs.



PLUG-IN DEPLOYMENT

Existing MDM/MAM integrates with the Virtual Workspace for access and control to enterprise resources.

HYPORI IN ACTION

From First Search to Deployed Solution

Following guidance from a trusted technology partner, the defense contractor evaluated Hypori—a Virtual Mobile Infrastructure (VMI) platform that streams a fully isolated virtual workspace to any personal phone. CUI stays inside a controlled environment. No customer data ever resides on the end user device.

01

INBOUND EVALUATION

After independently researching options, the Chief Information Security Officer (CISO) discovered Hypori's BYOD compliance content—specifically the architectural framing around keeping CUI off the mobile endpoint—and reached out directly.

02

TECHNICAL VALIDATION

The defense contractor's team met with Hypori's technical subject matter experts to validate the architecture and confirm the scope reduction posture.

03

DEPLOYMENT & COMPLIANCE

The team was live within days of contract execution—no rip-and-replace, no new hardware. With Hypori active across the BYOD population, the defense contractor's SSP reflected a documented architectural boundary, giving assessors a clear, defensible rationale for excluding personal devices from scope.

THE RESULTS

Compliance Restored. Hardware Budget Preserved. End User Personal Privacy Protected.

The defense contractor entered its CMMC audit cycle with a defensible BYOD posture—ahead of its deadline—without issuing a single corporate device or deploying MDM/MAM on any personal phone. Employees retained full privacy on their own devices, eliminating the adoption friction that had blocked every prior approach.

With Hypori active across the BYOD population, the defense contractor's SSP reflected a documented architectural boundary—giving assessors a clear, defensible rationale for excluding personal devices from scope.

ABOUT HYPORI

FedRAMP High Authorized · SOC 2 Certified · CMMC Level 2

Hypori VMI streams a fully isolated virtual workspace to any mobile device—no MDM/MAM, no data on the endpoint, no corporate hardware required. The mobile device acts only as a display and input surface; applications, data, and identity stay inside a controlled environment.

BUILT TO PULL MOBILE DEVICES OUT OF CMMC SCOPE.