Hypori®

One Device, Zero Worries™

Secure BYOD

Protect data and privacy with
Hypori's Mobile Access Platform

Easy onboarding and deployment at scale for BYOD.

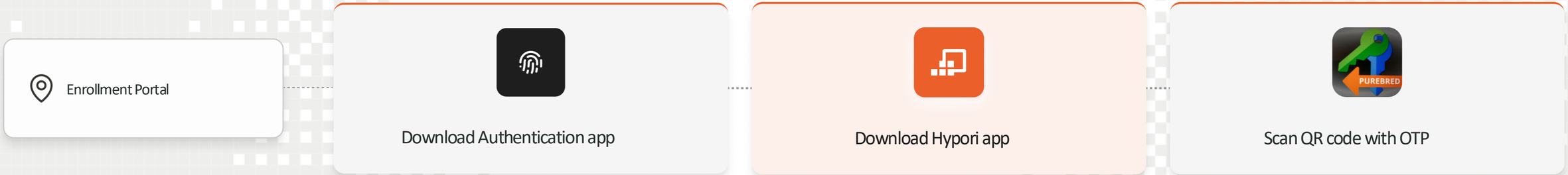
With Hypori, organizations can scale secure mobile access instantly - deploy today, onboard in minutes.

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 can gain full access in under 10 minutes.

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

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



Trusted by U.S. ARMY AIR FORCE

Hypori

www.hypori.com

Use Case: Work from anywhere anywhere with total privacy

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

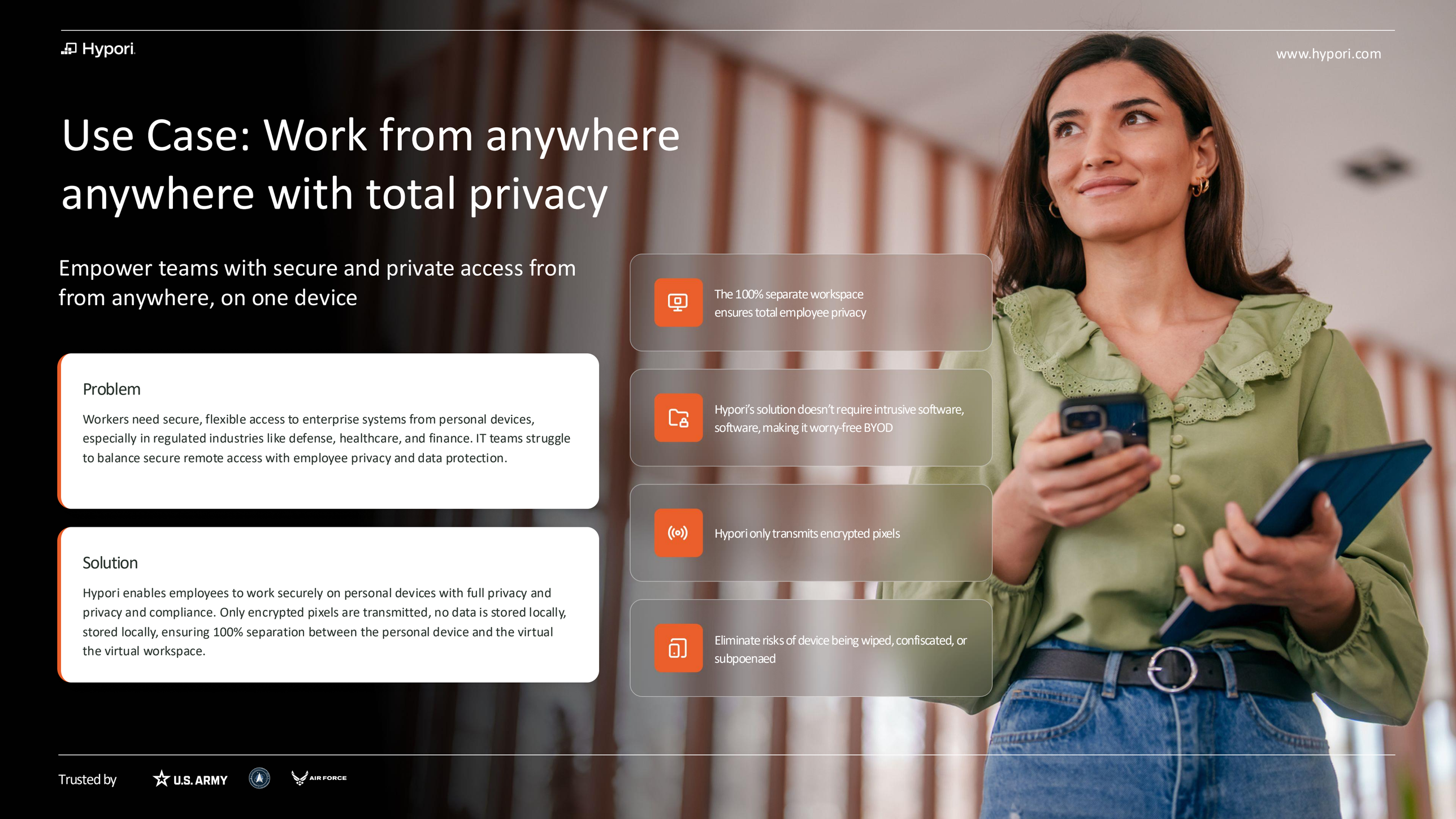
Problem

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 privacy and compliance. Only encrypted pixels are transmitted, no data is stored locally, stored locally, ensuring 100% separation between the personal device and the virtual the virtual workspace.

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



Trusted by U.S. ARMY AIR FORCE

Use Case: BYOD for Department of Defense

Empower war fighters, civilians, and contractors with with secure virtual access to critical apps and data 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 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 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 intact, and administration easy.

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

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 management headaches. New employees can be provisioned in under 10 minutes or minutes or deprovisioned with one click.

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

Use Case: Enable CMMC compliance for mobile

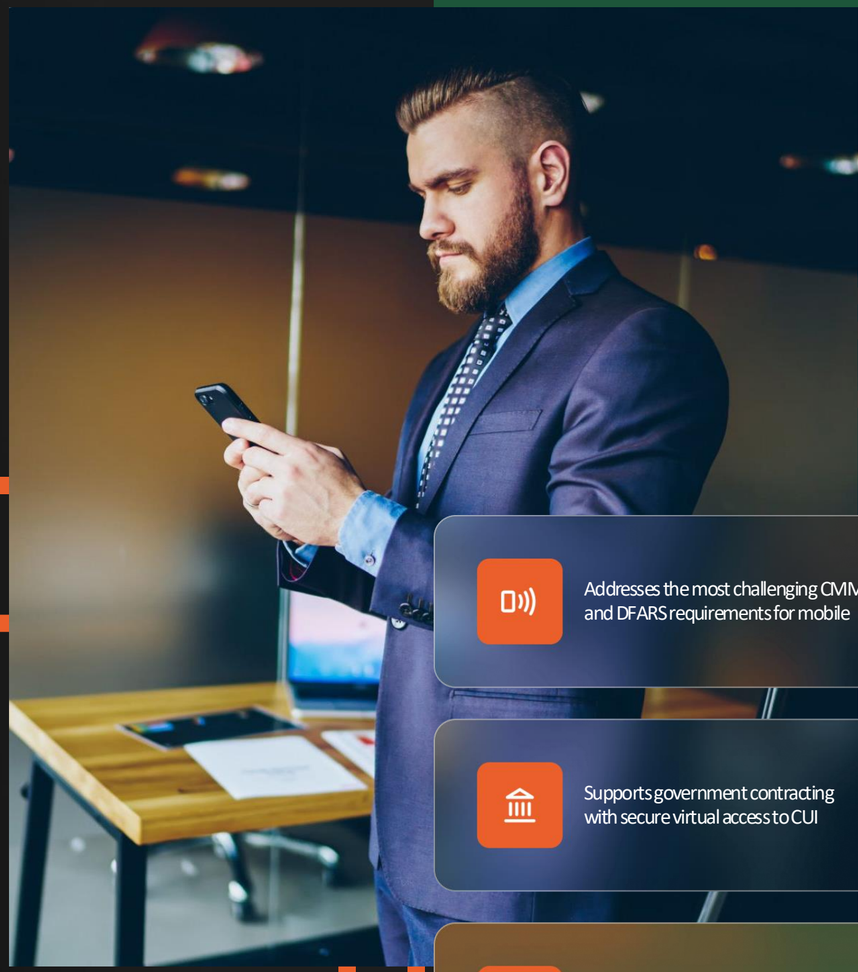
Tackle the most challenging Cybersecurity Maturity Model Certification Certification requirements for mobile. With ~220,000 contractors and subcontractors in the DOD's multi-tier supply chain, compliance isn't just a isn't just a necessity, it's a competitive advantage.

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, transmitting, processing, or storing data on the physical mobile device, adhering to DFARS for protecting 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

Use Case: HIPAA-compliant access from personal devices

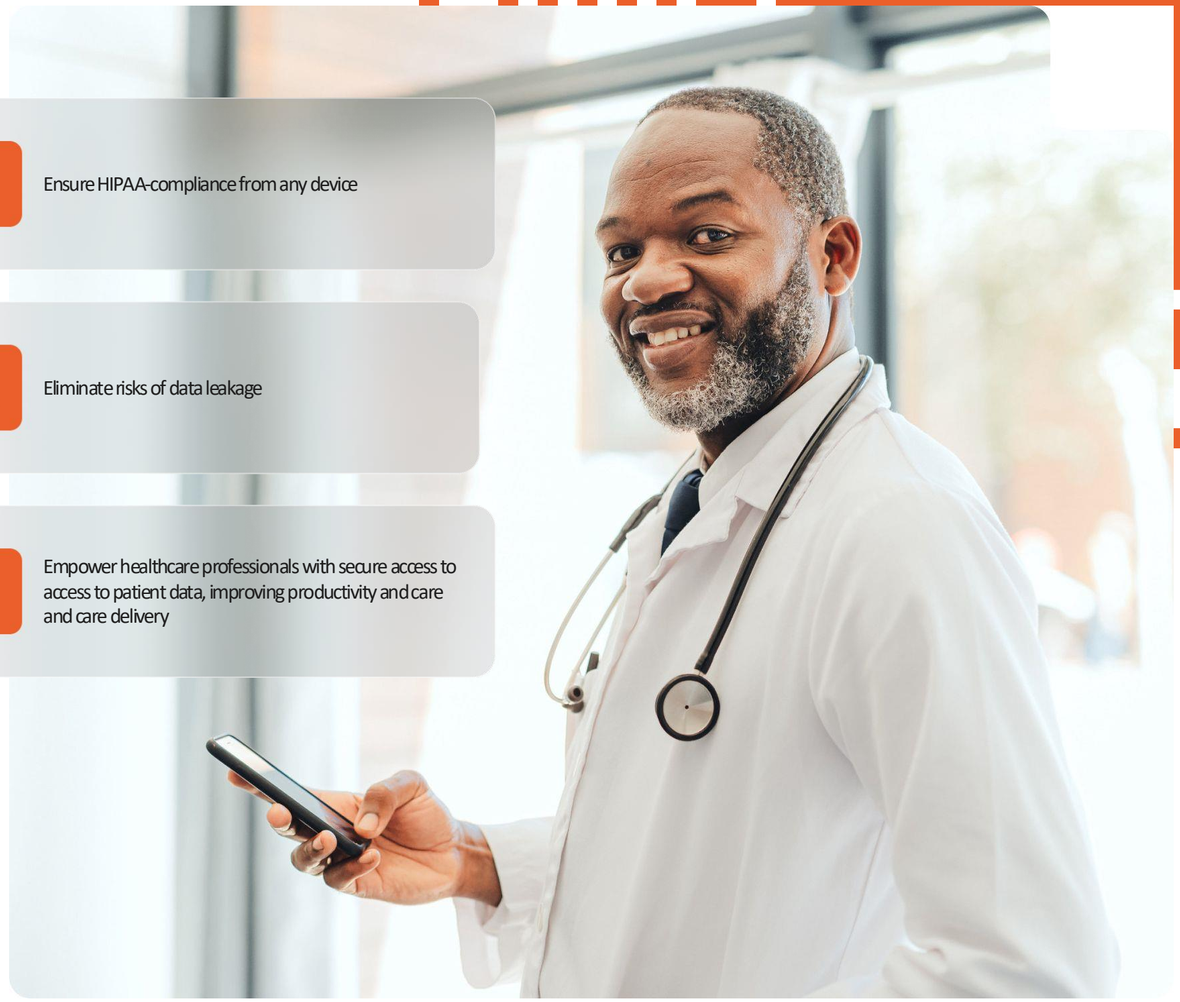
Protect patient data with secure virtual access

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, personal devices, eliminating the risks of data leakage and streamlining workflows for workflows for healthcare professionals.



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

Use Case: Travel globally with secure mobile access

Protect sensitive data wherever you go

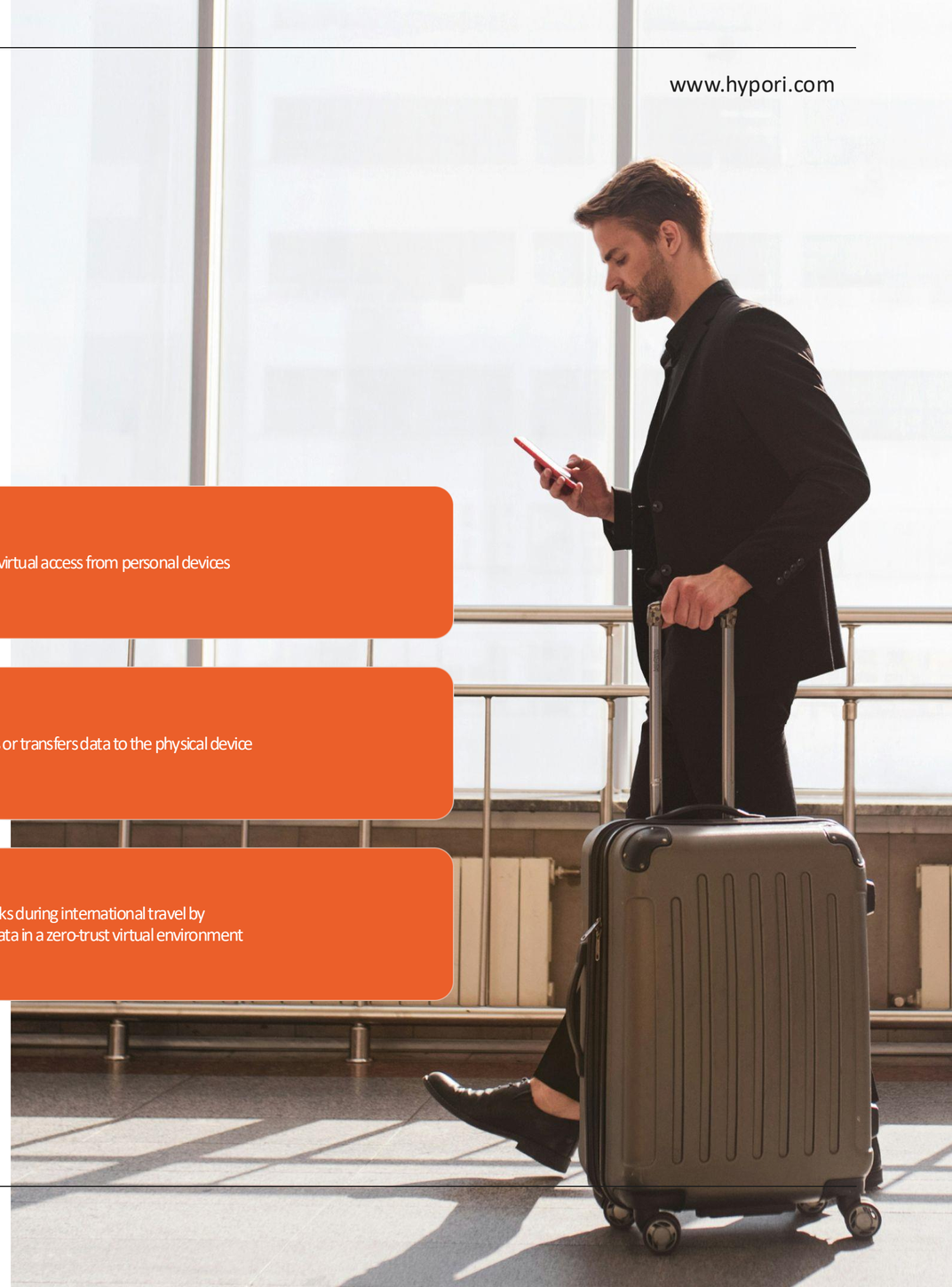
Problem

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 to malware and data duplication tools targeting the physical device. By never storing data on storing data on the physical device and isolating the virtual workspace in the cloud, Hypori 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



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 government data to the physical device, stores no data on the physical device, and keeps keeps government data isolated and protected in the virtual device environment. It is is impossible for data, malware, or aggressive data-harvesting apps on the physical device to device to access the Hypori environment and vice versa. Agencies and contractors using Hypori using Hypori are in full compliance of the No TikTok act.