

Mobility Without Vulnerability

Removing the Mobile Attack Vector





Wayne Lewandowski

Chief Revenue Officer, Hypori

30-year IT & security industry veteran

Revenue leadership, Multi start up experience
with over \$500MM in Exit value

Sales & Ops Advisory board member

St Petersburg, FL



The Evolution of Modern Work

IDC: More than 1B smartphones shipped annually; Into an already dense market



Centralized



Distributed



Anywhere

The Proliferation of Mobile Work and BYOD

From 2000s



From 2010s



From 2020s



**From company-owned
to personal devices**

• Business-driven • Opportunistic • MDM



**Basic enterprise
applications**

• Content-driven • Broad • MAM/EMM



**Extensive library of cloud
applications and data**

• Experience-driven • Ubiquitous • UEM/Secure Virtual Mobility



Office 365



Google



Adobe



X



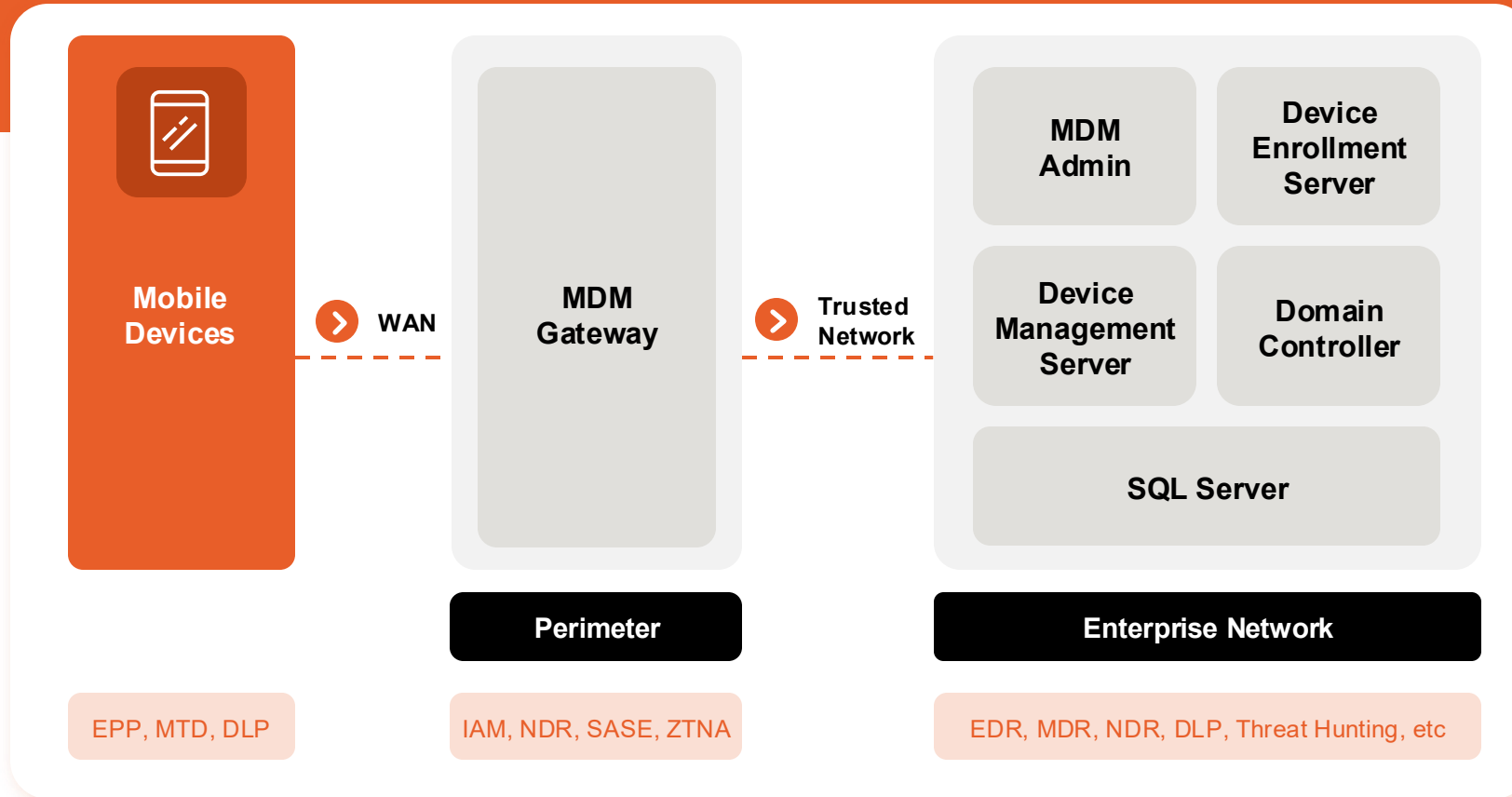
Reddit



LinkedIn

MDM Architecture: An Example

Resource intensive. A changing landscape. Risks and challenges.



- **Protecting data** from MitM attacks, breaches/leakage/loss.
- **Contractor challenges** including MAM limitations; GFE restrictions.
- **Jailbreaking** and **rooting**.
- The need to **secure mobile attack surface** against malware and viruses.
- The possibility of a mobile device being **wiped, confiscated, subpoenaed**.
- **Unsecured Wi-Fi**
- Protection against **phishing** attacks

Challenges from the MDM-based BYOD era



SECURITY

Data exposure risks



PRIVACY

Monitoring and wipe of personal device



COMPLIANCE

MAM doesn't stop download of apps



COMPLEXITY

Layers of systems to manage devices



COST EFFICIENCY

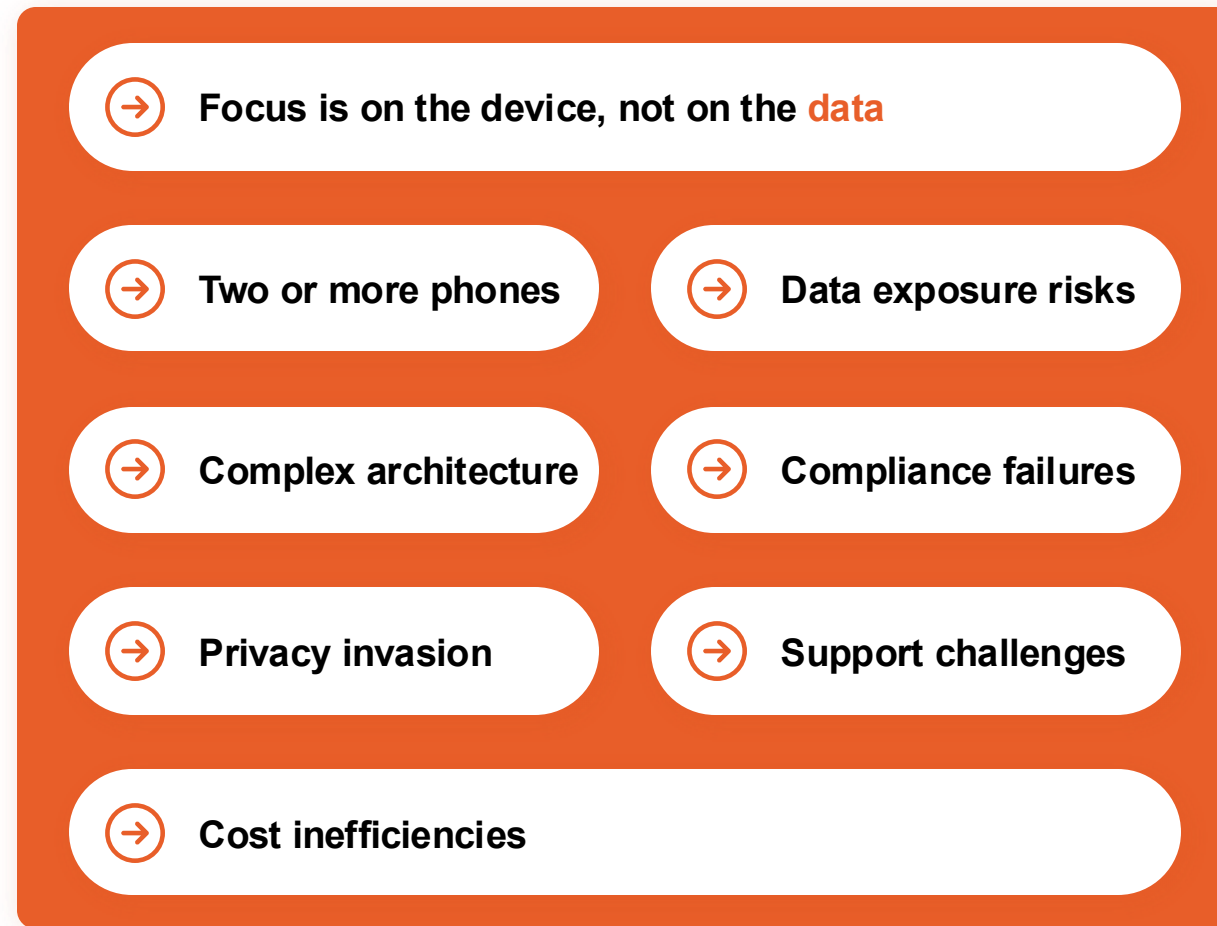
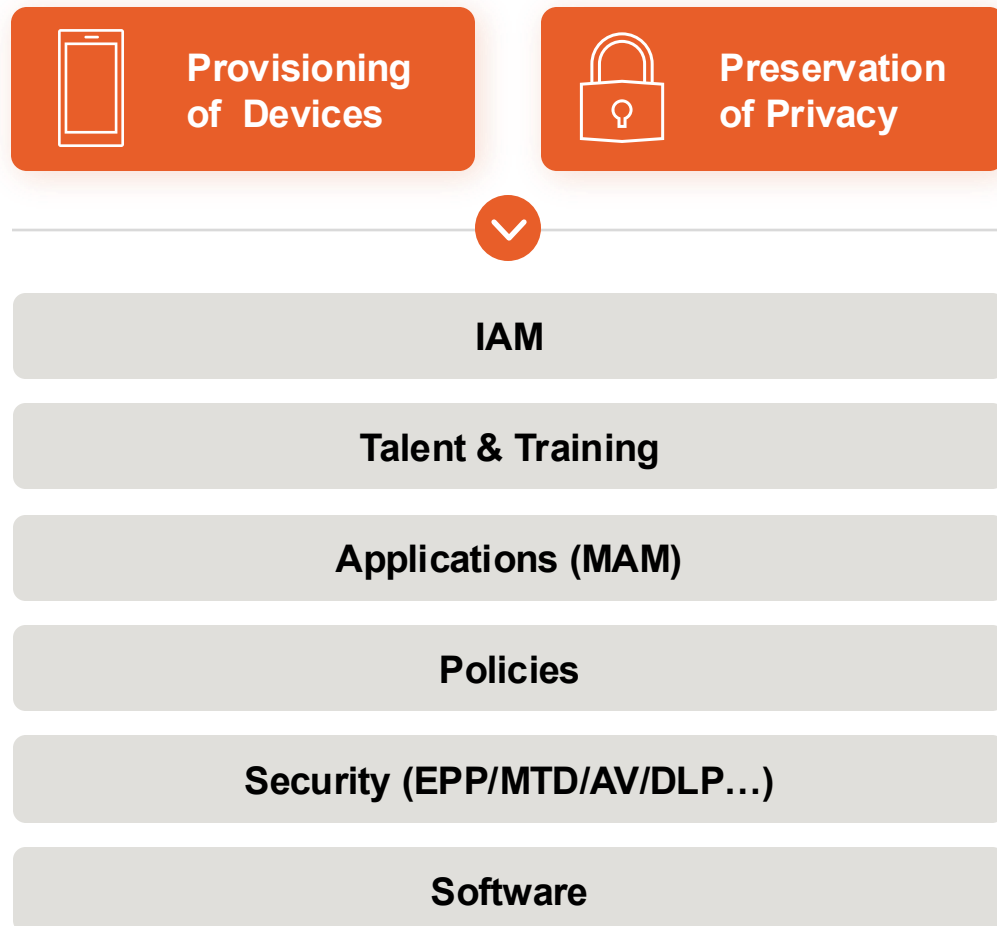
Layers of systems means layers of costs



PERFORMANCE

Consumes system resources and battery life

The Downside of Complexity



How can this be minimized?



In 2024, 56% of zero-day exploits targeted end-user tech, including mobile devices.

(Source: Google TIG)



Hypori assumes the edge is compromised.

The perimeter needs protection like never before: Better and stronger than MDM/MAM/EMM/UEM.





Hypori®

One Device, Zero Worries™

The New, Elegant, BYOD from the
World's Leading VMI Innovator

**Total Personal
Privacy**

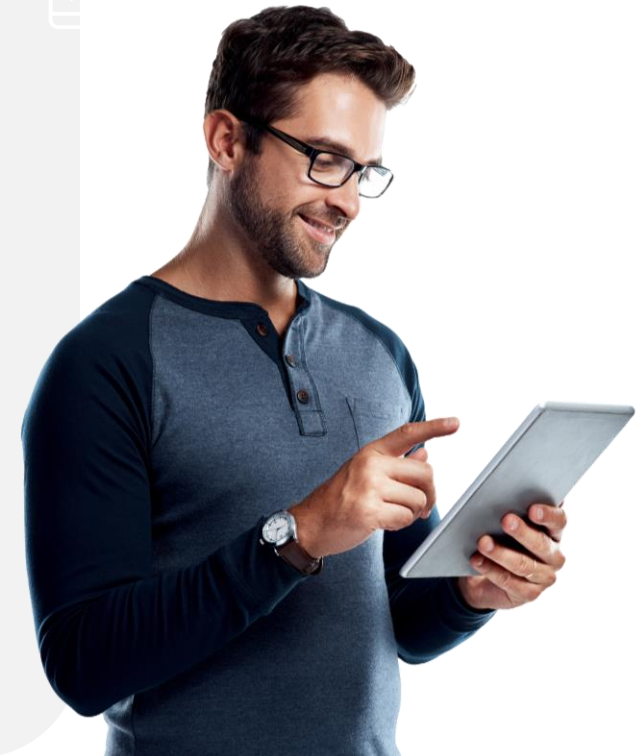
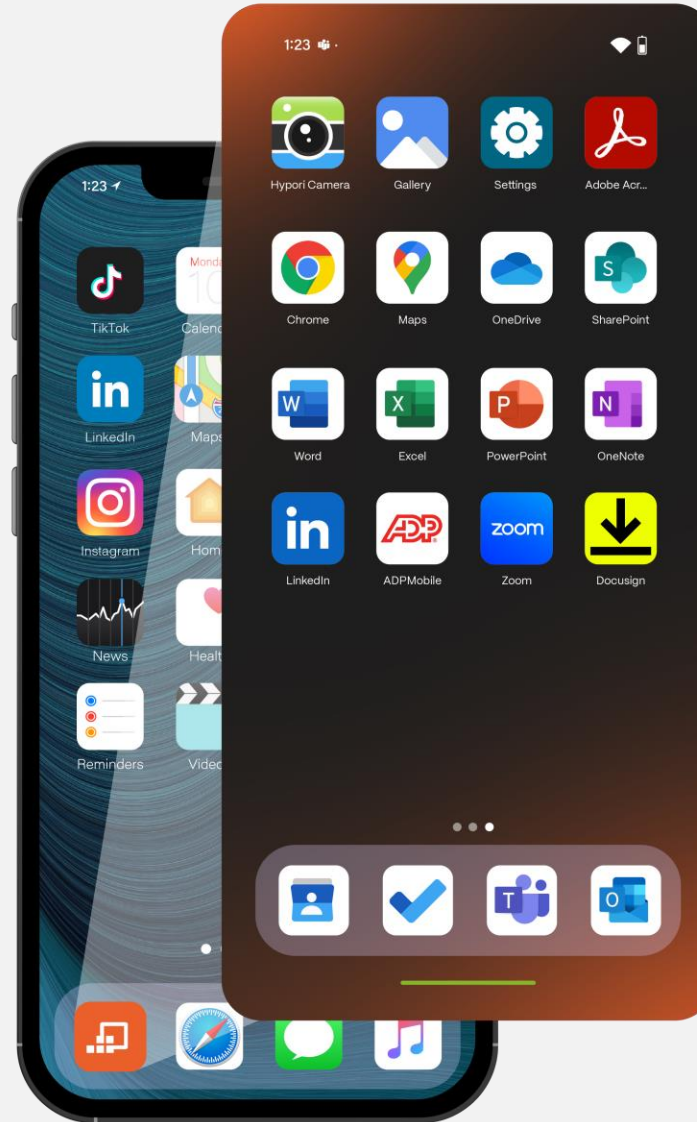
**Secure Virtual
Access**

**Worry-Free
BYOD**

**Reduce Risk
& Liability**

**Proven &
Compliant**

**Easy &
Cost-Efficient**



Cost Efficiency: 42%+ Savings



Traditional BYOD Program (MDM/MAM)

vs.



Virtual Mobility Infrastructure (VMI)

- > Multiple cost layers: applications, support, SaaS/software, training, people, infrastructure, and more.
- > Attack surface remains a growing a challenge
- > An estimated \$518/year on BYOD for each employee

- > Only cost is SaaS license
- > No attack surface
- > An estimated \$300/year on VMI

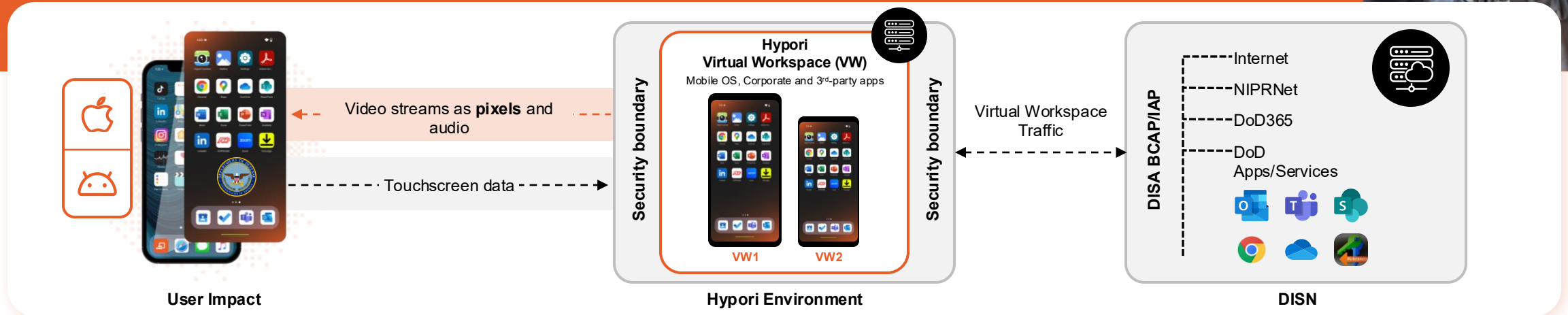


Hypori. vs Traditional MDM Vendors

One Device, Zero Worries™

	Hypori.	vmware	mobileiron	Microsoft Intune	ManageEngine	SOTI	IBM	XenMobile	BlackBerry UEM
Guaranteed user privacy with 100% separation of corporate & personal data	●								
Access to multiple secure enclaves	●								
Android & iOS app	●	●	●	●	●	●	●	●	●
App performance independent of device compute limitations	●								
Geofencing / location services	●	●	●	●	●	●	●	●	
Mobile bandwidth use management	●	●	●	●			●	●	
No data at rest on the device	●								
No device enrollment required	●								
Remote wipe / selective wipe	UNNECESSARY: NO DATA ON THE DEVICE	●	●	●	●	●	●	●	●
Remote lock	UNNECESSARY: NO DATA ON THE DEVICE	●	●	●	●	●	●	●	●
Single sign on (SSO) for all apps	●	●	●	●	●	●	●	●	●

No Data in Transit, No Data on Device



User Impact

- Access enterprise apps and data from anywhere on any device.
- No loss of privacy.
- Enhance employee efficiency allowing secure work on the move and outside business hours.

Enterprise Impact

- No data saved on the device.
- No data transmitted.
- No spillages.
- No exposure to behavior/apps.
- No liability from personal device.

More secure, more flexible, at a fraction of the cost

Hypori is Secure and Compliant

Single Tenant Secure Cloud



FedRAMP High



IL5 High



All Hypori Apps have
been Common
Criteria Certified for
5+yrs



"Most Secure
Mobile platform
tested to date"



CUI

Approved to provide access
to CUI



Secure Multi Tenancy Cloud



CMMC



Rated to protect PHI

Secure Work: Use cases



Eliminate corporate-issued devices



Travel globally with secure mobile access



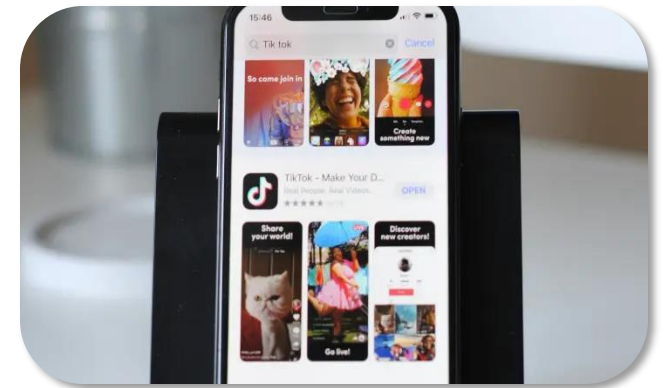
Enable CMMC compliance for mobile



Protect patient data with secure virtual access



Swiftly mobilize contractors



Protect against malware and malicious apps

Trusted Globally by Commercial & Government Customers



**Trusted BYOD program
for the DoD**



**Tested & Verified: 15+
NSA Red Team
exercises**



**Highest levels of
Gov/DoD certifications**



**Large-scale customer
deployments**



The Magic of Hypori



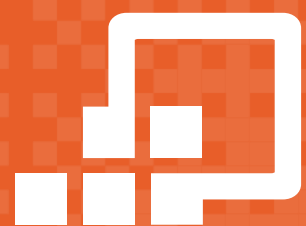
A demo by

Michael Leonard
Account Executive

“Where the idea of the enterprise, the encrypted pixels of its apps and data, is securely streamed to your device for you to touch, type, swipe, and interact with information that never leaves the cloud.”

Jared Shepard
Founder and CEO, Hypori

Embed Video – it is too big to email.
[HYPORI BrandSpot 60 FINAL.mov](#)



Hypori[®]

One Device, Zero Worries[™]