ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 14, Issue 3, pp: (65-68), Month: July – September 2026, Available at: www.researchpublish.com

Managing Mobile Devices in the Oil and Gas Sector: On-Premise vs Cloud

Mohammed Bin Jahlan[1], Mohammad Yagoub[2], Mohammed Alharthi[3]

Saudi Arabian Oil company, Dhahran, Kingdom of Saudi Arabia

DOI: https://doi.org/10.5281/zenodo.22079249

Published Date: 24-August-2026

Abstract: **As Oil & Gas organizational workforces become increasingly distributed and mobile, the management, security, and resilience of endpoint devices have become critical operational tools. Managing large-scale fleets, exceeding 30,000 mixed-use devices across corporate-owned, bring-your-own-device (BYOD), and intrinsically safe ruggedized endpoints which presents unique architectural and security challenges. This paper examines the paradigm of transitioning from on-premise Mobile Device Management (MDM), such as Omnissa Workspace One, to cloud-based MDM. Structured around three interconnected pillars, scalability, zero-trust security, and operational resilience, this analysis presents an objective case for both on-premise and cloud architectures. It explores the structural advantages of cloud elasticity and continuous posture evaluation, alongside the realities of technical debt, application migration, and the stringent data sovereignty requirements of the oil and gas sector. Rather than recommending a universal migration path, this paper provides a comparative framework to help organizations evaluate which deployment model best aligns with their operational, regulatory, and security needs.**

Keywords: **Cloud Computing, MDM, Information Security, Zero Trust, SaaS, Endpoint Management.**

I. INTRODUCTION

The proliferation of mobile devices in the enterprise has fundamentally altered the IT landscape. In large enterprises, IT departments routinely manage fleets exceeding 30,000 endpoints. These fleets are highly diverse, spanning standard consumer devices (iOS and Android) in corporate-owned and bring-your-own-device (BYOD) models, as well as specialized intrinsically safe (IS) devices designed for extreme conditions and hazardous environments [5].

Historically, Mobile Device Management (MDM) has been deployed via on-premise servers, requiring organizations to provision, maintain, and scale their own infrastructure. Platforms such as Omnissa Workspace One have provided robust, centralized management for these mixed fleets [2]. However, as device counts grow, executives become increasingly reliant on mobile devices for critical business functions, and cyber threats evolve, organizations are forced to evaluate whether traditional on-premise models can sustain the required scale, security, and availability.

The shift to cloud-based MDM represents a fundamental architectural alternative. This paper examines the case for both on-premise and cloud-based MDM, structured around three critical capabilities: elastic scalability to manage massive fleets, zero-trust security to protect corporate data in a perimeter-less world, and operational resilience to ensure continuous service availability. By presenting an objective comparative analysis, this paper aims to equip IT and security leaders with the framework to evaluate the business and technical case for cloud migration versus on-premise retention in their specific organizational contexts.

II. BACKGROUND

MDM as a software emerged in the early 2000s as it was required as businesses grew and along with number of mobile devices used by their employees. This field evolved greatly from simple mobile enrolment to comprehensive Unified Endpoint Management (UEM) platforms that manage mobile phones, tablet and computers. Market leaders such as Microsoft Intune and Omnissa Workspace ONE have all transformed their core offerings from on-premises to cloud-based (SaaS) or hybrid delivery models [1][2].

In large-scale environments managing tens of thousands of devices, MDM platforms must handle complex application delivery, certificate management, and conditional access policies. The complexity is compounded in sectors like oil and gas, where fleets include both standard executive smartphones and intrinsically safe devices deployed to field operators in hazardous zones. Traditionally, this required substantial on-premise infrastructure. Organizations deployed dedicated servers to communicate with devices via push notification services (e.g., Apple Push Notification service and Android Enterprise). While on-premise solutions like Omnissa Workspace One provide deep control and integration with legacy identity systems, they inherently scale linearly. Doubling the device fleet necessitates roughly doubling the server capacity, database storage, and network bandwidth. Furthermore, on-premise solutions require dedicated IT staff to manage server updates, database backups, and hardware failures, shifting focus away from strategic device security to infrastructure maintenance.

By shifting the burden of infrastructure management to the cloud provider, organizations can redirect their focus toward device security and policy enforcement. This shift aligns naturally with Zero Trust architectures, which operate on the principle that no device or user should be inherently trusted, regardless of network location. Previous research has highlighted the security benefits of this integration, as cloud-based MDM enables policy enforcement driven by device-level security attributes such as operating system patch levels, encryption status, and jailbreak detection, rather than relying solely on network-based controls. Consequently, security policies are applied consistently whether a device is connected to the corporate network, a corporate VPN, or a public network [3].

III. COMPARATIVE ANALYSIS: CLOUD VS. ON-PREMISES

The evaluation between on-premise and cloud-based MDM is not merely a choice of hosting location, but a fundamental trade-off between control, scalability, and operational expenditure. Cloud computing provides on-demand network access to a shared pool of configurable computing resources, enabling rapid provisioning with minimal management effort [6].

The following table shows a comparison between MDM on on-premises and Cloud:

TABLE I: ON-PREMISES VS. CLOUD-NATIVE MDM COMPARISON

Feature	On-Premises	Cloud-Native
Initial Investment	High (Hardware + Licenses)	Low (Subscription-based)
Maintenance	IT Team	Automatic (Vendor-managed)
Security Posture	Perimeter-dependent	Compatible with Zero Trust
Scalability	Limited by Server Capacity	Flexible
Updates	Periodic / Delayed	Real-time / Zero-day

The primary difference between On-Premises and Cloud-Native infrastructure lies in shift from ownership of the infrastructure to subscription-based agility. An On-Premises setup requires a high initial investment in hardware and a dedicated IT team for maintenance and periodic updates, with growth strictly limited by physical server capacity.

The widespread migration to the cloud is not surprising, as cloud services offer many advantages over on-premises data centers. One of the primary benefits of cloud computing is its scalability. Cloud services enable organizations to flexibly increase or decrease their computing resources according to business requirements. As a result, businesses can quickly adapt to changing demands without the need to invest in costly hardware and infrastructure [4]. For a fleet of 30,000 devices, this elasticity eliminates the need for capacity planning and hardware refresh cycles, though it introduces a dependency on external cloud infrastructure.

However, cost effectiveness is only part of the equation. For organizations in highly regulated sectors like oil and gas, data sovereignty is paramount. On-premise MDM guarantees that all device telemetry, user data, and corporate intelligence remain within the organization's physical boundaries, providing absolute assurance of privacy and control. Cloud MDM, by contrast, requires rigorous evaluation of the provider's data residency capabilities. In regions such as Saudi Arabia, the Personal Data Protection Law (PDPL) and National Cybersecurity Authority (NCA) Cloud Computing Controls mandate strict requirements for data localization and cross-border data transfer [7]. Executives evaluating cloud MDM require contractual and architectural insurance that telemetry and personal data will not traverse unauthorized jurisdictions.

IV. CORE PILLARS: SCALABILITY, ZERO TRUST, AND OPERATIONAL RESILIENCE

The evaluation of cloud versus on-premise MDM is best framed through three interdependent pillars: scalability, zero-trust security, and operational resilience.

A. Scalability: Managing Fleets at Cloud Scale

Scalability in MDM extends beyond raw device count to encompass policy complexity and application management. Cloud-native architectures utilize microservices and API-driven integration, allowing MDM platforms to interface seamlessly with Identity Providers (IdPs) and Security Information and Event Management (SIEM) systems. In a 30,000-device fleet with a mix of BYOD, corporate-owned, and intrinsically safe devices, the number of configuration profiles, compliance rules, and internally developed applications grows non-linearly. Cloud platforms handle complex policy evaluation at scale without the performance degradation seen in on-premise databases.

B. Zero-Trust Security in MDM

In the context of mobile devices, Zero Trust is particularly critical. Management and executives rely heavily on mobile devices while on the move, accessing sensitive corporate data from various networks and geographies. Both on-premise and cloud MDM platforms can implement real-time compliance checks, monitoring OS versions, encryption status, jailbreak/root detection, and security configurations. However, cloud MDM platforms often offer tighter, native integration with cloud-hosted IdPs to feed device posture directly into conditional access engines. If a device falls out of compliance, access to corporate resources is revoked in near real-time [3].

A significant challenge in zero-trust MDM is the friction between security features and user experience. Executives require seamless access to email, VPNs, and internal applications on their mobile devices. Overly aggressive conditional access policies, such as frequent step-up authentication or blocking access due to minor OS version delays, can frustrate users and impact business velocity. Cloud MDM platforms provide granular, adaptive access controls that factor in device context and user risk, attempting to balance security with usability [5]. On-premise solutions can achieve this through custom integrations, but often with greater development overhead.

C. Operational Resilience

Operational resilience in MDM requires maintaining service availability through disruptions and ensuring devices remain secure and functional even when disconnected from the management platform. Cloud MDM platforms inherit the resilience of their underlying cloud infrastructure. Leading providers deploy across multiple cloud regions with automated failover. This multi-region redundancy is backed by Service Level Agreements (SLAs) of 99.9% or higher, which are expensive and complex to replicate on-premise.

Resilience must also exist at the edge, particularly for intrinsically safe devices operating in extreme conditions such as offshore rigs, refineries, and remote desert fields. These devices often experience intermittent connectivity due to network isolation or harsh environmental factors. Devices cache their last-known compliance policies locally. If the MDM platform, whether cloud or on-premise, is unreachable, the device OS continues to enforce existing encryption, passcode, and Data Loss Prevention (DLP) policies. Grace periods prevent immediate non-compliance flags during transient network failures, preventing mass access revocation and ensuring field operators retain access to critical operational procedures.

V. CLOUD MIGRATION REALITIES

For organizations considering the transition from on-premise to cloud MDM, the migration process is often the most significant hurdle. Moving a fleet of 30,000+ devices is not a simple lift-and-shift operation; it involves substantial technical debt and integration efforts.

Legacy on-premise MDM deployments often accumulate years of custom configurations, complex profile hierarchies, and bespoke integrations with internal HR, ERP, and ITSM systems. Ensuring that these legacy systems are compatible with a new cloud MDM API architecture requires rigorous testing and re-engineering. Furthermore, in large enterprises, MDM is not just about device configuration; it is a primary channel for internal application distribution. Migrating 30,000 devices means re-packaging, re-signing, and redeploying hundreds of internal iOS and Android applications to the new cloud platform. This includes specialized operational applications deployed to intrinsically safe devices.

Though cloud deployment offers many advantages, there are many challenges associated with migrations to Cloud such as the complexity of full-scale migration that may require years to implement depending on the size of the organization. The skills required for cloud operations are different from on-premises. Cloud environments rely on new operating models like automation, infrastructure as code (IaC) and DevOps [4]. Migrations are typically executed in phases, running on-premise and cloud platforms in parallel. Device groups are migrated incrementally to avoid overwhelming the IT helpdesk. However, during this coexistence period, managing a hybrid environment increases operational complexity.

VI. CONCLUSION

The transition from on-premise to cloud-based Mobile Device Management presents a complex architectural and operational decision. On-premise solutions like Omnissa Workspace One provide deep control, absolute data sovereignty, and reliance on existing infrastructure investments, which are critical considerations for highly regulated sectors like oil and gas managing diverse fleets of standard and intrinsically safe devices. However, as fleets grow to tens of thousands of devices and executives demand seamless, secure access on the move, the elastic scalability, native zero-trust integrations, and multi-region operational resilience of cloud-based MDM present a compelling alternative.

This paper does not advocate a universal migration to the cloud, nor does it endorse the indefinite retention of on-premise infrastructure. Rather, it highlights that the business case for cloud MDM hinges on an organization's ability to overcome technical debt, ensure regulatory compliance regarding data sovereignty, and demonstrate cost effectiveness. Organizations must weigh the structural advantages of cloud architecture against the control and localized resilience of on-premise deployments, selecting the model that best aligns with their specific security posture, operational scale, and regulatory obligations.

REFERENCES

[1] Bitdefender. (n.d.). What is mobile device management (MDM). InfoZone. https://www.bitdefender.com/en-us/business/infozone/what-is-mobile-device-management-mdm

[2] Gordon, G., Lanusse, A., & Minihan, C. (2024, October 7). Workspace ONE UEM architecture. Omnissa Tech Zone. https://techzone.omnissa.com/resource/workspace-one-uem-architecture

[3] NIST, “Zero Trust Architecture,” NIST Special Publication 800-207, National Institute of Standards and Technology, 2020.

[4] Nar, F. E. (n.d.). Cloud vs. on-premises datacenters: How to choose for your workload. Red Hat. https://www.redhat.com/en/blog/cloud-vs-on-premises

[5] Souppaya, M., & Scarfone, K. (2013). Guidelines for managing the security of mobile devices in the enterprise (NIST Special Publication 800-124 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-124r1

[6] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (NIST Special Publication 800-145). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

[7] Saudi Data & Artificial Intelligence Authority (SDAIA). (2023). Personal Data Protection Law (PDPL). Royal Decree No. M/19. Riyadh, Saudi Arabia. https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf