How to choose the Right MDM solution

by Waqas Khan

Cloud and mobility have changed the way we work, and created an environment where employees want access to corporate applications and data at any time, from anywhere, from whatever device they choose. Organizations are increasingly realizing the power of a flexible mobile work environment, and in many ways, the COVID-19 pandemic has significantly accelerated the need for mobility. This assists employees in striking a balance between their professional and personal life, and helps companies establish a seamless communication between the field employees and base office.

However, enterprise mobility may lead to critical security concerns for business data, apps, and devices if not managed and secured efficiently. Thus, to meet the security challenges, enterprises need a powerful secured mobile device management (MDM) solution. An MDM solution monitors, secures, and controls the mobile devices used by the organization's employees. It allows access to corporate apps, data, and content under assured security.

Enterprise mobility involves challenges, and organizations are required to choose from several mobility solution providers in the market. Before choosing an MDM solution, companies should complete a thorough requirement and feasibility analysis. After the analysis, the company can prepare a comprehensive report of their pain points that will give them an informed position from which to choose an MDM solution. It is important to understand the pros and cons of any MDM solution before deciding if it is the best fit for your organization. To ensure enterprises choose the right MDM solution, there are important factors to be considered.

INTEGRATION

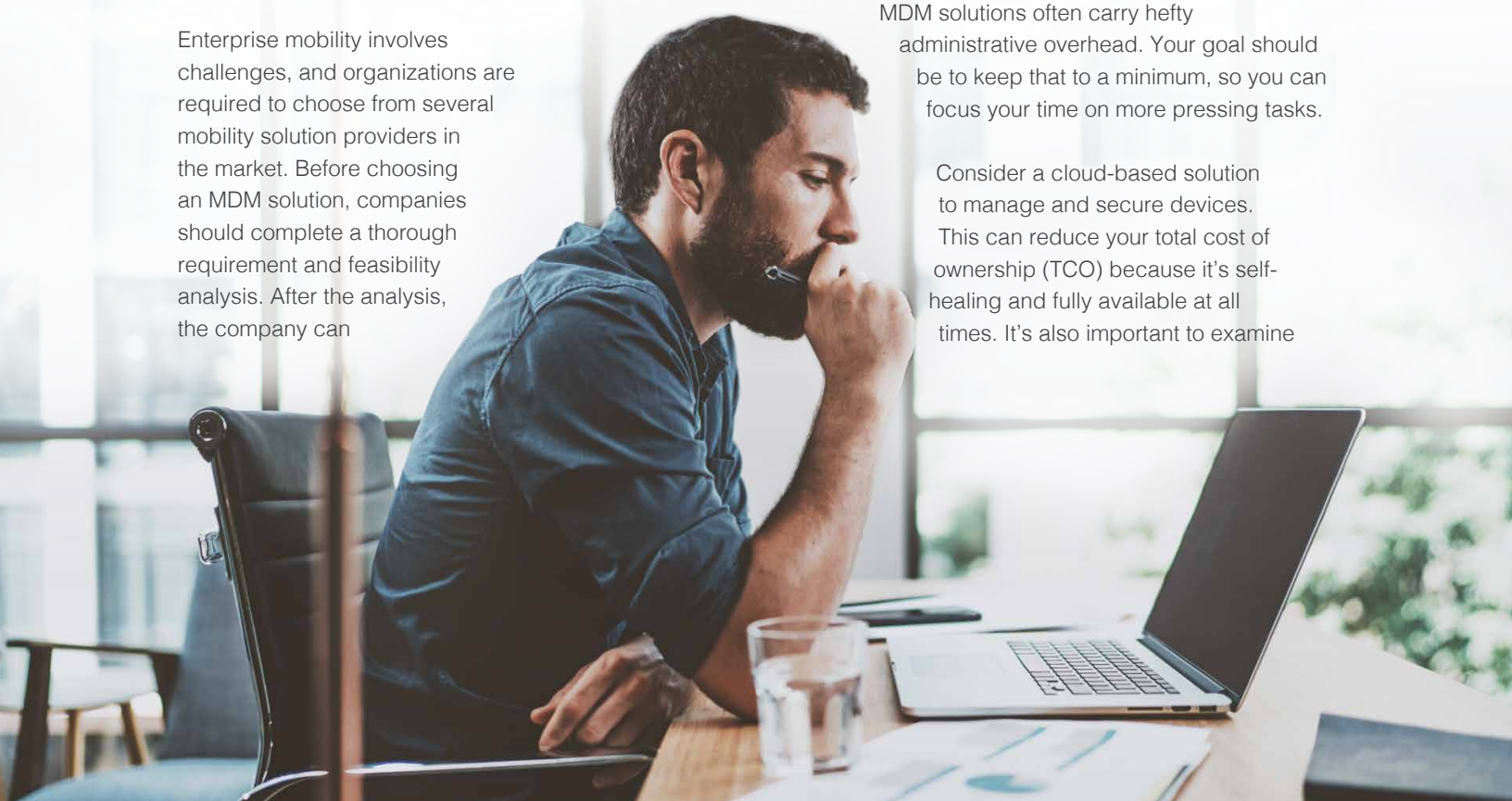
The smooth, painless integration of an MDM solution into your ecosystem is imperative to protecting existing technology investments and avoiding rip and replace. Most solutions provide options for on-premises, cloud-based or hybrid installation and integration. Integration with other management, support and reporting tools significantly adds to the overall service.

Consider a solution that integrates easily with existing device management tools and vendors to share information on device state.

ADMINISTRATION

MDM solutions often carry hefty administrative overhead. Your goal should be to keep that to a minimum, so you can focus your time on more pressing tasks.

Consider a cloud-based solution to manage and secure devices. This can reduce your total cost of ownership (TCO) because it's self-healing and fully available at all times. It's also important to examine



solutions through which you can manage access to applications based on user groups and individual roles and automate security patches and updates, further reducing your administrative overhead. With adequate acknowledgment of the risk that comes with data in the cloud, you'll save both time and money.

DEVICE AND DATA SECURITY

Organizations should be able to enforce security policies to reduce the risk of breaches and prevent vulnerable or unsecured devices from accessing sensitive data. Security policies are unique to each organization and you should be able to customize policies based on the risk associated with certain applications.

For example: is the device using passcodes and biometrics? Is encryption turned on? What OS and browser versions are installed and are they up to date, properly configured and patched? Device security status will help you detect and stop out-of-date and/or vulnerable devices from gaining access. It also only allows devices whose security posture conforms to the baselines established by the organization.

Consider a solution that provides insights into the security posture of all devices and empowers you to enforce security policies rather than prescribing them on paper to ensure adherence. That way you can set consistent policies across applications, whether on-premises or in the cloud, to deliver a seamless user experience.

USER EXPERIENCE

The process of enrolling devices in your chosen solution is often overlooked, but with an increased emphasis on user experience by all major platforms, it's important to evaluate the features and capabilities of the solution

Consider a solution that offers users flexible onboarding options like automated enrollment, self-enrollment and self-service for support. It eases the burden on administrators and promotes confidence in user base, without requiring additional training.

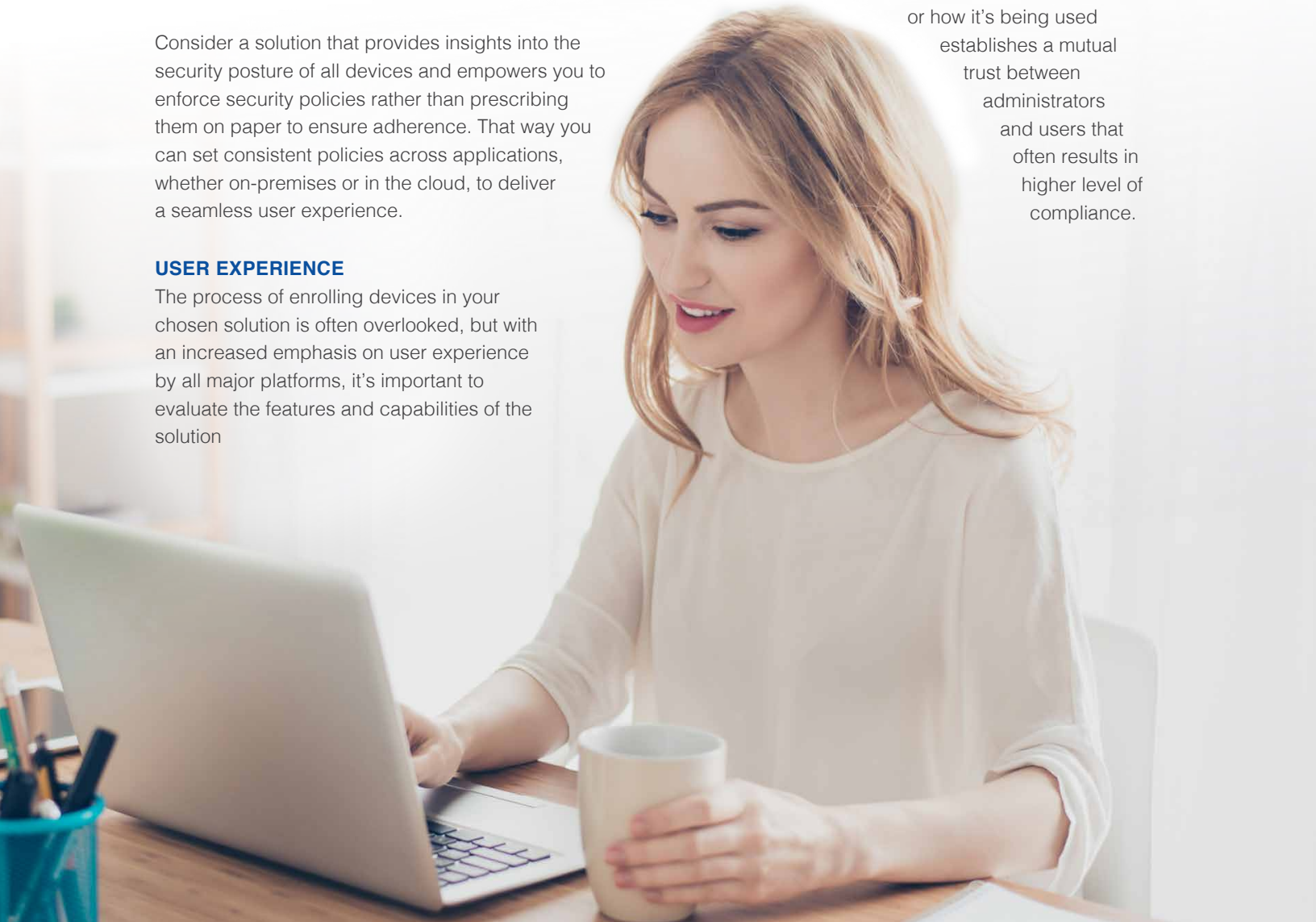
UNIFIED VISIBILITY

Most endpoint visibility solutions are siloed. They are often designed exclusively for Windows, Macs, or mobile devices. A solution specific to each platform results in a massive productivity drain and major administration headaches.

A solution offering a unified, comprehensive view from a single dashboard into all managed, unmanaged endpoints and platforms can streamline administration and reduce complexity.

TRANSPARENCY

Most MDM solutions are considered intrusive. Users fear their privacy may be invaded and they will lose control of certain features and functions of their devices. Keeping users informed about what information is being collected or how it's being used establishes a mutual trust between administrators and users that often results in higher level of compliance.



A transparent solution that only collects a device's security information is optimal. The less personal data collected, the better – and notify users what type of information will be collected and examined.

INVENTORY MANAGEMENT

Many MDM solutions lack the ability to provide a detailed device inventory. A device inventory gives you additional information and reduces the burden of device lifecycle management while also eliminating the surprise of unknown devices accessing your applications.

Consider a solution that enables you to identify all devices that access your environment and tag assets to specific users so that you can understand which device is assigned to whom, how many devices are being used, and which applications are being accessed.

COMPLIANCE AND REPORTING

Most organizations adhere to strict compliance regulations, such as HIPAA, PCI DSS, NIST, SOC 2, or ISO 27001 and require all devices to be compliant.

A good solution for your company might be one that enables you to generate user and device reports and security logs with just a few clicks to help meet compliance requirements for tracking and security event logging, as well as provides valuable assets for audits and incident response and recovery.

SERVICE AND SUPPORT

Support and after-sales services are the deciding factors for many organizations when evaluating and selecting new solutions and services. Many MDM solutions have varying tiers of support, depending on customers' requirements and needs.

Look for a solution that offers multiple tiers of support options for the type of devices you'll be managing. Thoroughly review and vet SLAs of every option along with support availability in different regions and languages.

ABOUT THE AUTHOR

Waqas Khan

Wipro Sr. Solutions Architect – Apple Device Services

Waqas is a System Engineer and Solutions Architect, specializing in integrating Apple devices in large multinational corporations. He has held similar positions in multiple organizations, promoting, creating, and delivering device as a choice programs in each of them. He's a member of Apple's Consultant Network and various other Apple-centric forums. He loves traveling, playing tennis and can talk DC and Marvel all day, everyday.

apple.experts@wipro.com

wipro.com/innovation/live-workspace-for-apple

About Wipro

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 180,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.