

Hypori Halo Data Isolation for Complete Separation

No data access between the physical and virtual devices for OMB M-23-13 compliance.

This document outlines how Hypori Halo complies with White House issued M-23-13 (the memorandum), dated 27 February 2023, “No TikTok on Government Devices.” This memorandum gives government agencies, including the Department of Defense, Intelligence Community, and National Security Sector, 30 days to ensure they do not have TikTok on government-owned or contractor devices that come in contact with United States Government data.

Agencies & contractors using Hypori Halo devices are already in full compliance with M-23-13.

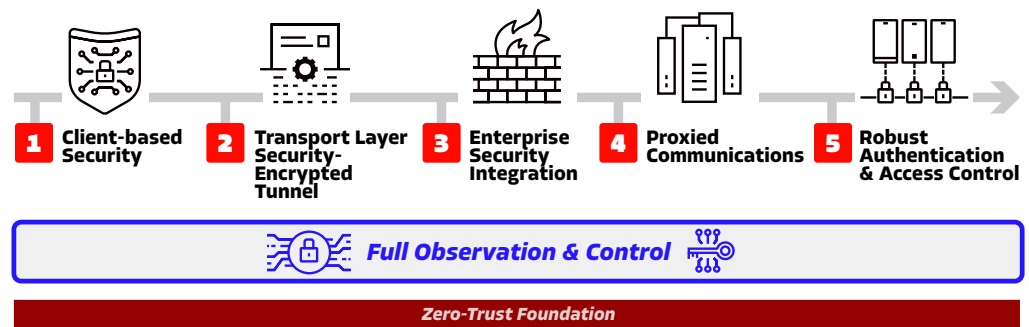



Figure 1: Hypori Halo Zero-Trust Architecture

 As a 100% separate, zero-trust, virtual Android OS workspace, accessible from any edge device, Hypori Halo transmits no data to the physical device, leaves no data at rest on your 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 Halo environment and vice versa. Threat Systems Management Office (TSMO) described Hypori Halo as a “Virtual GFE” device, implying that the virtual instance operating within the protected network is a physically and logically separate GFE device. This virtual GFE device cannot be impacted by the edge device, or applications

operating on that edge platform. Agencies using Hypori Halo have total control of the Hypori Halo workspace across the application stack (Layer 1-7) with complete enterprise control of what apps are available on the virtual platform. Hypori Halo’s separate and isolated environment protects the government data and network and meets the OMB prescribed guidelines as detailed below. Implementation of Hypori Halo does not infringe on their employees’ privacy or control of personal owned devices by restricting their downloads to their BYOD devices. It is unnecessary to monitor users’ physical devices because their personal apps can’t access or infiltrate the Hypori Halo virtual device.

Addressing OMB M-23-13 Actions

Section III, “Actions,” of the memorandum provides instructions and deadlines for the removal of TikTok on the aforementioned devices. See how Hypori Halo addresses each action.

III. Actions

A. No later than 30 days following the issuance of this memorandum, agencies shall–

i. Identify the use or presence of a covered application on information technology;

- ✓ **Fully Compliant.** By design, Hypori Halo is an isolated, secure operating system that resides within the protected environment only (IL5 / NIPR). Access to applications within Hypori Halo is prescribed through security templates. Users cannot independently add applications to Hypori Halo. Complete inventory of all applications allowed and operating within is available at all times and controlled by the enterprise.

ii. Establish an internal process to adjudicate limited exceptions, as defined by the Act and described in Section IV;

- ✓ **Fully Compliant.** Hypori and the data accessed through Hypori Halo remain within the secured government network at all times and cannot be exposed to malicious applications on the user’s edge devices.

iii. Remove and disallow installations of a covered application on IT owned or operated by agencies, except in cases of approved exceptions; and,

- ✓ **Fully Compliant.** This is a default feature of Hypori Halo, as only approved apps can be loaded into the application security templates. Users do not have access to any application store, nor can they “side load” any applications. This has been tested and validated via security testing by the Army’s Threat Systems Management Office (TSMO), Director of Test and Evaluation, (DOT&E), and other Defense and Intelligence Agencies.

iv. Prohibit internet traffic from IT owned by agencies to a covered application, except in cases of approved exceptions.

- ✓ **Fully Compliant.** Hypori Halo is set behind a security architecture that isolates all virtual workspace traffic to DoD cloud computing security requirements guide IL5 and .mil resources. Firewall rules within the architecture prevent traffic from accessing anything outside of approved sources.

For more information on Hypori’s zero-trust approach to secure BYOD, please request our [Hypori Defense In-Depth](#) whitepaper.