The Best Enterprise Mobility Solutions for Your Organization's Remote Workforce

by Jenny Kanevsky | Jan 15, 2021 | EMM | 0 comments

According to an IDC study, the US mobile worker population will rise from 78.5 million to 93.5 million by 2024. As a result, employee mobility solution needs will continue to grow. Mobile device use, and the associated enterprise attack surface, increased significantly in 2020, in large part due to COVID-19 and a growing remote workforce. In Q1 2020 alone, mobile phishing attacks on corporate users increased by 66.3%.

Organizations mobilizing their workforces must stay competitive, but they must also consider and accommodate security concerns, cost, data access, employee acceptance, and other issues.

Employees and How They Work Best

Remote work increases require heightened and diverse digital security that protects enterprise data wherever it's accessed. For IT professionals, securing these devices is a

challenge. According to Cisco, more than 50% of Chief Information Security Officers (CISOs) say that mobile devices are significantly challenging to defend. Enterprise mobility solutions address security executives' mobile security concerns, though their methods vary.

Characteristics like workforce size, IT budget, and regulatory compliance determine whether a company builds a Bring Your Own Device (BYOD) program or issues devices under a Mobile Device Management (MDM) program. MDM solutions can also be BYOD. However, these MDM programs allow IT to control employee devices raising privacy and liability issues. The workforce's size and organizational complexity impact the time and effort spent to roll out policy changes.

Working styles and responsibilities play a critical role in which solution to choose. Salespeople and engineers who split time between offices and client sites require seamless integration between office and travel. Alternatively, fully remote employees don't need traditional in-office platform integration. The off-site responsibilities and environment will dictate whether employees need a smartphone, tablet, or laptop.

An enterprise mobility solution's design dictates security protocols. Traditional MDM relies heavily upon on-device security, so users earn most of the data protection responsibilities. A Virtual Mobility Solution (VMS) secures data, not devices, so usage protocols are less invasive.

Employee resistance to security policies, such as those required with MDM solutions, may cause data loss. When a solution's security protocols restrict freedom and productivity, employees may circumvent or reject its protocols, for example, by using personal email instead of a secured corporate account.
When a solution can't provide sufficient access or local processing power, managers may authorize the use of less secure methods such as transferring data to a personal computer for processing. In these cases, the company loses control of the data, regardless of MDM's remote wipe capabilities.

Enterprises cannot overlook the importance of solution acceptance and adoption.

Mobile Device Use

Companies must also consider the actual devices and their features. Devices need sufficient processing power, and mobile networks must provide adequate bandwidth. If the

devices enrolled in the BYOD program do not meet the minimum standards, the company must weigh whether to subsidize upgrades or take another approach.

Non-virtualized solutions like MDM, Virtual Private Networks (VPNs), and Mobile App Management (MAM) deplete storage space, reduce battery life, and impact personal device processing speeds. Alternatively, VMSs operate at data center connectivity speeds and don't rely on the end-user device processor. With VMSs there is minimal impact on the device processor and battery life.

From the security angle, compromised devices infected by viruses can lead to data loss and leakage. Immediate software patching significantly mitigates this risk. Solutions like MDM and MAM have complicated update processes, mostly where programmers must write code for many different environments (e.g., iOS and Android operating systems, and various device models).

Having multiple computing environments further complicates security for custom apps and introduces new attack surfaces. Conversely, a virtualized container solution provides a single computing environment for developers, and IT administrators can push updates to all containers with a one-click procedure.

Data Considerations

Data types, sizes, and processing needs are also considerations. Massive files and heavy processing demand virtualized solutions because their architecture shifts heavy lifting to remote corporate servers. A battery-powered, single-processor smartphone cannot outperform a server rack.

Non-networked solutions cannot handle dynamic data, which is a concern for healthcare, infrastructure monitoring, and finance applications. Monitoring applications require an always-on, always-connected solution with centralized data management, which ensures data integrity.

Lost and stolen devices also present security problems. Mobile Information Management (MIM) and MDM solutions can solve this problem by encrypting data on the device. MAM may solve this problem with ring-fencing and encryption. However, MDM can remotely wipe devices creating privacy and liability issues. All of these non-virtual solutions suffer from potential employee circumvention and loss of control over data. Virtualized solutions

eliminate data storage on the device, avoiding the problem altogether. End-users access and interact with data via encrypted pixelated streams with no data at rest.

Different solutions have varying degrees of success in mitigating more advanced attacks. VPNs may fall victim to security against man-in-the-middle (MITM) attacks, which silently intercept data flows between senders and receivers. RAM attacks affect MAM, MIM, and MDM, taking advantage of the local data-decryption process. A VMS keeps data on the corporate server and prevents RAM attacks.

The Solution Shapes the Company

As industries move toward greater mobility and fully remote work, an enterprise mobility solution's importance grows. Companies must consider many mobile workforce concerns, including cost, employee adoption, security, and data accessibility. The chosen solution will shape the company's direction and culture.

Remote work challenges call for a networked, virtualized, and centralized solution that promotes scalability, ease of implementation, cost-effectiveness, and wide-adoption. Hypori Virtual Mobility™ is the answer.

Hypori® is a military-grade secure, budget-conscious, user-friendly BYOD solution. Its innovative architecture provides instant, consistent data protection. Remembering to switch on the VPN or re-encrypting data isn't necessary. Employee flexibility promotes better adoption and less circumvention, and seamless integration minimizes technology-based frustrations.

Hypori keeps organizational data current and limits productivity and workflow disruptions. The virtualized design prevents data loss from network failure because all information remains safely stored on central company servers. Hypori solves enterprise mobility challenges with ease, at scale, and within budget.