# HYPORI HALO™

SECURE BYOD YOU CAN TRUST.

## 100% USER PRIVACY & NO DATA AT REST

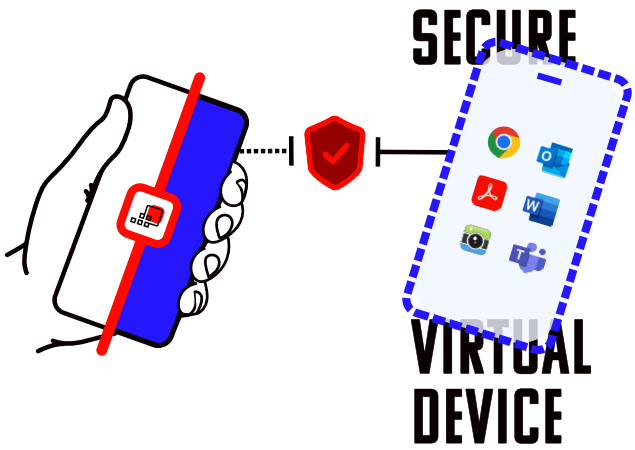
Zero-trust access to enterprise apps and data via a separate, secure virtual device from any smartphone or tablet. Protect corporate data, preserve employee privacy, and provide on-the-go access from their own mobile device.

## BENEFITS OF HYPORI HALO

- 100% user privacy
- Remove risk of lost or stolen data with no data on the device
- Frees customers from liability for end-user behavior
- Defense against malware and data-harvesting apps
- No need for a second physical device – only carry one phone

## KEY FEATURES

- Employer can't view or access user's personal data on the physical device
- No enterprise data stored on user's physical device
- NIAP Common Criteria certified since 2016
- Works on iOS, Android, and Windows 10 devices
- No hardware cost - affordable SaaS model




## PROTECTING DATA & PRESERVING PRIVACY FOR DEFENSE AND REGULATED INDUSTRIES

Hypori Halo addresses the complex challenges of accessing secure datasets, protecting government data from TikTok, meeting CMMC 2.0 "data at rest" requirements, and restricting personal health information (PHI) leakage from personal mobile devices.

### DEPARTMENT OF DEFENSE

Secure access to government environments – IL4/5, NIPRNet

### DEFENSE INDUSTRIAL BASE

Access corporate & GCC high email from a single device

### HEALTHCARE ORGANIZATIONS

Ensure HIPAA-Compliance from any device

HYPORI HALO

See How It Works

**Customers requiring classified access can use Hypori Halo on GFE.**

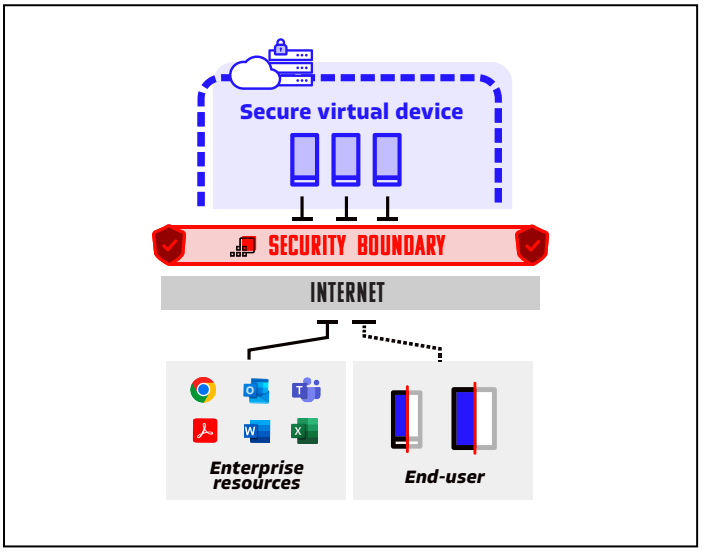
Hypori is an NSA Commercial Solution for Classified (CSfC) compliant vendor, enabling secure access to classified networks (I.e., SIPRNet) from managed government-furnished equipment (GFE).

# HYPORI USES VIRTUALIZATION TO SOLVE THE PROBLEM

Hypori Halo uses zero-trust architecture, isolation, and virtualization to eliminate data at rest on the device and data in transit, reducing the threat and spread of cyber-attacks. The unique separation of the secure virtual device in the cloud or on-prem eliminates the risk of data spillage, and no data on the device means **no need to seize the user's device**.

**Each user's virtual device is isolated in the cloud or on-prem.**

**Customize and control your catalog of enterprise apps per user profile.**




**Have 1 or many profiles per user – access them all from a single device.**

**User accounts work across their tablets and smartphone.**

## ONLY ENCRYPTED PIXELS ARE TRANSMITTED TO AND FROM THE PHYSICAL DEVICE.

Zero-trust PKI credential-based multi-factor authentication. TPM and NIST FIPS 140-2 protected with security-enhanced Linux in Android.

Manage single, centralized, mobile OS virtual environment. Develop and test apps without wrapping or modification.

Securely access IL4/5 services and capabilities from personal mobile devices with Hypori IL5 SaaS.