UOT:002
DOİ: https://doi.org/10.30546/09090.2024.110.203

EVALUATING THE EFFECTIVENESS OF MICROSOFT INTUNE IN SECURING DEVICES: BALANCING SECURITY FEATURES AND USER EXPERIENCE IN ENTERPRISE ENVIRONMENTS

SAMUR AHMADOV

Azerbaijan Technical University

ARTICLE INFO

Article history:
Received: 2024-08-06
Received in revised form: 2024-09-12
Accepted: 2024-10-01
Available online

Keywords: Microsoft Intune;
Mobile device management;
Cloud security;
Enterprise mobility and security
JEL codes:
L86, O33, M15

ABSTRACT

Nearly every organization would like to adapt their environment to the cloud to increase productivity and decrease operational costs. By moving to the cloud, organizations are still struggling with enterprise mobile management systems. Managing devices can be challenging because of the complexity of the Microsoft ecosystem. However, Microsoft Intune is a service which was created to solve issues with managing devices and increase device security. This product can help to reduce potential security incidents within the organization and even during collaboration with other organizations.

The research employs a methodical approach where organizations utilize Microsoft Intune with its full capabilities and all available security configurations. This paper will examine Microsoft Intune's effectiveness in the matter of device management and security with different aspects.

1. Introduction

Users' device security is one of the significantly under-researched fields in Cloud Security. From the technical perspective, users can adapt to any changes within the organization. However, changes that were made previously need to provide a good user experience and not be overcomplicated. Consider a scenario where a device requires a BitLocker key, fingerprint, face recognition, and an additional password for sign-in. From a security perspective, it is a strongly secure way to have access to corporate devices and data. Users can find it frustrating and challenging to remember the BitLocker key and a strong password to type in every time users need to do their day-to-day tasks. This dichotomy between stringent security measures and user experience highlights a critical area for further investigation in device management.

More than 10 years ago, this topic was researched by Gustavo et al. [1], where researchers proposed a new security architecture for the mobile enterprise that uses network-based security and cloud computing. Other research was conducted in mobile device management by Song, X., & Yang, C.-H. [2]. They used the Android Open Source Project and SELinux to help enterprises manage and secure both corporate and bring-your-own-device (BYOD) mobile devices. The solution has options to track location, verify files, control permissions in real-time, and send informational push notifications. The system was developed using the Java programming language and tested on a customized Android 7.1.1 device.

Baltazar et al. [3] conducted research that underscores how Enterprise Information Systems (EIS) can be a key driver for improved and sustainable mobility. A case study was performed in one of the Portuguese companies for a carsharing platform. They also noted the significance of AI/ML for security.

Hasan et al. [4] presented a framework and guidelines for securing mobile enterprise applications. The framework includes a meta-model (UML diagram) that describes the framework components, a guidance model listing mobile security threats and countermeasures, and decision-making for logging security design decisions. The challenge of that framework could be with new threats and countermeasures and undefined or zero-day attacks. However, the proposed framework still supports enterprises in the decision-making process for mobile applications.

BYOD devices were discussed by Hina Batool [5], where the researcher discusses Mobile Device Management (MDM) systems for enterprises and partially for BYOD devices. The researcher identified major features of MDM such as profile management, location tracking, remote lock and wipe, malware detection, data backup and encryption, and URL blacklisting. The researcher reviewed MDM solutions such as AirWatch by VMware, IBM MaaS360, and Kaspersky Lab, and made a comparison. A comparison table was designed with Yes/No answers to security requirements. Almost all requirements were satisfied or partially satisfied by vendors. This research also doesn't cover the effectiveness of MDM in terms of security.

Another paper discussing the importance of developing strategies was written by Yucel [6]. The researcher used characterization of the mobile strategy based on different parameters such as objectives, users, mobile solution, mobile and backend platforms, benefits, drawbacks, risks and mitigation plans, strategies for distribution, launch, marketing, promotion and positioning, costs, etc. The generic model counts the rate of potential users and shows relationships between factors such as user adoption, benefits, economic utilities, and others. The idea of that research was increasing return on investment while receiving benefits from enterprise mobility.

Another field to study is mobile application management (MAM) for pushing applications through a centralized console. The MAM question was researched by Yamin, M. M., & Katt, B [7]. The research includes an introduction to MDM and its main functions, discussion of enabling protocols for MDM such as Smart Message, Open Mobile Alliance Device Management, and Over-The-Air Programming. MAM questions and challenges were also researched in different papers [8], [9].

Ana Maria Suduca and Mihai Bizoia [10] explored ways of integrating and pushing apps in the easiest way. Microsoft Intune was utilized to minimize application pushing effort. During the research, they pushed the videoconferencing application Zoom through Intune, which significantly reduced the amount of time required.

The majority of the researched articles use a similar research method – comparative analysis. In the modern world, comparing features is not sufficient for building a security fortress, especially for enterprises and government entities. Thus, this article will present a real test scenario with the proposed solution and highlight advantages for Security Operations Teams to quickly identify and address security issues.

2. Background

Microsoft Intune is Microsoft's cloud-based service that acts as an enterprise mobility management (EMM) and MDM solution. Microsoft Intune supports a diverse range of operating systems: Windows, macOS, Android, Linux, and iOS devices. There are several ways to accomplish the onboarding process for devices to Microsoft Intune: group-based, Autopilot, Apple Business Manager for iOS devices, and Android Enterprise for Android devices. Additionally, the user onboarding process can be performed automatically during the first sign-in with Windows credentials, or via the Company Portal application from the store for mobile devices. After the onboarding process, users will receive a set of policies that were configured in Microsoft's security portal and can receive new policy enforcements during subsequent policy update cycles. The high-level architecture of Microsoft Intune is given in the following figure.

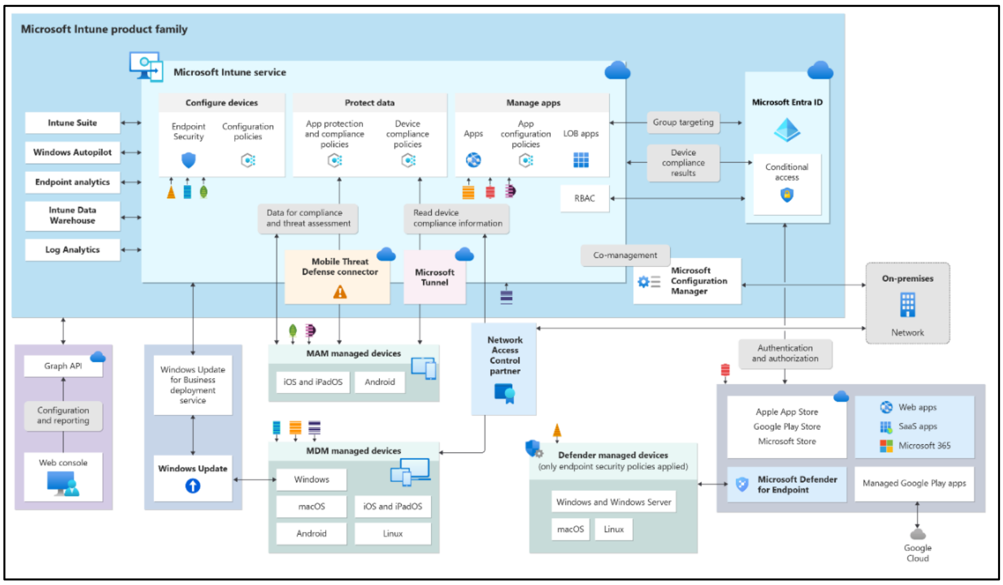

Fig. 1 High-level Microsoft Intune architecture

As shown in Fig. 1, the architecture consists of several components such as: Microsoft Intune service, Graph API, Windows Update for Business deployment service, MAM managed devices, Network Access Control partner, and Microsoft Configuration Manager for on-premises deployment. Moreover, the figure depicts Intune's integration with Microsoft Defender for Endpoint, a comprehensive security solution that functions as both an antivirus and endpoint detection and response suite. This integration underscores the security measures that can be implemented via Microsoft Defender for Endpoint within the Microsoft ecosystem.

3. Methodology

To evaluate the effectiveness of the solution, a structured approach is needed. The following figure shows the methodological steps.

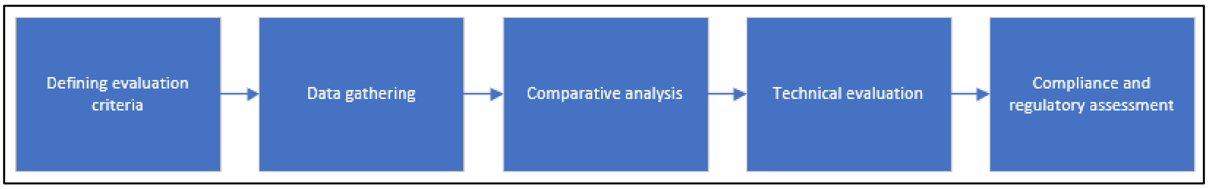
Defining evaluation criteria
Data gathering
Comparative analysis
Technical evaluation
Compliance and regulatory assessment

Fig. 2 Main steps to evaluate effectiveness of Microsoft Intune

These steps should be considered high-level steps that underscore the importance of Microsoft Intune and its capabilities across both Microsoft and non-Microsoft ecosystems

Defining evaluation criteria. This step includes several factors which should be evaluated during the usage of Microsoft Intune: device compliance rates, malware detection and prevention, remote wipe effectiveness, time to deploy security patches, time to update policies, app protection policy enforcement.

Microsoft Intune has compliance policies which can be defined in the portal. They are a set of rules and conditions that would be evaluated during the policy update timeframe. Malware detection and prevention criteria rely on Microsoft Defender for Endpoint system.

Data gathering. This step underscores the necessity of gathering important data for preventing attacks. For instance, an endpoint's IP address and agent status can be considered as data to understand the endpoint's current security status.

Comparative analysis. Microsoft Intune has many mechanisms in terms of configuration, policies, and integrations. Considering this, best practices will be used to build a secure ecosystem across the organization.

Technical evaluation. From a technical perspective, the solution should be scalable, adaptable for end users in terms of user experience, and easy to use for security administrators. This step will evaluate these parameters. The research was conducted in different environments that have varying compliance requirements and restriction levels.

Compliance and regulatory. Compliance ensures that this data is handled according to legal requirements and industry standards. There are global regulations, such as GDPR in the EU and HIPAA in US healthcare, as well as various industry-specific standards. Having compliance and regulation methods in place helps to quickly pass audits.

During this research, metrics will be used to calculate overall security posture and user experience. The following table contains information about metrics. Metrics were evaluated based on the security features, where 2 indicates the feature significantly affects user experience, 1 indicates the feature affects user experience, and 0 indicates the feature does not affect user experience.

Table 1
Parameters

Security features	User experience
Device encryption	Ease of enrollment
Multi-factor authentication	App accessibility
App protection policies	Performance impact
Conditional access	Privacy considerations
Data loss prevention	Self-service capabilities
Remote wipe capabilities	User interface intuitiveness
Compliance policies	Support and troubleshooting experience

4. Comparative Analysis of MDM Solutions

To provide context for Microsoft Intune's effectiveness, it's important to compare it with other major Mobile Device Management (MDM) solutions in the market. For this analysis, we'll compare Microsoft Intune with two other prominent solutions: VMware Workspace ONE (formerly AirWatch) and IBM MaaS360. Table 3 provides a high-level comparison of key features across the three MDM solutions:

Table 3

Feature Comparison of MDM Solutions

Feature	Microsoft Intune	VMware Workspace ONE	IBM MaaS360
Device enrollment	+	+	+
OS support	Windows, iOS, Android, macOS	Windows, iOS, Android, macOS, Linux	Windows, iOS, Android, macOS
App management	+	+	+
Device encryption	+	+	+
Remote wipe	+	+	+
Conditional access	+	+	+
Integration with identity managementt	Entra ID	VMware Identity Manager	IBM Cloud Identity
Threat defense integration	Microsoft Defender for Endpoint	VMware Carbon Black	IBM Trusteer
Unified endpoint management	+	+	+
Container-based separation	+	+	+

While Microsoft Intune, VMware Workspace ONE, and IBM MaaS360 all offer robust MDM capabilities, the choice between them often depends on an organization's existing IT infrastructure, specific security needs, and integration requirements.

5. Implementation and tests

Implementation and testing were performed in a test environment to ensure network isolation. To ensure data reliability, data were gathered from different types of organizations: financial institutions, accommodation businesses, hotels, and resorts.

Device encryption analysis. BitLocker provides full device encryption for Windows OS. Microsoft Intune allows creation of policies that ensure BitLocker is utilized across all devices. To perform encryption, security administrators can create a configuration profile in Intune. This setting can be implemented silently without user interaction, which significantly improves user experience.

Multi-factor authentication. The impact of multi-factor authentication (MFA) is significant in the modern world. MFA reduces almost 80% of attacks. Research conducted by Liu W. et al. [11] shows how MFA can be utilized not only in enterprises but also in the Internet of Things (IoT). While MFA reduces the risk of user credential theft, it adds an additional step during sign-in to the system. MFA can be performed in various ways: using push notifications, SMS, voice, or an authenticator app (code).

App protection policies. App protection policies (APP) are rules that ensure an organization's data remains safe or contained in managed apps. These policies protect company data at the app level. For instance, users can be required to enter a PIN to open an app in a work container, can have limited sharing options between apps, and cannot save company data in personal storage. These settings can reduce user-experience and require additional step for accessing company data.

Conditional access. Conditional access is a solution that works like an if-then statement. If the requirements are met, then access will be granted, blocked, or monitored. Microsoft Intune has an option called "device state". Device state can be compliant, non-compliant, or in a grace period, depending on the compliance policies. By using this parameter, entities can block access to high-level applications by requiring devices to be marked as compliant in the Intune portal. Conditional access policies have impact on the user-experience.

Data Loss Prevention. With profile isolation on mobile devices, Intune can use data loss prevention mechanisms. For example, with the help of mobile application management policies, users are unable to copy data from the work profile to personal profiles. It is also possible to enable redirection to company internal resources during searches in the Microsoft Edge web browser. These policies have impact on the user-experience.

Remote wipe capabilities. Wiping devices can be critically necessary when an employee is terminated or when a device is stolen. Based on the tests, remote wipe will take effect in less than one minute for Android devices and almost immediately for iOS devices. There are also different scenarios, such as when an organization buys corporate phones for workers and the devices need to be reassigned to other employees or departments. Other scenarios could include decommissioning old devices or providing access to contractors who will have only limited access to company applications to perform their jobs.

Compliance policies. Every organization has its own local policies and processes. Users should adhere to the principles and processes that were established previously and remain compliant while working with company data. Considering this, compliance policies have a significant impact on user experience.

During the research, all the mentioned parameters were evaluated. After testing on 650 devices, the statistical analysis mentioned earlier could be performed. Evaluating based on features alone is not enough; however, where security features and user experience have intersection points, statistical analysis can be performed. This analysis consists of all mentioned security features and user experience metrics. To gather information, a survey was conducted among users from different organizations. Based on the answers and the results of tests inside the laboratory environment, Table 3 was created.

The following table illustrates scoring based on different parameters across different organizations.

Table 3
Survey results

Security features	Ease of enrollment	App accessib ility	Perfor-mance	Privacy	Self-service capabilities	User interface intuitiveness	Sup port
Device encryption	1	0	1	0	0	1	1
Multi-factor authentication	1	1	2	2	2	2	1
App protection policies	0	1	1	1	0	1	1
Conditional access	2	1	2	1	0	1	1
Data loss prevention	1	1	2	2	0	1	1
Remote wipe capabilities	2	2	0	2	0	0	2
Compliance policies	2	2	1	2	0	1	2

This table could be used to evaluate the trade-offs between security features and user experience, helping to make informed decisions about which features to implement based on organizational priorities and the impact on various aspects of system use and management.

For each security feature, mean, median, and standard deviation were used. Considering that a number of coefficients are 7 and middle value could be used without averaging two middle numbers, median was used to determine standard deviation. Standard deviation helps quantify how consistently each security feature impacts different aspects of user experience. A low standard deviation indicates that a feature has a similar impact across various user experience factors, while a high standard deviation suggests the impact varies widely. The following formulas show the calculations for mean and standard deviation.

$$\mu = (\sum X)/n, \qquad (1)$$

where μ – mean, x – each value in dataset, n – number of values

$$\sigma = \sqrt{[\sum(x - \mu)^2/N]} \qquad (2)$$

where σ – standard deviation, μ – mean, x – each value in dataset, n – number of values

Table 4
Statistical Analysis of Survey Results

Security Feature	Mean	Median	Standard Deviation
Device encryption	0.57	1	0.53
MFA	1.57	2	0.53
APP	0.71	1	0.49
Conditional access	1.14	1	0.69
DLP	1.14	1	0.69
Remote wipe	1.14	2	1.07
Compliance policies	1.43	2	0.79

Statistical analysis of the survey results reveals interesting patterns in the impact of security features on user experience. Device encryption had the lowest mean impact (0.57), suggesting it's generally well-tolerated by users. In contrast, multi-factor authentication showed the highest mean impact (1.57), indicating it's perceived as more disruptive to the user experience. The following chart illustrates the mean, median, and standard deviation of the impact each security feature has on user experience. Higher values for mean and median indicate a greater impact on user experience, while higher standard deviation suggests more variability in how the feature affects different aspects of user experience

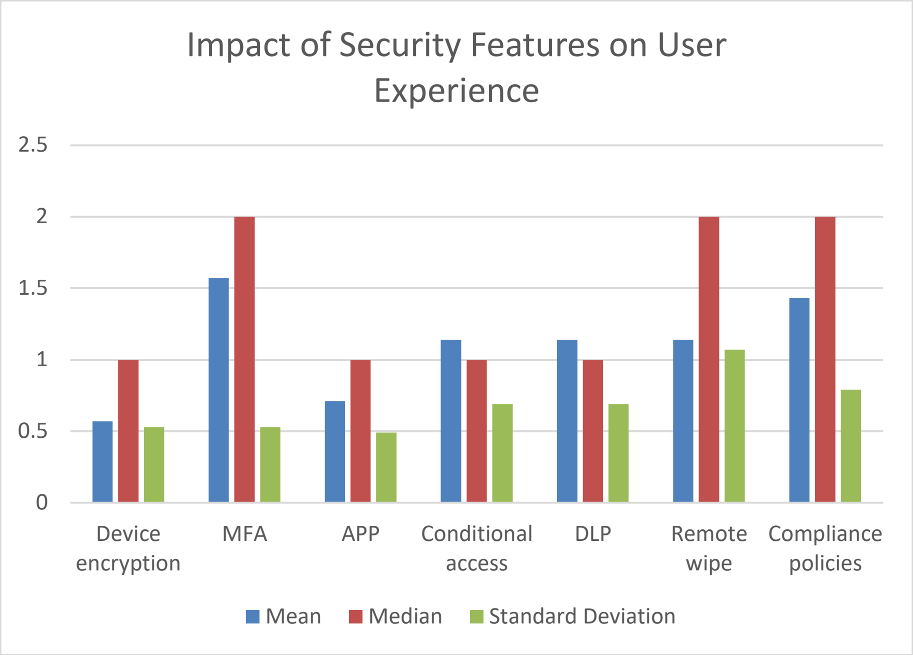

Fig. 3 Impact of Security Features on User Experience

The Fig.3 shows trade-off in a graphical way to easier to understand and compare security features and their impact on user experience. It helps identify features that might have extreme impacts in certain areas, which could be masked by looking at averages alone. Including standard deviation adds statistical rigor to your analysis, demonstrating a more thorough examination of the data beyond simple averages.

6. Conclusion

This research has conducted a comprehensive evaluation of Microsoft Intune's effectiveness in securing devices within enterprise environments, with a particular focus on the delicate balance between robust security features and user experience. Through a structured methodology of evaluation criteria definition, data gathering, comparative analysis, technical evaluation, and compliance considerations, valuable insights were obtained regarding Intune's capabilities.

The findings indicate that Microsoft Intune offers a set of features for device management, security, and integration between the two. To ensure device security, the following features were researched: device encryption, multi-factor authentication, app protection policies, conditional access, data loss prevention, remote wipe capabilities, and compliance policies. Each of these features contributes significantly to enhancing the organization's security posture.

The trade-off analysis between security features and user experience revealed that while some security measures like device encryption have minimal impact on usability, others such as multi-factor authentication and conditional access policies can significantly affect the user experience. This highlights the need for organizations to carefully balance security requirements with usability considerations when implementing Intune.

Research across different types of organizations, including financial institutions and hospitality businesses, demonstrated that Intune's effectiveness can vary depending on the specific needs and constraints of each sector. However, overall, Intune proved to be a versatile and powerful tool for managing and securing diverse device ecosystems.

While Intune demonstrates strong capabilities in device management and security, it is important to note that no single solution can address all security challenges. Organizations should view Intune as a critical component of a broader, layered security strategy that includes other measures such as regular security training for employees, network security solutions, and continuous monitoring and improvement of security practices.

In conclusion, Microsoft Intune proves to be an effective solution for securing devices in modern organizational environments. Its comprehensive feature set, coupled with its ability to balance security needs with user experience considerations, makes it a valuable tool for organizations seeking to enhance their mobile device management and security capabilities. However, successful implementation requires careful planning, ongoing management, and a clear understanding of the organization's specific security needs and user requirements.

Reference list

1. De los Reyes, G., Macwan, S., Chawla, D., & Serban, C. (2012). Securing the mobile enterprise with network-based security and cloud computing. 35th IEEE Sarnoff Symposium.
2. Song, X., & Yang, C.-H. (2017). Mobile Device Management System Based on AOSP and SELinux. IEEE Second International Conference on Data Science in Cyberspace (DSC).
3. Baltazar, S., Barreto, L., Amaral, A., & Pereira, T. (2020). Enterprise Information Systems (EIS) as a key driver towards improved mobility. 2020 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC).
4. Hasan, B., Dmitriyev, V., Gomez, J. M., & Kurzhofer, J. (2014). A framework along with guidelines for designing secure mobile enterprise applications. 2014 International Carnahan Conference on Security Technology (ICCST).
5. Batool, H., & Masood, A. (2020). Enterprise Mobile Device Management Requirements and Features. IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS).
6. Yucel, S. (2017). Evaluating Enterprise Mobility Strategy. 2017 International Conference on Computational Science and Computational Intelligence (CSCI).
7. Yamin, M. M., & Katt, B. (2019). Mobile device management (MDM) technologies, issues and challenges. Proceedings of the 3rd International Conference on Cryptography, Security and Privacy - ICCSP '19.
8. Raj Kumar Koneru, Pattabhi Rama Rao Dasari, Prajakt Deshpande, Vivek Iyer, Rajendra Komandur, Aravind Perumal, Sriram Ramanathan, Matthew Terry, Vamsi Krishna Vagvala, Sathyanarayana Vennapusala, et al. (2016). Mobile application management systems and methods thereof. US Patent 9,405,723.
9. Murali Krishna Medudula, Mahim Sagar, and Ravi Parkash Gandhi (2016). Mobile Device: Applications, Over the Top Services, Identity Protection and BYOD Policy. In Telecom Management in Emerging Economies. Springer, 207–227.
10. Ana Maria Suduca, Mihai Bizoia (2022). AI shapes the future of web conferencing platforms. 9th International Conference on Information Technology and Quantitative Management.
11. Liu, W., Wang, X., & Peng, W. (2019). Secure Remote Multi-Factor Authentication Scheme Based on Chaotic Map Zero-knowledge proof for Crowdsourcing Internet of Things. IEEE Access, 1–1.