

Access Mission Apps. Any Device. No Data at Risk.



Zero trust access to C2 apps, AI tools, messaging, and full desktop environments – without storing data on the device.

Special Operations Forces (SOF) units need secure access to sensitive data and applications from any device, anywhere:

-  C2 applications (ATAK, mission systems)
-  AI tools (GenAI.mil, Maven)
-  Sensitive mission data (classified/unclassified)

Current solutions require managed endpoints that can't keep pace with deployment timelines or mission partner environments (MPE).

-  Access depends on managed devices
-  Devices can't scale to deployment timelines
-  Partner environments break access models
-  Data is exposed at the endpoint

The provisioning tail is killing mission readiness.

Why Hypori for SOF

Hypori delivers zero trust access to mission applications from any device:

-  Secure access to apps, messaging, and full desktop environments
-  No data stored on the endpoint
-  Delivered from a controlled environment – not the device
-  Works across personal, government, and partner devices

Access mission systems and apps
today—without device risk or delay

[Request a demo](#)

hypori.com/request-a-demo

Mission Use Cases



C2 App Access (ATAK)
Command & control from any device



AI at the Edge (GenAI.mil / Maven)
Secure AI usage without data exposure



Secure Messaging
Communicate securely at the right classification level without consumer apps (i.e. WhatsApp, Signal)



Full Desktop Access
Access complete virtual workstations from any device



Coalition Environments
Enable access without provisioning partner devices

Cyber / J6

The Problem

- Devices can't be trusted
- Apps expose data at the endpoint

Hypori

- Apps run in controlled environment
- No data on device
- Full visibility
- Removes endpoint as an attack surface

Compliance / Risk

The Problem

- No audit trail
- No control over data exposure

Hypori

- Logs all activity
- Centralized enforcement
- Defensible, auditable access

Operators / S&T

The Problem

- Need access now, not after provisioning
- Tools exist – but aren't accessible

Hypori

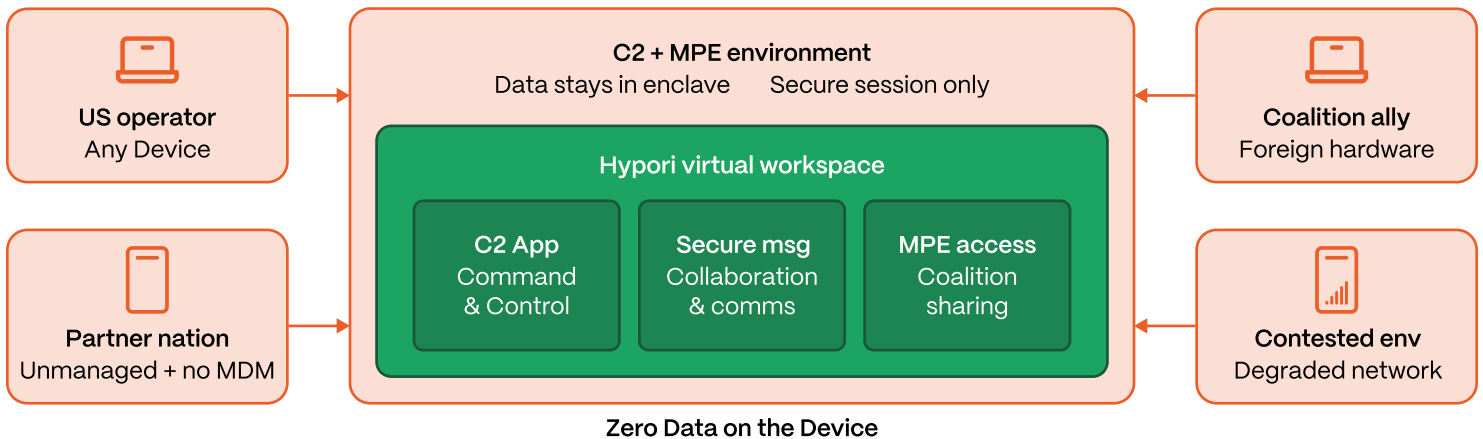
- Immediate access to ATAK, GenAI.mil, and Maven
- Secure messaging at the correct classification level
- Full desktop access from any device
- No provisioning delay
- Faster mission execution

Why Traditional Approaches Fail

- Require managed devices
- Don't scale to coalition environments
- Create provisioning delays

The provisioning tail kills mission readiness.

Stop provisioning devices.
Start delivering access.



50,000+

U.S. Army BYOD Users

CSfC

Authorized to meet operational requirements for classified

IL5 SaaS

Authorized for DoD Impact Level 5 workloads

12,000+

Department of Air Force Secure Messaging Licenses