Hypori®

One Device, Zero Worries™

Secure BYOD

Protect data and privacy with Hypori's Mobile Access Platform

One Device, Zero Worries

Today, we live in a world where the boundaries between personal and professional life are increasingly blurred. As "work from anywhere" has become the new norm, the mobile edge has emerged as the largest attack surface organizations must defend. People are concerned about the privacy of their personal information and the risks their personal device might get wiped. Employers worry that bring your own device -- (BYOD) can lead to data breaches and leaks.

This ebook answers how Hypori's mobile access platform addresses today's most critical BYOD issues facing government and private sector enterprises by securing enterprise data and protecting personal privacy, all on one device with zero worries.

- How do we enable secure access to enterprise apps and data from any mobile device with total personal privacy?
- How do we ensure the security of sensitive information?
- How do we protect total personal privacy and increase BYOD user adoption?
- How do we meet federal classified and sensitive information standards for mobile devices?
- How do we provide easy BYOD onboarding and deployment at scale?

Contents

Introduction

Use cases

Secure access to enterprise apps and data from any mobile device with total personal privacy.

Hypori's mobile access platform combines an app that provides a virtualized and isolated environment on any mobile device with zero-trust architecture. Working together, this framework enables secure access to enterprise apps and data with total personal privacy.

Users download the Hypori client from the Google Play or the Apple App Store and scan a QR code with one-time password from their administrator to gain secure access to a virtual corporate workspace on any mobile device, keeping work completely separate from everything else on the phone.

Security is assured because the Hypori app never processes, stores, or transmits data to the mobile device. Instead, it is a virtual window into a cloud-based workspace protected by zero-trust architecture. Since the workspace is streamed using only encrypted pixels, there is nothing stored on the mobile device to attack, steal, lose, or wipe.

Hypori provides a high level of protection against threats to mobile attack surfaces, enabling the Hypori platform to meet the most rigorous security standards required for defense, government, healthcare, and other regulated organizations.

By isolating personal and work on the mobile device, Hypori simplifies the challenges faced by global organizations to empower their workforce to access data securely and privately from their personal devices. This unique approach eliminates the need for traditional application and mobile device management (MDM) solutions that invade privacy and discourage user participation.

Protect total personal privacy and increase BYOD user adoption.

Hypori ensures total privacy by isolating the corporate virtual workspace from personal data on the physical device. Since only encrypted pixels are streamed, no data is stored, downloaded, or transmitted on the device, eliminating security concerns for loss, theft, leaks, confiscation, or device wiping. Unlike traditional mobile device management (MDM) solutions, Hypori's cloud-based approach minimizes data usage, has no impact on device performance, and enhances security without requiring intrusive software.

Users benefit from zero-trust access to enterprise data without carrying multiple devices or dealing with forced upgrades. Any mobile device still being supported by its manufacturer, regardless of age or model, can run the latest version of Hypori. This worry-free experience increases BYOD adoption by ensuring total personal privacy, zero risk of data spillage, and optimal performance.

Ensure the security of sensitive information.

Hypori ensures enterprise security by streaming pixels, not data, creating a virtual workspace that keeps corporate/government and personal information completely separate.

100% data separation – No enterprise data is stored, processed, or transmitted on the mobile device, eliminating the risk of leaks, confiscation, or subpoenas.

Zero-trust architecture – Hypori establishes an encrypted TLS tunnel to provide a window to view the virtual workspace in a secure enclave. The TLS tunnel is encrypted in accordance with NIST Federal Information Processing Standards (FIPS).

1-Click offboarding – If a device is lost or an employee leaves, admins can simply revoke access without requiring a remote wipe.

Hypori's approach reduces the attack surface and minimizes cybersecurity risks, ensuring secure, worry-free BYOD access without compromising privacy.

Meet federal classified and sensitive information standards for mobile devices.

Trusted by global systems integrators, defense, government, healthcare, and other regulated industries, Hypori's virtualized mobile app and zero-trust architecture meet the highest security and compliance standards for protecting sensitive information while enabling the use of BYOD mobile devices. Hypori meets the following robust security criteria:

- No TikTok on Government Devices Act
- NSA's Commercial Solutions for Classified (CSfC)
- FedRAMP High (in process)
- CMMC
- NIST 800-171
- HIPAA
- DOD Impact Level 5 (IL5)
- NIAP Common Criteria
- SOC 2 Type II

Trusted by U.S. ARMY AIR FORCE

Easy onboarding and deployment at scale for BYOD.

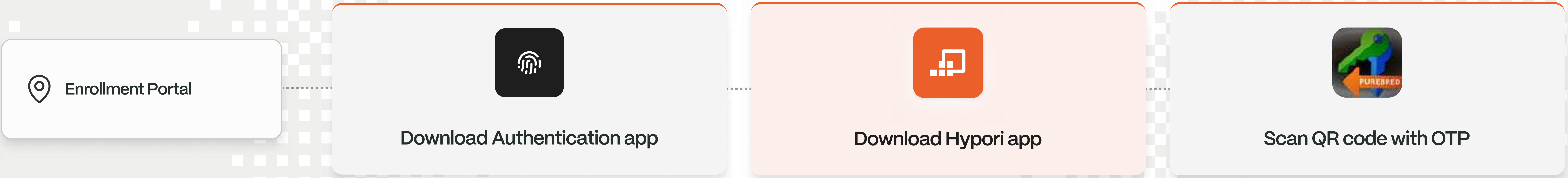
With Hypori, organizations can scale secure mobile access instantly – deploy today, onboard in minutes.

Hypori makes onboarding thousands of users simple and fast – no device shipping, no complex setup. Unlike traditional MDM, Hypori enables organizations to quickly deploy, deprovision, and manage mobile access without touching personal devices.

Up and running in minutes – New users can gain full access in under 10 minutes.

Bulk user management – Admins can import users via LDAP or CSV, assign privileges, and manage authentication with QR codes or one-time passwords (OTPs).

Flexible deployment – Works in commercial or government clouds, or on-premise, to fit organizational needs.



Enrollment Portal

Download Authentication app

Download Hypori app

Scan QR code with OTP

Putting Hypori to work

Hypori tackles today's most pressing BYOD challenges with its secure and privacy-focused mobile access platform.

Now that we have identified the problems Hypori can solve, in the next section, we'll explore how these capabilities are applied in real-world scenarios.

Zero-trust data security

Streams encrypted pixels without storing or processing data on devices, ensuring sensitive information stays protected.

Total personal privacy

Separates work and personal environments on the same device, eliminating privacy concerns tied to traditional MDM solutions.

Simplified onboarding

Enables quick setup, with users gaining secure access to corporate workspaces in under 10 minutes.

Compliance with high standards

Meets rigorous security and compliance benchmarks, including FedRAMP High (in process), CMMC, and NSA CSfC certification.

Enhanced BYOD adoption

Offers worry-free usage with no impact on device performance, low data consumption, and support for devices of any age or model.

Scalable management

Features centralized administration for streamlined deployment, bulk user onboarding, and easy deprovisioning.

Trusted by U.S. ARMY AIR FORCE

Use Case: Work from anywhere with total privacy

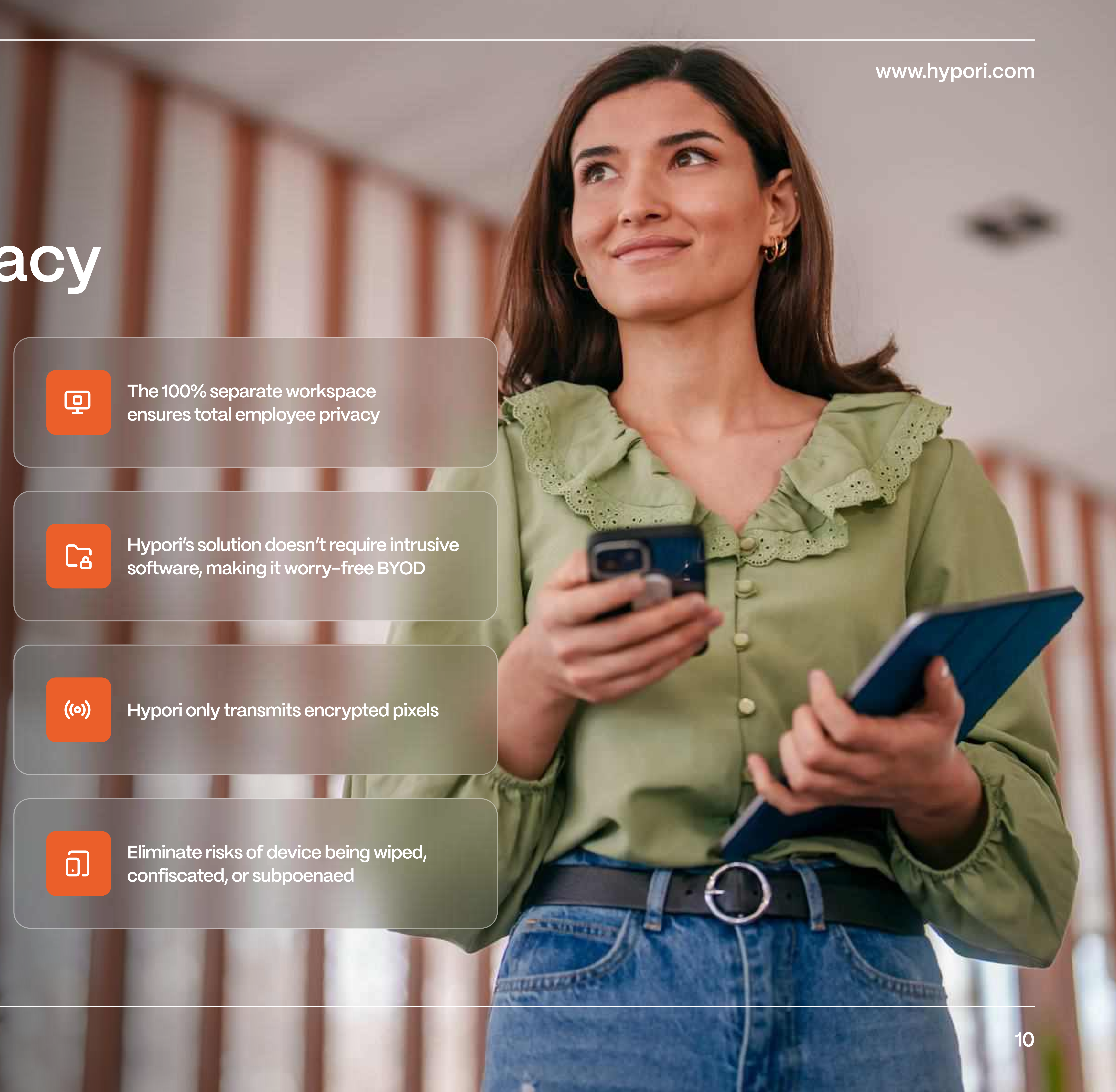
Empower teams with secure and private access from anywhere, on one device

Problem

Workers need secure, flexible access to enterprise systems from personal devices, especially in regulated industries like defense, healthcare, and finance. IT teams struggle to balance secure remote access with employee privacy and data protection.

Solution

Hypori enables employees to work securely on personal devices with full privacy and compliance. Only encrypted pixels are transmitted, no data is stored locally, ensuring 100% separation between the personal device and the virtual workspace.



- The 100% separate workspace ensures total employee privacy
- Hypori's solution doesn't require intrusive software, making it worry-free BYOD
- Hypori only transmits encrypted pixels
- Eliminate risks of device being wiped, confiscated, or subpoenaed

Use Case:
Swiftly mobilize contractors

Mobilize your workforce with speed and security

Problem

Organizations need to rapidly onboard and offboard contractors during emergencies or high-growth periods, but traditional device distribution is slow, costly, and puts data at risk.

Solution

Hypori enables fast, secure onboarding and offboarding without device management headaches. New employees can be provisioned in under 10 minutes or deprovisioned with one click.

- Swiftly onboard and offboard contractors
- Improve BYOD adoption with a user-friendly experience that prioritizes privacy and reduces complexity
- Easy deployment at scale

Use Case: HIPAA-compliant access from personal devices

Protect patient data with secure virtual access

Problem

Delivering quality healthcare requires secure access to sensitive patient data at home, on the road, at a conference, or in the office.

Solution

Hypori's mobile virtual workspace enables HIPAA-compliant access from personal devices, eliminating the risks of data leakage and streamlining workflows for healthcare professionals.

- Ensure HIPAA-compliance from any device
- Eliminate risks of data leakage
- Empower healthcare professionals with secure access to patient data, improving productivity and care delivery

Use Case: Travel globally with secure mobile access

Protect sensitive data wherever you go

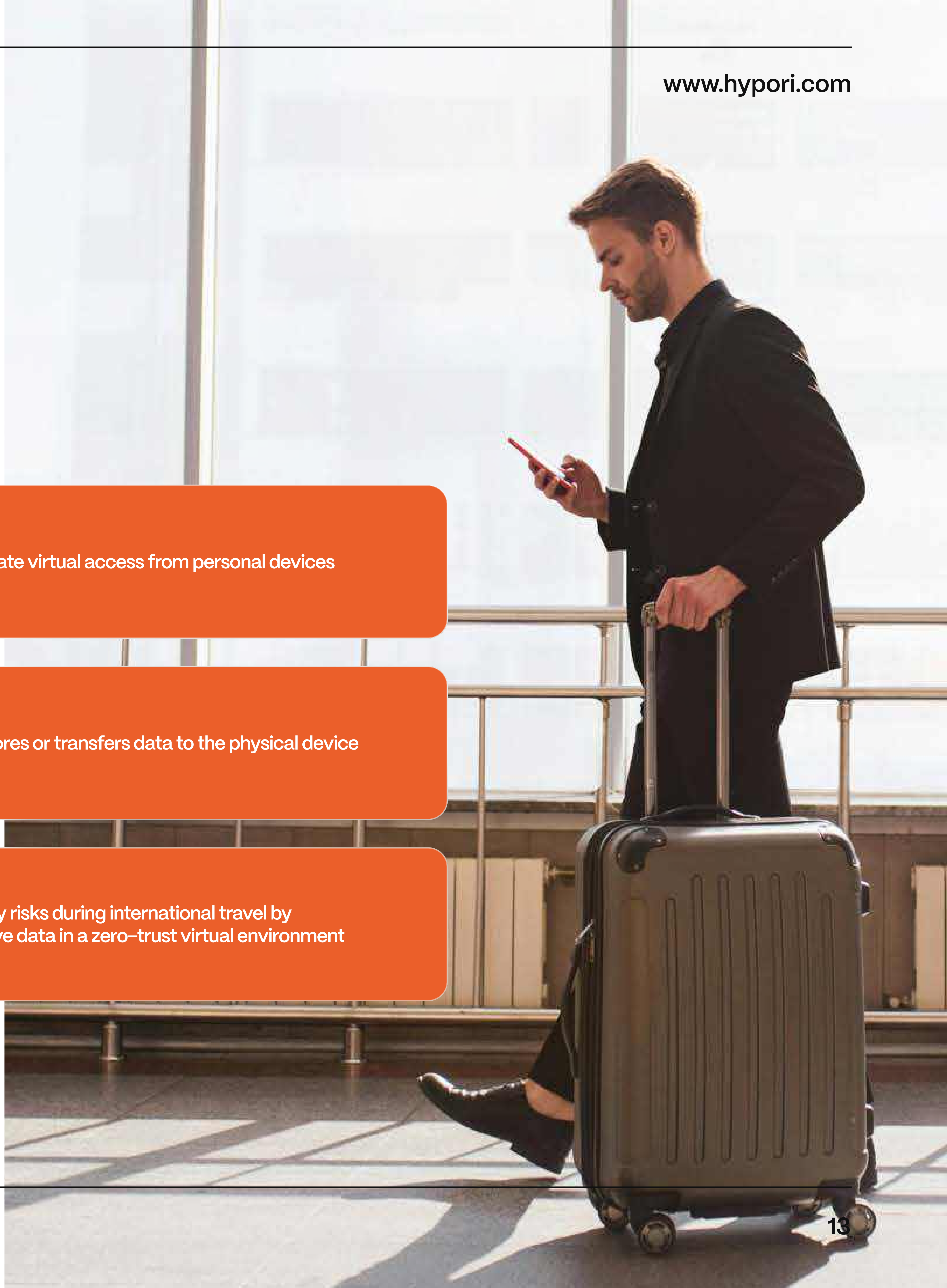
Problem

While global travel is essential for many industries, it exposes mobile devices to unique and serious security threats including interception, theft, and ransomware installation at checkpoints.

Solution

Hypori's virtual workspace ensures sensitive data stays protected, inaccessible to malware and data duplication tools targeting the physical device. By never storing data on the physical device and isolating the virtual workspace in the cloud, Hypori keeps mobile devices secure, even in high-risk environments.

- Secure and private virtual access from personal devices
- Hypori never stores or transfers data to the physical device
- Mitigate security risks during international travel by isolating sensitive data in a zero-trust virtual environment



Trusted by U.S. ARMY AIR FORCE

Use Case: Enable CMMC compliance for mobile

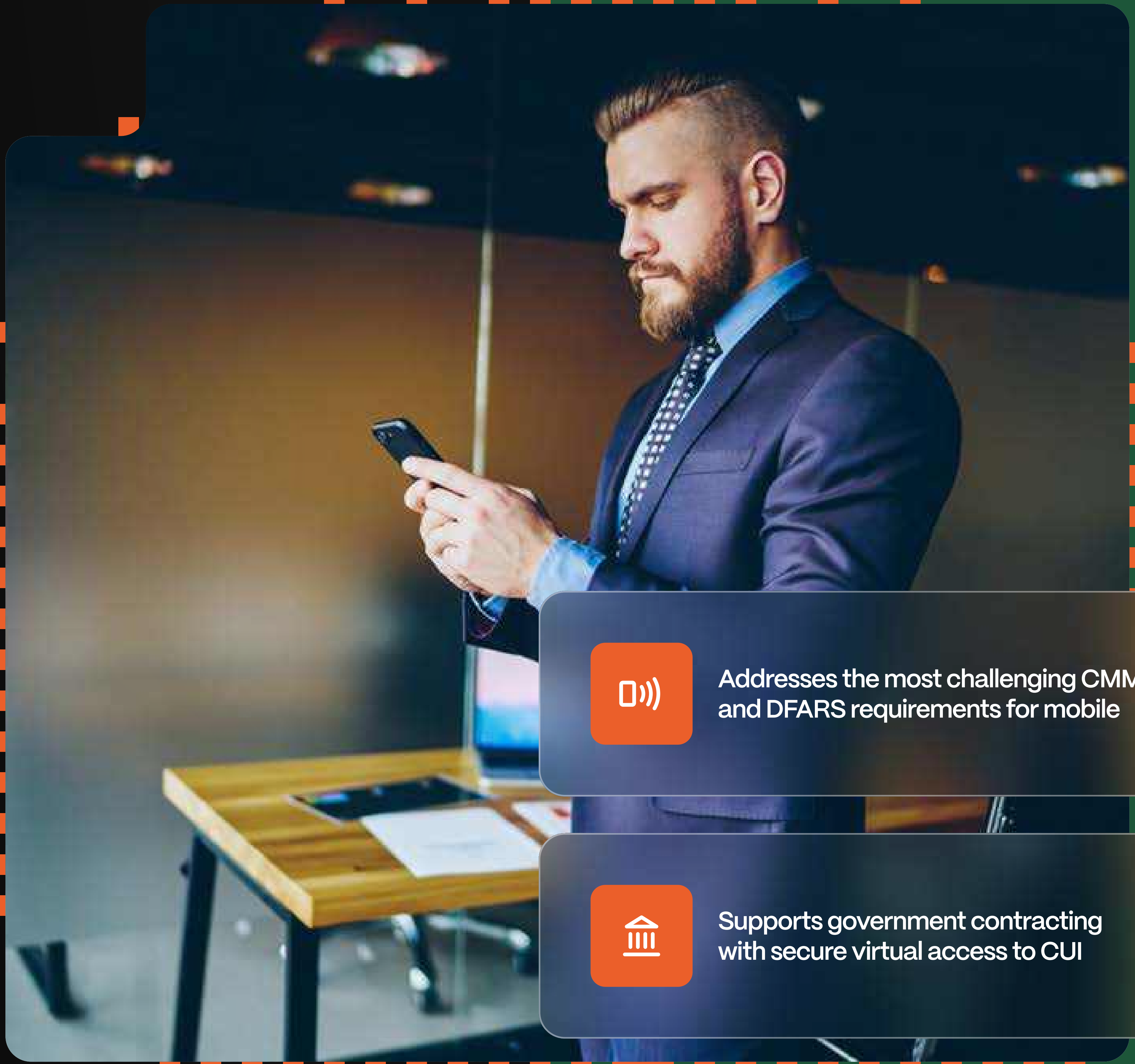
Tackle the most challenging Cybersecurity Maturity Model Certification requirements for mobile. With ~220,000 contractors and subcontractors in the DOD's multi-tier supply chain, compliance isn't just a necessity, it's a competitive advantage.

Problem

CMMC requires stringent measures to safeguard sensitive data, particularly for organizations that process, store, or transmit controlled unclassified information (CUI) or federal contract information (FCI). Yet achieving compliance on mobile devices introduces unique challenges, from managing secure environments to ensuring malware cannot compromise critical data.

Solution

Hypori addresses this with a zero-trust virtual workspace that ensures compliance by never transmitting, processing, or storing data on the physical mobile device, adhering to DFARS for protecting CUI and FCI based on NIST 800-171.



- Addresses the most challenging CMMC and DFARS requirements for mobile
- Supports government contracting with secure virtual access to CUI
- Protect data while preserving total user privacy of DOD personnel on own devices

Trusted by U.S. ARMY AIR FORCE

Use Case: BYOD for Department of Defense

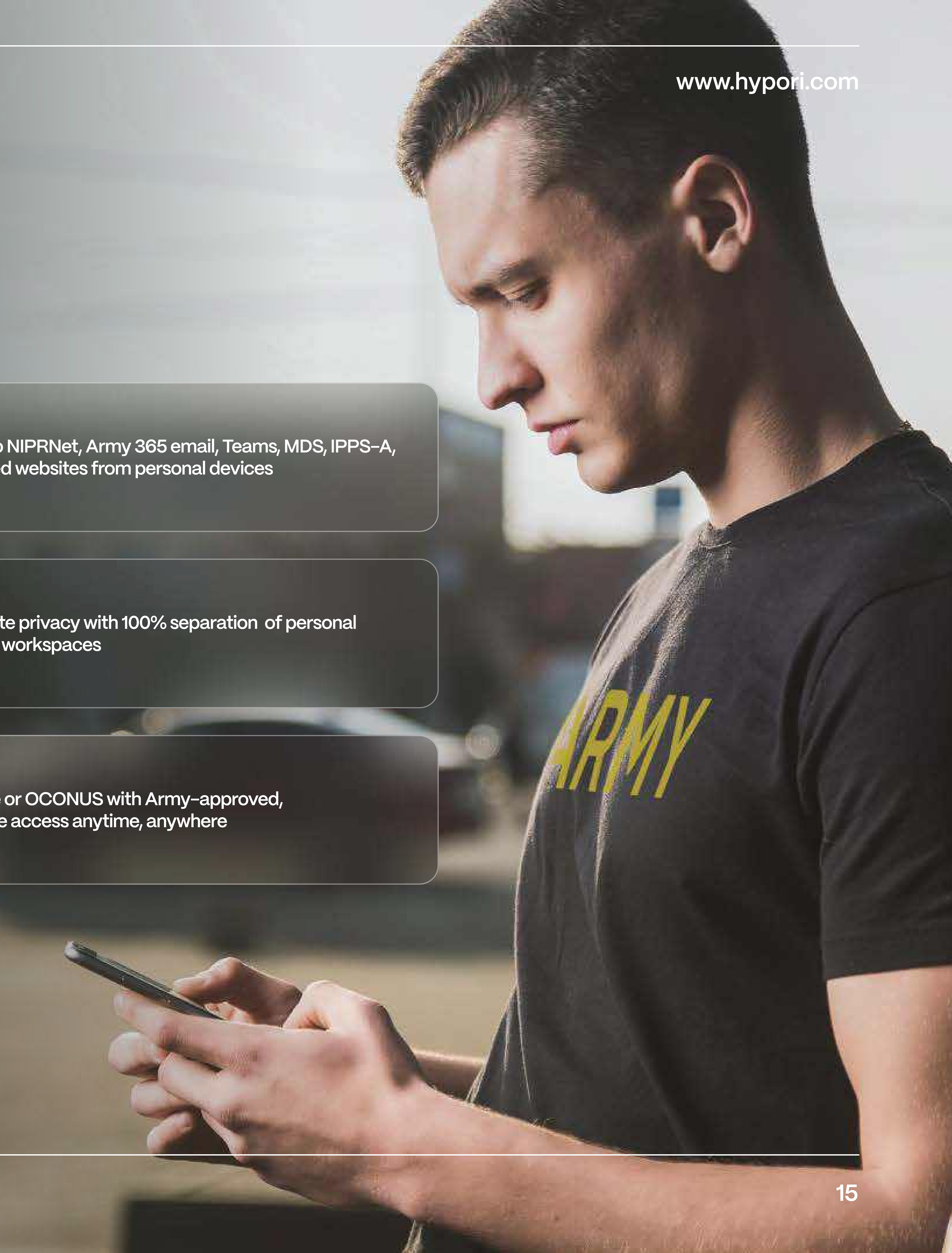
Empower war fighters, civilians, and contractors with secure virtual access to critical apps and data from personal devices

Problem

DOD personnel need secure access to government data and applications from personal devices, anytime, anywhere, without risking security breaches or their personal privacy.

Solution

No data is stored on the personal device, eliminating the edge as an attack surface. Hypori provides total separation between personal and government workspaces.



- Secure access to NIPRNet, Army 365 email, Teams, MDS, IPPS-A, and CAC-enabled websites from personal devices
- Maintain complete privacy with 100% separation of personal and professional workspaces
- Work from home or OCONUS with Army-approved, CAC-reader-free access anytime, anywhere

Use Case: BYOD for federal employees

Secure access for federal teams with total personal privacy

Problem

The federal workforce operates in dynamic environments, requiring secure and convenient access to critical applications and data from personal devices.

Whether managing sensitive projects, collaborating across agencies, or accessing GCC-High environments, federal employees need a solution that enables productivity without sacrificing security, privacy, or compliance.

Solution

Hypori provides a virtual workspace that keeps government data secure, personal privacy intact, and administration easy.

Government organizations, federal agencies, and the intelligence community count on Hypori to arm their hybrid workforce and contractors with secure access to government networks and data from personal devices while meeting FedRAMP High and CMMC compliance standards and cybersecurity imperatives from the Office of Management and Budget (OMB).

Use Case: Comply with No TikTok on Government Devices Act

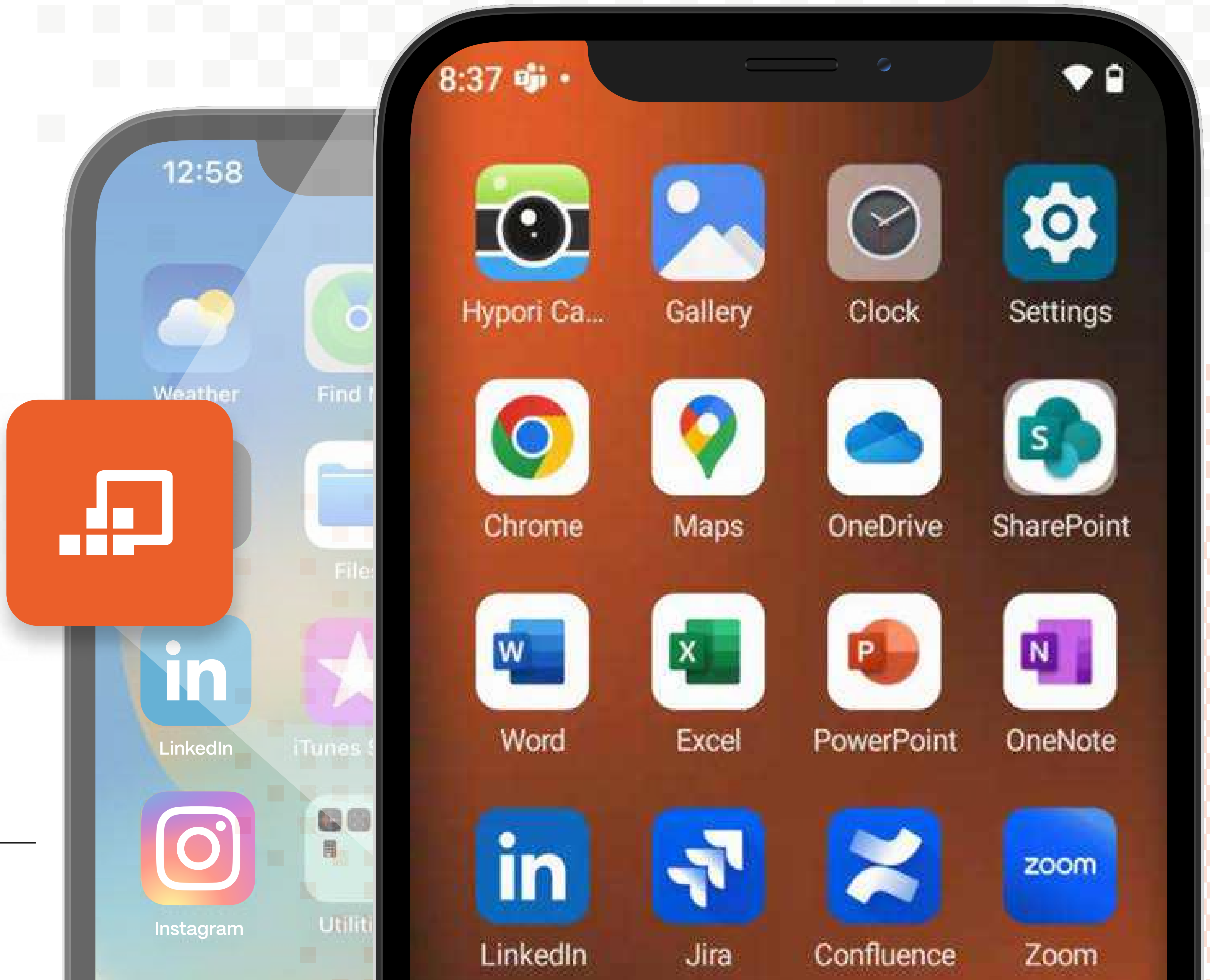
Secure, compliant BYOD for government

Problem

The White House and Department of Defense have banned TikTok from any device that interacts with U.S. government data, including those owned by contractors.

Solution

As a 100% separate, zero-trust, virtual Android OS workspace, Hypori transmits no government data to the physical device, stores no data on the physical device, and keeps government data isolated and protected in the virtual device environment. It is impossible for data, malware, or aggressive data-harvesting apps on the physical device to access the Hypori environment and vice versa. Agencies and contractors using Hypori are in full compliance of the No TikTok act.



One Device, Zero Worries

Now that you've explored how Hypori transforms the way organizations approach secure mobility—ensuring security, privacy, and compliance—it's time to take the next step. Hypori empowers organizations to embrace BYOD while eliminating security risks, protecting sensitive data, and ensuring users maintain complete privacy.

What's Next?

Ready to put Hypori to work for your organization? Here's how you can get started:

Schedule a Demo

See Hypori in action.
www.hypori.com/request-a-demo

Talk to Our Experts

Discuss how Hypori can support your secure mobility goals.
www.hypori.com/contact

Stay Connected

Follow us for the latest insights on secure mobility.
www.linkedin.com/company/hypori/

Trusted by U.S. ARMY AIR FORCE