Mobile Device Remote Work Technology in the age of COVID-19 - Why MDM Doesn't Work

Today, mobile device use has never been higher, particularly in the workplace. Even before COVID-19, organizations saw increased use of mobile devices for work functions. Recent Stanford University research reports that 42% of the US workforce is now 100% remote, and work-from-home employees contribute more than 66% of today's US GDP.

While necessary, the COVID-19-related remote-work explosion, increased mobile device use, and rapid BYOD implementation present an expanded attack surface and robust opportunity for cybercriminals. Cybersecurity concerns are more prevalent now than ever. According to the Federal Trade Commission, from January to September 2020, Americans lost more than $145 million to COVID-19-related fraud.

A recent IBM Cost of A Data Breach Report found that in 2020, the average cost of a malicious attack data breach was $4.27 million. Data breach costs are expected to reach $5 trillion worldwide by 2024. More remote work and increased employee use of mobile devices compound the data breach response challenge. Bad actors are capitalizing on economic and social changes while legitimate IT and security leaders seek answers.

MDM - A Solution That Misses the Mark

Many organizations use Mobile Device Management (MDM) software solutions to address organizational mobile device use, implement safe, user-friendly BYOD, and secure enterprise data and networks. MDM began to control and secure mobile devices as they infiltrated the workplace and safeguard the systems these devices accessed. MDM relies on endpoint software—an MDM agent installed on the user device and an MDM server in a data center. MDM solutions are not inexpensive and are administratively cumbersome. Every employee device must be maintained, updated, and managed throughout the employee's tenure. Also, once company data moves to the mobile device, it is challenging to protect and control.

MDM allows employees to use their devices for work functions; however, it requires them to cede device rights and privileges to IT, thereby risking privacy for convenience. End-users have been

willing to allow this intrusion for the sake of BYOD. However, this willingness is waning. Today, rather than comply with MDM protocols, many employees circumvent or outright refuse to use company-installed MDM solutions, rendering them useless and a waste of administrative and financial resources.

Because personal device information is both viewable and controllable by the company, MDM is considered intrusive. MDM solutions also demand strict security settings, allowing organizations to police app use, deny web traffic, and otherwise intrude on the end-user experience. Finally, should an employee device be compromised, IT must do a remote wipe, meaning they may lose all personal data, a significant price to pay for any employee. These factors all create a love/hate relationship with MDM. Users appreciate the convenience of BYOD but resist or reject having to forfeit their privacy and control.

Virtual Mobility Solutions - A Better Option

Virtual Mobility Solutions (VMS) are next-gen BYOD technology in a global Mobile Device Management market expected to grow from $4.3 billion in 2020 to $15.7 billion by 2025. VMS deliver the freedom of mobile device use, end-user privacy, and the highest level of enterprise network security. VMS come in a "mobile-first" thin client experience that keeps all apps, data, and management in the enterprise enclave on enterprise servers rather than on endpoint devices. The Virtual Mobility platform allows users to access a remote, secure company-owned virtual mobile device from their physical iOs, Android, or Windows 10 device. VMS are similar to Virtual Desktop Infrastructure (VDI) but designed for touch interaction.

VMS allow low-end devices like smartphones to run high-end software while maintaining a 100% separation of personal and enterprise data. Since no company data resides on the personal device, security is enhanced. Bad actors have no inroads via app downloads, email providers, text messages, or other typical end-user avenues. Employees use their own devices, increasing productivity and adoption and maintaining privacy and control. Companies address compromised device issues on the organization side without accessing individual devices, reducing costs, and simplifying IT management.

Mobile device use and BYOD are mainstays in today's remote workforce, and your organization needs a secure, cost-efficient, user-friendly solution. If you're looking to implement enterprise-wide BYOD or recognize that your MDM solution is not addressing your business needs, it’s time for VMS. Your employees will love it, your IT department will thank you, and your enterprise will be safe.