HYPORI™
VIRTUAL MOBILITY

Understanding the Security Risks of BYOD and Mobile Device Use in Today's Enterprise

WHITEPAPER

Summary

Mobile devices are central to our personal and professional lives. Even before COVID-19, today's enterprise saw increased use of mobile devices for work functions. Employees show increased workplace productivity and satisfaction with personal device use, and they reject carrying more than one device making corporate-issued devices obsolete.

For employers, mobile device use is also advantageous. With BYOD, there is no need to invest in corporate devices leading to cost savings. Today, employers rely more and more on widespread mobile device use, in many cases, without formal BYOD policies or procedures in place.

While employees prefer mobile device use and employers have had to allow it, it presents security risks to enterprise networks and systems. Although some of the same risks apply to mobile devices as to PCs, using the same security protocols does not cover the full mobile risk spectrum. Enterprise risk management must evolve to incorporate mobile-specific security solutions.

The Situation

Mobile accessibility is the key to more connectivity, improved productivity, and economic sustainability in today's remote work environment.

Work-function mobile device use was widespread before COVID-19. However, today it is essential. Yet, heavy reliance on mobile devices with their inherent security risks creates vulnerabilities for both enterprises and individuals.

Cybersecurity risks have been on the rise year-on-year for the last decade. Over the previous nine months, that increase has been exponential and shows no sign of slowing. According to a Verizon 2020 Data Breach Investigations Report, before the pandemic, phishing and credential theft made up 67% of breaches. Today, users are three times more likely to click on suspicious links, particularly because bad actors capitalize on COVID-19-related fears and use pandemic-specific terms as bait.

In today's organization, over 60% of endpoints accessing or storing enterprise data are mobile. Most of these mobile devices do not have security solutions and may even be running out-of-date operating systems, and COVID-19 has meant fewer or more flexible security measures.

With mobile device use on the rise, remote work now commonplace, and increased cyber risks, there is no question that we must understand and plan for the inherent security challenges in these changes.

The Problem

Understanding the scope of mobile threats means looking at a range of security concerns. Three major risk components relate to mobile device use: threats, software vulnerabilities, and behaviors and configurations.

Each organization must assess these factors as they relate to their business, but there are general consistencies in these risks facing enterprises today. An overall understanding of the mobile risk landscape is imperative to keep pace with increased remote work, mobile device use, and the future of enterprise IT.

Threats

Mobile threats include malicious attacks on apps, devices, networks, and even web content. One significant concern is malicious mobile apps. They can steal information, cause physical device damage, and give remote access to unauthorized devices. Device threats are another problem where attackers gain higher permission levels than with apps causing catastrophic data loss. Mobile threats impact networks because of multiple network entry points and data in continual transit. Finally, web and content-based threats include things like phishing emails containing false links masquerading as login pages, downloads, or updates.

Vulnerabilities

A few vulnerabilities stand out when it comes to mobile security. Mobile apps are a significant concern because end-users select apps based on personal preference. The enterprise has no control over what is used, nor are IT departments able to vet them.

Security vulnerabilities are also present in out-of-date devices. End-users not only control their apps, but they also decide when they update or patch their devices, leaving them open to attack. Only with official and policed enterprise-wide BYOD policies can these vulnerabilities be eliminated.

The Problem (continued)

Behaviors & Configurations

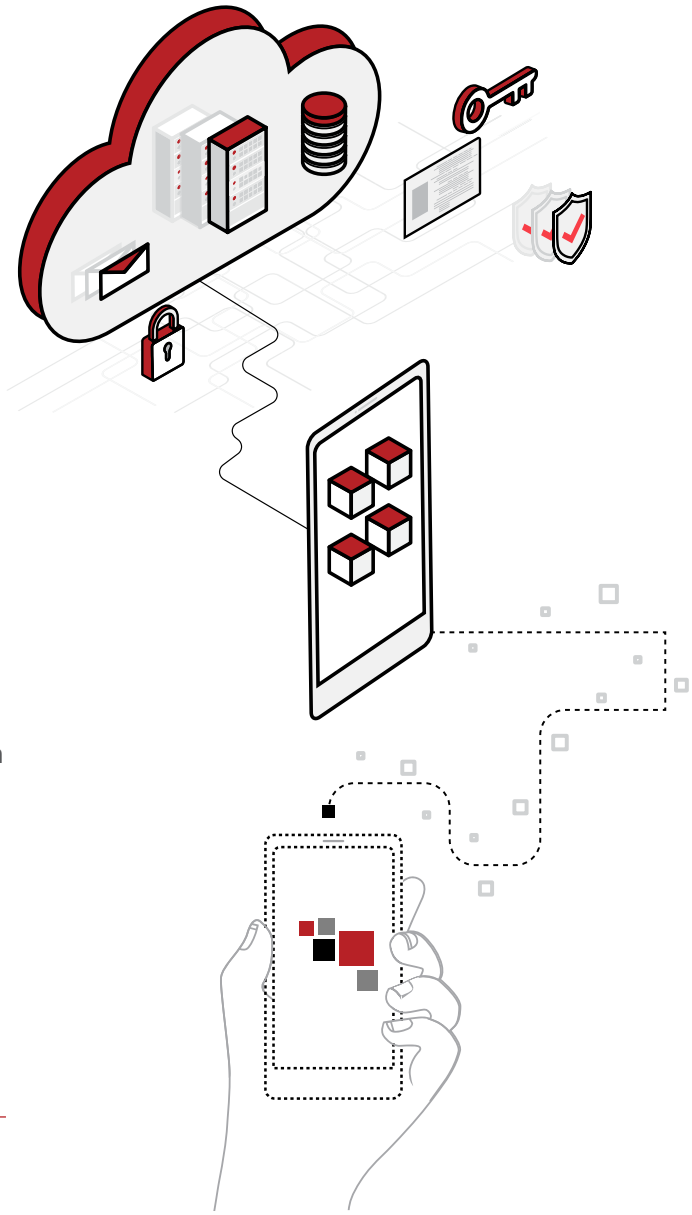
User behavior is another significant factor in enterprise management mobility risk. Employees access sensitive enterprise data and store it on their mobile devices. They also use public cloud-based storage services and access compliance data such as credit card or personally identifiable information (PII) without adequate security protection. Data leakage is a risk when stored on a vulnerable, unsecured employee device lacking a sufficiently strong password or PIN.

Another major behavior-related problem is network-related. Imagine every employee accessing public Wi-Fi with multiple devices. As users access numerous networks daily, each connection poses a threat to the enterprise. Web and content risks in this category are related to opening malicious content that can infect devices and then compromise enterprise systems.

While many companies look to MDM to address these issues, it's critical to note MDM's drawbacks. MDM solutions demand strict security settings, deny web traffic, and otherwise intrude on user experiences requiring end-users to cede their phones' control and allow corporate visibility into their data. With MDM, personal information is visible to the organization and can be remotely wiped, raising privacy concerns and liability issues for the enterprise. Many employees resist, circumvent, or refuse corporate MDM solutions rendering them ineffective and a waste of corporate resources.

The Solution

Hypori Virtual Mobility addresses the security risks of BYOD and increased mobile device use in today's enterprise. Hypori's solution securely contains all enterprise data on a fully-featured virtual mobile device in the company-owned data center with 100% separation from end-user details and total administrative transparency. Since all enterprise data resides safely on the company-owned device, there is no need to secure or control end-user personal devices eliminating the privacy and legal concerns associated with MDM solutions.



With Hypori, the enterprise shifts cybersecurity management from vulnerable personal devices to a secure data center. Organizations have no access to personal data on end-user devices, and no exposure should they be compromised. All mobile device users have secure virtual access to the enterprise data needed for maximum productivity, are empowered with their own devices, and are confident that their privacy is protected.

Hypori delivers a military-grade secure, centrally managed, admin-friendly Virtual Mobility Solution for your enterprise that is regulatory compliant, cost-efficient, and user-intuitive.

To learn more about Hypori Virtual Mobility, contact us for a demonstration today.

Contact us

info@hypori.com

*The National Security Agency Commercial Solutions for Classified (CSfC) provides DoD entities the ability to conduct secure classified communications using Commercial-off-the-Shelf (COTS) products. Under this program the Mobile Access Capability Package v2.0 provides a framework for how to secure these communications from mobile end user devices into government enterprise resources. Under the MACP v 2.0, communications must be established using an inner and outer tunnel to provide the secure communications path. Intelligent Waves, LLC's Hypori Client v4.1 for iOS and Android is eligible to be used as a TLS Software Application Product component in a CSfC solution. This means that in combination with a CSfC eligible TLS Protected Server, Hypori is eligible to provide the inner tunnel for secure communications.

11 March 2019

hypori.com