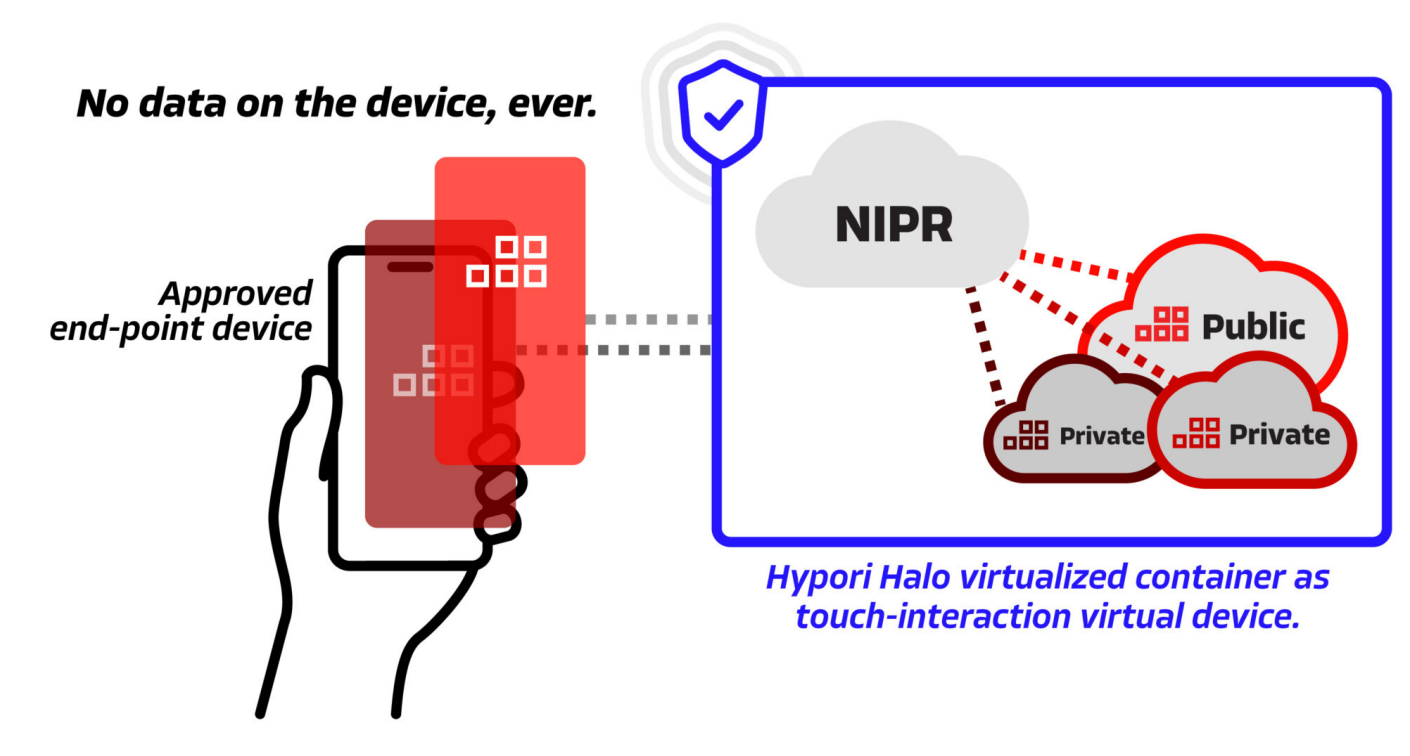
NETWORKS / CYBER, SPONSORED POST

Only Hypori Halo addresses the biggest telework work issue the pentagon faces: Trust

"Arguably, the most valuable thing that Hypori provides to DoD is the ability to allow endpoint users access to information, but with no loss of privacy and no inherent risk to DoD. I'm hoping that we can change the entire BYOD paradigm." - Hypori CEO, Jared Shepard

By HYPORI on February 22, 2023 at 8:30 AM

presented by HYPORI HALO



Hypori enables Army personnel remote access to Army's secure NIPR environment from their personal devices. Image courtesy of Hypori.

The U.S. military is in the midst of a seminal transition to a fully digital infrastructure. The shift will affect the way it fights and works, helping it capitalize both on the power of information and the opportunity to strategically disperse while staying connected. But the gains our armed forces make from this transition will only be realized if the remote systems underpinning it can be trusted.

Hypori Halo enables military personnel to securely use their own edge devices – mobile phones, tablet and iPads – to work from anywhere, increasing productivity and mission execution while collaborating with their colleagues and their chain-of-command. It's an application that users can download from the Apple App Store or Google Play in minutes.

Hypori Halo is central to the U.S. Army's Bring Your Own Device (BYOD) program and it's the only cloud access system which can be fully trusted by the Pentagon and by its users.

Bring Your Own

Telework ballooned across the private sector during the Pandemic and America's Armed Forces followed suit. The Pentagon turned to a commercial solution for the vastly expanded remote work it believed was necessary to continue to function, enabling Microsoft Office 365 mobile capability for the military/civilian workforce. The capability was well received but in the span of less than a year DoD recognized it wasn't secure the way it was configured. In June, 2021 Office 365 mobile capability was turned off.

But the military's need for telework has remained strong even as COVID-19 has faded. In fact, DoD's Mobility Unclassified Capability (DMUC) program for smartphones still exists. Ironically, the trauma of the Pandemic makes it easy to forget that the Army and other services have enabled service members and DoD civilians to work remotely via Government Furnished Equipment (GFE) for over 15 years. The once ubiquitous "BlackBerry" phones that Soldiers, Airmen, Sailors and Marines carried for over a decade exemplified this.

Uncle Sam paid for and supplied these devices and users were/are expected to conduct only official business on them with the resulting "phone in each hand" a common sight among service people and government officials. But a lot has changed in the last few years including the rise of the DoD cloud enterprise.

The Army's dedicated cloud environment is known as "cArmy" and the service is pushing to migrate most all administrative and semi-classified work to it, spending roughly $290 million this year to accelerate the process. BYOD is fundamental to its plans to allow service members to access shared data anytime, anywhere. The U.S. Air Force and Navy have their own BYOD efforts but the Army's is the most advanced.

Lieutenant General John B. Morrison Jr., the Army's Deputy Chief of Staff for Command, Control, Communications, Cyber Operations and Networks, recently affirmed that BYOD is no longer a pilot program. It is, he told an audience at the Army's IT Day 2023 conference, a "rolling start to the Army's enterprise". By March, it's expected that 20,000 Army personnel will be enrolled, using their own devices for remote work.

Hypori Halo is the Army's key enabler, in large part because of what it takes out of the BYOD equation.

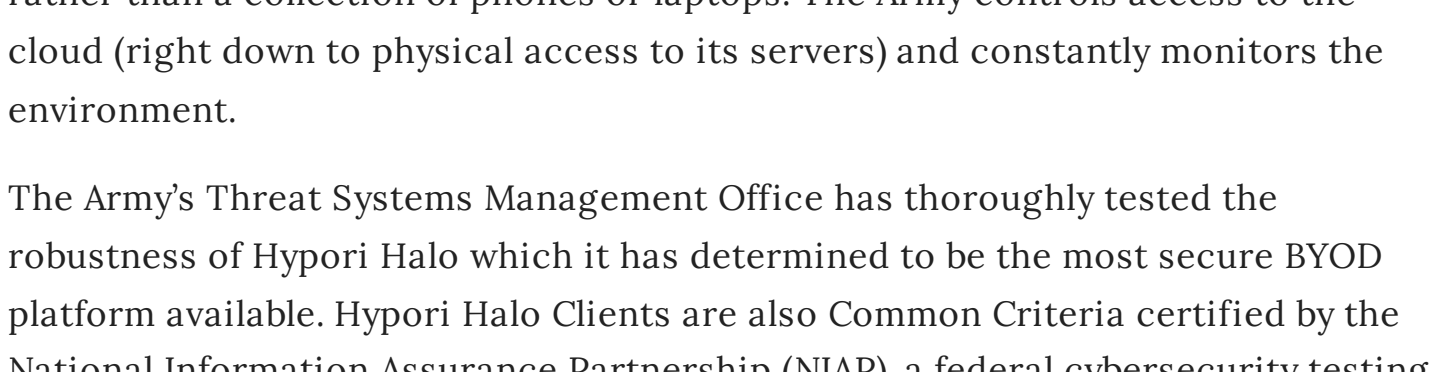
No Data At Rest

Hypori Halo adheres to the "zero trust" cybersecurity principle now widely accepted across the private sector, military and government. Zero trust requires that IT systems "never trust, always verify." The concept assumes that everything behind a firewall is vulnerable and mandates that every request for access to a system or network is fully authenticated, authorized, and encrypted before being granted.

But Hypori, based in northern Virginia, has taken an approach with its Hypori Halo solution that goes beyond zero trust. That's because it enables users' mobile phones and iPads to access cArmy to do all the things they need to do – exchange email, files, send messages/chats, draft documents, spreadsheets, conduct video conferences and work in other Army formats – without actually exchanging any data.

To put it simply, there is no data at rest on, nor any data in transit from any Hypori Halo user's device.

Instead, Hypori Halo renders applications and data that reside inside the cArmy cloud on a user's device as pixels. They are virtual images of what lies inside the Army cloud. Outgoing Army CIO, Dr. Raj Iyer, has been a staunch advocate of Hypori Halo. He describes Hypori Halo-enabled phones as "dumb display" units which show representations of email, scheduling, spreadsheets or other applications hosted by cArmy.



The Hypori Halo App leverages FIPS 140-2 crypto and TLS 1.2 encryption, supports PKI credential-based multi-factor authentication, and is NIAP Common Criteria certified. Image courtesy of Hypori.

This approach shifts security from the device to the cloud itself. Hypori Halo implements the true nature of zero trust on the end user device. The end user cannot connect if it is compromised, meta data from the device is encrypted in transmission and data is never transferred back to the device – only pixels. Hypori Halo allows the service to focus its efforts on defending a single point – cArmy – rather than a collection of phones or laptops. The Army controls access to the cloud (right down to physical access to its servers) and constantly monitors the environment.

The Army's Threat Systems Management Office has thoroughly tested the robustness of Hypori Halo which it has determined to be the most secure BYOD platform available. Hypori Halo Clients are also Common Criteria certified by the National Information Assurance Partnership (NIAP), a federal cybersecurity testing organization managed by the National Security Agency. The solution is so secure that it can be used to connect to the most sensitive government networks with appropriate controls in place.

"We have had it red teamed ad nauseam by elements outside of the Department of the Army," Gen. Morrison told *Signal* magazine late last year, "and the assessment that came back in said the path that we're on is one of the most mature that's out there."

Hypori Halo represents a path and an application that others in the defense establishment are recognizing. In a recent paper published by the Center For Strategic and International Studies, CSIS Fellow and active duty Marine Corps Colonel, Atiim O. Phillips, stressed that Army's approach to BYOD has redefined the concept of telework for service members.

"The implied and forward-thinking aspect of this new definition," Phillips said, "is that government data should no longer be authorized to be stored on personal devices."

That's precisely what Hypori Halo makes possible.

"The term 'virtual government furnished equipment' was coined by the Army's director of test and evaluation [ATEC] to describe Hypori Halo," Hypori CEO, Jared Shepard observes. "We are virtual GFE which they found to be more secure than physical GFE."

The Paradigm of Two-Way Trust

For the military's vision of collaborative, remote work to become reality, the Army, and more broadly DoD, are depending on the security of software access to the cloud and something perhaps even more important – user trust.

Personnel from the Army and other services rightly perceive personal risks in BYOD. When their own phones and laptops can become the front-line in information warfare, they recognize how vulnerable they, and their families, may be.

A well-placed cybersecurity source within the Army recently observed that "if folks are aware of privacy issues, they're generally aware that anything they do on their [BYOD] platforms isn't private."

That's because the cloud access applications used in other BYOD programs, both military and commercial, come with a Mobile Device Management (MDM) approach which requires the environment (cloud) owner to take control of the device to ensure security and compliance issues. They must follow this "endpoint control" approach because data is transmitted to and from the device and resides on it – right next to vulnerable popular applications like Tik-Tok, Snapchat or Twitter.

"What was interesting to us about Hypori Halo," Dr. Iyer told *Forbes,* "was that we could implement it on devices that were unmanaged. Before BYOD, one of the things we consistently heard from our users was that they didn't want their cellphones to be monitored or wiped if there was any potential [data] spillage."

MDM cloud access applications raise that spectre with a potential negative impact on user adoption and resulting legal entanglement. Hypori's CEO points out that the Air Force's BYOD end user license agreement includes 13 pages of warnings with respect to user responsibilities and liabilities.

"Who wants to sign up for that kind of thing?" Shepard asks.

In cases where there is a data spillage from an endpoint-controlled user device, DoD will likely need to seize the device with all of the private data aboard it, opening a Pandora's Box of liability. In such cases, the BYOD service member may have justifiable cause to download data (family photos of children) they don't want the government to access before handing over a device.

If that device has downloaded controlled classified information from the cloud, the service member could be held liable for committing a felony. The legal investigations the military might have to carry out in such cases (potentially numerous) would strain both its own resources and its trust-relationship with service members. Other risks, from bad-actor exploits arising from endpoint control access inside MDM software providers to the presence of malware on BYOD users devices, are present as well.

Hypori Halo does *not* have the ability to view or access the user's personal information on the physical device – nor does the Army. As such, Hypori Halo obviates legal risk from GDPR-like laws (General Data Protection Regulation, Europe's data privacy and security law) now arising in places like California (CCPA). As Hypori executives note, the Army does not *want* access to the user's physical device.

The Hypori Halo app for Army BYOD keeps Army data 100% separate from user personal data. For example, the Army cannot see browser history, social media used, or access photos. There is total separation between the Army Hypori virtual workspace and the user's personal environment. It's two environments in a single device with 100% privacy for both. Image courtesy of Hypori.

"Arguably, the most valuable thing that we provide to DoD is the ability to allow endpoint users access to information but with no loss of privacy and no inheritance of risk to DoD," Shepard says. "I'm hoping that we can change the entire BYOD paradigm."

Scalable Trust

Among the attributes which make Hypori Halo attractive are its scalability and flexibility. It can be acquired for large or small user populations and its single license/multiple device use contract saves the government money. As Hypori's CEO notes, "There's no additional infrastructure cost, no additional hardware cost."

Such cost saving is making it possible for the Army to do something it couldn't previously do. It can now broadly extend telework capability to the National Guard and Reserves. In fact, expanding collaborative remote work capability to Citizen-Soldiers was the "driving force" in BYOD from start Shepard explains.

"The National Guard, Air National Guard and Army Reserve arguably have the greatest need for this capability. Part-time military members don't have access to the same resources their active duty counterparts do which means they don't have access to GFE. They also have day jobs."

Shepard points out that many of those with civilian jobs from bank employees to airline pilots already have work-mandated MDM cloud access applications on their phones.

"But you can't have two MDMs on a single mobile phone. That means Hypori is actually providing the Guard and Reserves a mechanism with which they can securely remote work for the military that does not disrupt their day job."

And since a Hypori Halo-enabled device affords them the opportunity to work remotely, they no longer have to drive 45 minutes each way to an Armory to get 20 minutes worth of work done. "That productivity is worth a lot to the Guard and Reserves," Shepard adds.

So is Hypori Halo's operational flexibility. The solution works with Android and Apple phones and is backward compatible with a wide range of devices so long as they are currently supported by their manufacturers. For example, the iPhone 6 and 7 are still supported by Apple. This flexibility in-turn eases adoption for users who don't need the latest and greatest phones or laptops with large memory (RAM) capacity or the latest, fastest processors (CPU) to participate in BYOD.

By lowering the bar for adoption and the risks of use (security, liability) of BYOD, Hypori Halo is an effective out-of-the-box SaaS solution for the Army and other military and civilian customers. Its operating logic wherein no data is saved on the device means there's no data to lose, no data to leak, no data to wipe.

"We've essentially taken the endpoint [risk] out of the equation," Shepard affirms. "We're changing the way any other competitor out there thinks about zero-trust."

In an environment where just 13% of Americans say they have a high willingness to join the military, where the services face serious recruiting shortfalls, and where cyber-attacks on military infrastructure occur in ceaseless intervals measured in minutes, trust matters.

Hypori Halo is the only remote mobile application which truly offers it.

Topics: cyber, cybersecurity, Hypori, Hypori Custom, Pentagon, Presented by Hypori, sponsored content, telework