WHITE PAPER

USING MICROSOFT INTUNE FOR DEVICE MANAGEMENT: BENEFITS AND LIMITATIONS

BlueFletch

OVERVIEW

From the warehouse to the IT department, employees depend on their devices to find success in the workplace. These devices are only as strong as their endpoint managers and rely on UEMs (Unified Endpoint Manager) that integrate with existing tools. An organization needs to consider which UEM works best for its dedicated devices to run an efficient workplace. For companies subscribed to Microsoft's Application suite, their Endpoint Manager (formerly InTune) may be the best fit.

This whitepaper provides an Android-focused viewpoint of Microsoft's Endpoint Manager, including considerations for using it as a UEM. Before switching, we'll break down every crucial aspect of Endpoint an organization needs to know.

BACKGROUND

What is a UEM?
Unified Endpoint Manager brings all dashboards onto one single screen. In the industry, this is known as a single pane of glass, allowing organizations to configure, manage and secure endpoint devices (e.g., laptops, tablets, and handheld devices). UEMs enable companies to enforce security standards and ensure software installation. As well as set network configurations to prevent WiFi password sharing. UEMs also allow organizations to keep users from altering device settings. All this and more is done via a UEM, acting as the device owner.

What does Microsoft offer?
Microsoft offers Endpoint Manager (formerly Intune) for managing Windows, Apple, and Android devices. Existing Microsoft 365 subscriptions can add licenses, but not every device/user requires an individual license.

What other options are available?
Compared to other UEMs, Endpoint Manager costs less but isn't as feature-rich or mature. Companies usually migrate to InTune to reduce device management spending and integrate with their existing O365 and Active Directory accounts.

INTUNE-ENDPOINT MANAGER: BENEFITS/UNIQUE OFFERINGS

As part of the Microsoft ecosystem, many benefits come with consolidating existing platforms and vendors. If an organization is already paying for Microsoft's services, InTune is an ideal fit from both a cost and user experience perspective.

Lower License Price

Microsoft's license cost is lower than other UEMs, especially with an existing Microsoft subscription. But prices ultimately depend on a company's size. Organizations with a Microsoft

365 Enterprise License may be able to access Endpoint Manager at no additional cost.

Microsoft's price point may be budget-friendly. Organizations with a Microsoft 365 Enterprise License may be able to access Endpoint Manager at no additional cost.

- Organizations can easily add the S3 or S5 Enterprise Mobility + Security package to an existing subscription. This solution is simple and cost-effective, but purchasing standalone access is just as easy without a subscription.
- A single user can cost as little as $6/year and enroll an unlimited number of dedicated devices (i.e., shared and kiosk).
- If the workplace uses a bring your own device (BYOD) model or corporate-owned, personally enabled (COPE) model, they must add a separate subscription for each user.

BlueFletch

Integration with Microsoft Applications

Endpoint Manager integrates seamlessly with Office 365 applications and other Microsoft products. Organizations already leveraging Microsoft tools will find Endpoint provides a familiar user experience. InTune is a single portal that allows companies to manage all their devices. For workplaces using Microsoft's tools and devices, the relationship built with Microsoft's ecosystem over the years is a significant reason why InTune could be the right choice. Employees familiar with Microsoft will find the transition to InTune easy. Additionally, implementing Microsoft integrations could be a natural evolution for employees to move from workstations and desktops to mobility.

Here are some examples of Microsoft integrations:

Azure Active Directory (AD)
Azure Active Directory is an identity management software that works seamlessly alongside InTune. Organizations that use Azure will find their users' accounts ready for access and assignments. Features include self-service password reset, group membership, and machine learning-based security. End-users should know their AD account credentials.

Microsoft Authenticator
Microsoft's 2FA app can easily be deployed and preconfigured. For organizations using a shared device model, Endpoint Manager is currently the only EMM that can preconfigure Authenticator to operate in a shared mode for Android and provide SSO to Teams. More apps will be added and supported in the future.

Office 365 Apps
Like other EMMs, Office 365 can be assigned and set up with Managed Configs from the Play Store. But a unique offering is the option to deploy them as a "built-in app" and customize the name and icon while automating the licensing of tools like Word and Excel.

UEM

Though this whitepaper focuses on Android, Endpoint Manager is a true Unified Management tool supporting Windows, Apple, and Android. iPhones, Macs, Windows, and Android devices alike can utilize InTune. It can be an organization's single tool for device management across all their dedicated devices.

Hosted in Azure, Endpoint Manager is a cloud-based solution without an option for on-prem hosting. Many other UEMs have an on-prem option, but we recommend the cloud-hosted version of UEMs/EMMs. There is no need to rotate between management solutions as InTune is a single platform that oversees all devices.

INTUNE-ENDPOINT MANAGER: LIMITATIONS

No UEM is without limitations, and organizations must be aware of the shortcomings to prepare for future workarounds.

Newer Product on the Market

Endpoint Manager is a relatively new solution with lots of features still in development. Microsoft is transparent about what's upcoming via their docs, but being an early adopter may not be worth the low license cost. Especially for organizations that rely on management features not currently supported by InTune. Endpoint is Android Enterprise Recommended, yet it lacks some richer features available in competitors' products.

In the latest Gartner UEM Magic Quadrant Report, Gartner writes that Microsoft is often held back by the complexity of its software, "Despite increased investment in Microsoft Learn courses, quick start guides, how-to videos, and more-prescriptive guidance, feedback collected during client interactions reveals clients still struggle to keep pace with changes.

They also underestimate the overhead required to operate Configuration Manager and integrate it with Intune, Azure AD, and on-premises AD. Those that migrated from other client management tools (CMTs) are also frustrated with the lack of third-party application patching capabilities that require a third-party solution."

Separate License for Remote Control

Remote Control is an invaluable tool for IT and Help Desk teams supporting large device deployments. This feature allows device managers to connect to and take control of devices in the organization, allowing for streamlined service when resolving issues.

Microsoft resells TeamViewer for remote control on handheld devices, but it's a separate license and considerably more expensive than Endpoint Manager. Windows PCs have remote control capabilities as well. Purchasing a separate remote control software may not be ideal for organizations depending on this technology.

Analytics and Compliance Reporting in Intune

Endpoint Manager's primary use cases are creating Android policies, approving apps, and assigning them to devices. The latency in compliance reporting and a lack of analytics data is a pitfall to consider. Device enrollment can take more than 10 minutes as app assignments show stale data.

In-depth device analytics give administrators a better way to troubleshoot and resolve potential issues. Without analytics, potentially dangerous threats could compromise the integrity of a company's most sensitive data. Operations teams depend on application utilization insight as it helps determine how to best focus efforts and resources in the future.

Pushing Files to Android Devices

The last limitation that is sure to give pause to many organizations is the lack of file manipulation on Android devices. Do applications have an external configuration file? Are there custom certificates that need installation? Does an organization's datawedge profile scan different barcodes? Endpoint Manager will require alternative strategies if an organization says yes to any of these questions.

FILLING THE GAPS WITH A SECURITY MANAGEMENT PLATFORM

Many companies rely heavily on their EMS solutions to run their workplace. Switching to a UEM that does not support every aspect of a device management routine may be a step backward. But considering the cost of InTune and the convenience of using a Microsoft integrated UEM, it may still be a viable option. So how can they fill in the gaps? Well, enterprise installers and launchers may provide a better solution.

A Security Management platform such as BlueFletch Enterprise can function with Endpoint Manager to supplement the UEM and provide more admin control, better end-user experience, and richer analytics for Android enrollment.

In fact, BlueFletch supplements any UEM/EMM that might lack features. Below is a highlight of features that may enhance Microsoft Intune/Endpoint Manager to make it more robust:

File deployment/installer (e.g., step-by-step plays)
BlueFletch Enterprise can coexist with Microsoft Intune and provide complete application and file management control as a MDM. If an organization needs to push a configuration file, a certificate, or trigger an Android intent, they can.

BlueFletch also supports sending Honeywell and Zebra XML without going through the cumbersome process of setting up Managed Configs for these OEM Config applications from the Google Play Store.

BlueFletch

Remote Control
BlueFletch allows for full view and control of a user's handheld, with the ability to execute advanced commands (e.g., reboots and file control) without the additional TeamView licenses. BlueFletch doesn't require the end-user to accept any prompt to allow screen share - it's completely automated!

Enterprise Launcher for a better end-user experience on devices.
Microsoft offers a basic home screen replacement for Android devices. While this may suffice for kiosks or single-use devices, it's a limited feature set for end users.

BlueFletch Enterprise Launcher presents a customized user interface to each user depending on their role, complete single sign-on (SSO) to their applications, and security controls to protect corporate property and data.

BlueFletch Enterprise Launcher also has site awareness based on network IP addresses or GPS data to customize and localize the home screen, all with one standard configuration across the enterprise.

The BlueFletch role-based access is another feature that will excite UEM/EMM admins. When a user logs into Azure AD, BlueFletch will capture the AD groups and roles within the organization and provide access to only the applications appropriate for that job role.

Admins can push all applications to all devices (and not worry about deployment groups) while leaving BlueFletch Launcher to handle access privileges dynamically.

SUMMARY

As a Unified Endpoint Manager (UEM), Microsoft InTune gives organizations the power to deploy, configure, and secure all endpoint devices. Some prominent tools include access to device analytics and remote control capabilities.

Since InTune is unified, it will operate on devices from various manufacturers. This list includes Apple, Samsung, Honeywell, Zebra, and more. InTune also integrates seamlessly into workplaces that have an existing Microsoft subscription.

This may be a cheaper alternative to some of the other solutions on the market. And if a company is paying for Microsoft services already, InTune may be the most cost-effective option.

Among its list of featured tools, here are a few standout InTune features:

- Seamless integration with Microsoft Applications
- Remote Control capabilities
- Access to device analytics
- Compatibility with devices from different manufacturers

InTune's library of features makes it easy to take advantage of new benefits. But if a company is considering InTune to manage enterprise endpoint devices, they must consider all other angles.

The cheaper price tag may be a significant factor in switching to InTune. But this comes with losing other tools that may be essential to different work environments. Microsoft is still working on providing other integrations an organization may need. As it stands now, switching to InTune might mean losing essential features from other UEMs.

An additional security management layer for mixed device environments is needed, especially with Android devices. No solution is perfect, and it's crucial to consider the needs and wants of a company before investing.

Test Intune/Endpoint Manager and find where the UEM fits into your company. InTune is excellent when matched with proper use cases. However, there are still many limitations to consider before switching. Some organizations may have requirements not covered in this whitepaper, so it's essential to understand your company's needs.

BlueFletch

ABOUT BLUEFLETCH

Based in Atlanta, BlueFletch is an award-winning innovator in the mobile industry, focused on helping enterprises secure, manage, and support their shared and rugged workforce devices.

The flagship product BlueFletch Enterprise is trusted by the Fortune 1000 in retail, transportation, healthcare, logistics, and warehousing, as well as organizations worldwide.

Providing a customized launcher, SSO, Support and Analytics, and MDM/EMM for Android workforce devices, BlueFletch Enterprise helps ensure an organization's digital transformation or management initiatives are effective and secure.

Learn more at https://www.bluefletch.com

BlueFletch