Hypori
One Device, Zero Worries™

Solution brief

The risks of BYOD and using virtualization to eliminate risk and preserve privacy

According to Gartner, 48% of employees will work remotely at least some of the time in the post-pandemic world, compared with 30% before. Mobile devices are essential to both personal and professional lives, with over 6B smartphones in use worldwide. Even before COVID-19, today's enterprise saw increased use of mobile devices for work functions and growing use of "bring your own device" (BYOD) by U.S. companies. Employees show increased workplace productivity and satisfaction with personal edge device use, and they reject carrying more than one device making corporate-issued device programs obsolete. Today, 83% of companies have a BYOD policy of some kind, many without establishing proper security policies or procedures.

Just like their commercial counterparts, Department of Defense (DoD) personnel need secure digital access to government data and applications and controlled unclassified information (CUI), from their personal devices easily, at scale, and without risk of data loss and privacy breach.

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

The situation

Secure, remote access to enterprise apps and data from the edge is the key to connectivity, increased productivity, and economic sustainability in today's remote/flex work environment but heavy reliance on mobile devices with their inherent security risks creates vulnerabilities for both enterprises and end-user privacy.

Cybersecurity attacks on mobile devices continue to put organizations at risk for theft, ransomware, and espionage. 42% of organizations report that vulnerabilities in mobile devices and web applications have led to a security incident. 97% of companies have faced cyberattacks involving mobile threats. Today, over 60% of endpoints accessing or storing enterprise data are mobile. Most of these edge devices do not have security solutions and may even be running out-of-date operating systems. With remote/flex work becoming the norm, we must reconsider how we secure the edge.

Hypori
One Device, Zero Worries™

Solution brief

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: behaviors and configurations, cyber threats, and software vulnerabilities. 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/flex 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. Bad actors also pose threats to individuals' personal identifiable information (PII) and organization networks using "man-in-the-middle" attacks to compromise any number of assets, including customer data, intellectual property (IP) or proprietary information about the organization and its employees. 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.

Behaviors and configurations

User behavior is a significant factor in enterprise mobility management 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 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 behavior-related problem is accessing and trusting unknown networks. As users access numerous WiFi networks daily from multiple devices, 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.

In addition to these risk components, organizations and government agencies must consider the user experience, employee preferences, and their privacy when implementing a BYOD solution.

Privacy concerns

While many companies look to mobile device management (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 surrender their phones' control and allow corporate visibility into their personal data. With MDM, personal information is visible to the organization and can be remotely wiped, invading personal privacy and raising liability concerns for the enterprise. Many employees resist, circumvent, or refuse corporate MDM solutions rendering them ineffective and a waste of corporate resources.

Hypori

One Device, Zero Worries™

The solution

Virtualize the workspace, eliminate the risk, and preserve end-user privacy.

Hypori challenges conventional thinking and proposes that organizations secure their data, not the device because data on the device is vulnerable. Hypori secures the enterprise data and apps in the cloud, does NOT transmit data to the device, and does NOT leave data at rest on the device. The Hypori app can be added to any edge device to deliver one, or multiple, zero-trust, 100% separate virtual workspaces that preserve end-user privacy while enabling enterprise access and employee productivity.

Contact us today at
www.hypori.com/contact
or email info@hypori.com

Request a Demo

Why Hypori?

- Total Personal **Privacy**
- **Secure** Virtual Access
- **Worry-free** BYOD
- **Reduce risk** and liability
- Proven and **compliant**
- **Easy** and convenient

WATCH VIDEO