WHITE PAPER

# 4 BENEFITS FROM ENHANCING MOBILE DEVICE MANAGEMENT WITH BLUEFLETCH ENTERPRISE

BlueFletch

## The Emergence of Mobile Device Management (MDM)

As of 2021, there are an estimated 6.37 billion smartphones worldwide; that's nearly as many devices as people on the planet. As a result, mobile devices have found their way into every facet of life. With more and more functionalities and unique applications, devices have become significant not only for personal use and business.

Emerging in the early 2000s alongside the rise of consumer-grade mobile devices, Mobile Device Management (MDM) software has become the premiere solution for managing shared devices. The launch of early Android smartphones piqued interest in using mobile devices in the workplace. Today many enterprises across the globe utilize fleets of Android devices in shared environments. Whether for day-to-day tasks in the warehouse or customer service on the floor, company-owned devices can be helpful.

Enterprises caught on to the growing list of benefits associated with deploying company-owned mobile devices, including improved performance, productivity, and efficiency amongst end-users. Thus many organizations revolve their business strategies around these devices. However, a significant issue arose around the security of shared devices; how could an organization manage an entire fleet?

As many organizations expand their mobile device use cases, the need to protect devices from outside threats grows. This is where MDMs come into play.

MDMs offer a wide range of management features that allow organizations to take control of their device fleets. Said benefits include, but are not limited to:

- **Secure Password Requirements**
- **Device and Application Access Control**
- **Remote Lockdown**
- **Advanced-Data Analytics**

These functions, among others, have continued to refine as the years go by. And now, having an MDM is essential in any environment when deploying a workforce device fleet.

## The Current State of MDM Providers

There is a healthy amount of competition between different MDMs in the mobile management space. Enterprises and industries are continuously evolving and looking forward to new technologies. And with the evolution of positive growth also comes new threats. Organizations need assurance from their MDMs that a single solution can grow with the needs of their workforce.

There are now hundreds of MDM solutions in the market, each company boasting its own toolset and unique features.

Existing MDMs include but are not limited to:

- **SOTI**
- **Airwatch Workspace One**
- **Microsoft Intune**
- **Avalanche**
- **42Gears**

Selecting the right MDM can be a headache for an organization with little to no knowledge of device security. Every IT department and management team must weigh the needs of their device fleet against the provided functionality of existing MDMs. This decision is made carefully and precisely as organizations aim to protect the integrity of their sensitive data.

## What To Consider When Selecting An MDM

When selecting an MDM, an organization needs to note a few things.

- **Survey End-Users**
  - The employees who handle rugged devices daily know what's working and what's not. When considering an MDM, ask the right questions and see what the workforce relies on.
- **Build an End Goal**
  - Before diving into a new solution, an organization should map out where this MDM fits into its

BlueFletch

security landscape. If there are conflicting features already present in the environment, assess them. Be sure that the selected MDM will be a welcomed security component.

- **Assess Costs**
  - Additionally, organizations must be cautious about overspending. Some solutions may host a variety of features, but not all of which benefit a given organization. Each workplace is unique, and to avoid spending money on features that will go unused, assess the cost breakdown of each MDM.

## Introducing BlueFletch Enterprise

BlueFletch Enterprise provides security features that compete with popular MDMs and work on top of them. BlueFletch is not an MDM nor a replacement for organizations already leveraging an existing MDM. All of the BlueFletch tools are available to run alongside whatever MDM an organization uses, making it easy to bring more power to the workplace.

The cost to run both may seem unnecessary to organizations looking to minimize security expenses. This hesitation is justifiable as the licensing cost of some popular MDMs is enough to run an entire management budget. Also, management teams may feel comfortable with the current MDM solution. The features, UI, and associated tools become second nature over time. But it's important to understand that BlueFletch is not a replacement; it's an enhancement.

BlueFletch Enterprise is a set of security management tools focused on Shared Android workforce device fleets. This platform increases end-user productivity and provides exceptional security at a reduced support cost. BlueFletch tools such as Single Sign-On (SSO), Chat, and Launcher offer advantageous benefits without sacrificing existing MDM tools.

**Why Choose BlueFletch**

95% of BlueFletch customers utilize BlueFletch on top of their existing MDM system. BlueFletch Enterprise explicitly designed for such scenarios. BlueFletch enhances existing MDMs, giving a dynamic experience to an integrated toolset and simple solution to fill any gaps in a workplace's shared device security. This means no switching systems and no hassle trying to transfer company data and information. BlueFletch Enterprise augments shared devices without eradicating existing toolsets, and functionalities are available to various organizations and device fleets.

***The BlueFletch Enterprise Launcher***

The core component is the BlueFletch Enterprise Launcher, which controls the user experience while offering plugins and modules for security, user experience, and device control.

The BlueFletch Launcher is an Android home screen replacement that controls the user experience and device settings across a fleet of devices. This highly customizable launcher allows organizations to manage user permissions, device applications, layout, and more. All while providing a seamless login experience with Single-Sign-On (SSO).

With the BlueFletch Launcher, organizations can:

- **Provide a frictionless login experience with SSO**
- **Manage user permissions and application access**
- **Customize the device layout**
- **Delegate roles and user groups**
- **Access device analytics and performance data**
- **Keep devices safe with the device finder feature**

The Launcher integrates with all major Identity providers, making it easy to tie into existing systems without the need to replace or restart.

## Four Benefits from Enhancing MDM with BlueFletch

This whitepaper covers the four key reasons why adding BlueFletch to enhance an existing MDM benefits enterprise organizations.

## 1. Login and SSO

### *Easy Integrations*

Right out of the box, BlueFletch comes stock with features like Single Sign-on (SSO), Facial recognition, NFC badge tap, and other seamless authentication methods to create a frictionless login experience. BlueFletch has a much more detailed and flexible login solution than what SOTI, Airwatch, and Intune provide. However, BlueFletch is not an MDM and is not trying to take over user management. Instead, BlueFletch aims to provide the best possible login experience for end-users.

Additionally, the BlueFletch login functionality is customizable, allowing an organization to create role-based access for users across the enterprise. A company can slip its existing company hierarchy into the login feature or create new ones. These features help curate a truly shared device environment to allow all verified users to interact with a customized user experience.

The BlueFletch software is flexible and works across a plethora of existing identity providers (IdPs). An organization can leverage its current IdP without additional overhead and plug BlueFletch tools into what they already have. The BlueFletch system easily integrates into existing environments without disrupting the current tools.

### *Single sign-on*

The cornerstone of the BlueFletch login solution is reducing login friction with Single sign-on (SSO).

SSO is a security feature that enables organizations to manage resource and application access across their network. Organizations can delegate individual users and role-based groups access to specific sets of applications. Once authorized, all it takes is one set of credentials for a user to use their apps. Users seamlessly alternate between these approved applications and web pages without re-authenticating. SSO reduces login stress and time to create a more productive work environment.

### *Reduced Login Time*

Password fatigue is a growing issue among enterprises that require users to access multiple applications. Without SSO, users must reenter their unique credentials when rotating between apps. Login takes an average of 42.3 seconds, and when multiplied across a subset of apps, this lost time eats away at a user’s productivity. Since every application requires a complex, unique password, users are more likely to forget or misplace it. This creates a frustrating work atmosphere when users waste time at the helpdesk.

SSO cuts login time down to 2 seconds by only requiring a single set of credentials. Once SSO authenticates a user, they’re part of an authorized, active session while they use the device. Upon logging out, this session expires and entirely cuts off the device’s access. Enhancing the level of security among shared devices by reducing time wasted logging in, forgotten passwords, and possible unauthorized entry.

SSO also supports alternative authentication methods. This fast re-authentication is compatible with facial recognition, NFC badge taps, Multi-Factor Authentication (MFA), and FIDO2 keys.

### *Tangible Returns with SSO*

Lost and forgotten passwords burden the end user and an organization’s support costs. BlueFletch concludes that organizations can save $871 per device (per year) when using BlueFletch’s SSO features. Over the years, these savings can accumulate as more device fleets adopt SSO as a standard login security protocol.

## 2. Improved Security Posture

BlueFletch works to improve the security posture of shared Android devices by clearing application and user data upon logging out, enforcing access policies defined by the organization, and running inside the four walls. BlueFletch keeps user/application data safe, always protecting the privacy of the individual and the organization.

Since BlueFletch allows organizations to set their own security policies, BlueFletch creates an environment built upon the foundation defined by the enterprise. BlueFletch never changes access policies and only allows authorized organizational members to make necessary changes. This is just another way in which BlueFletch Enterprise works to protect the needs of an organization.

***Device Accountability and Tracking***

Lost and stolen devices plague the enterprise, as replacing devices or losing sensitive data can be costly. Device accountability ensures devices are always visible to an organization, giving management access to location, login, and activity analytics.

Shared devices find their way across the entirety of an enterprise. And in organizations with a wide range of use cases and many end users, having access to critical device telemetry and information can be the difference between a secure environment and compromised information. For this reason, BlueFletch tracks various actionable data sets for organizations to monitor and manage.

BlueFletch logs data related to device activity that helps improve device accountability. BlueFletch stores information on what activities a user does on a device, the applications they access, what network or access points they connect to, and the device's battery level. This paints a vivid portrait of the scenario and helps retrace steps to determine why a device may have gone missing in the first place.

Additionally, these accountability features give end users another reason to be responsible when using company-owned devices. When a user is aware that their organization monitors device activity, they may be less likely to use a device for inappropriate reasons.

***Device Finder***

A standout feature of BlueFletch's device accountability protocol is the Device Finder tool. BlueFletch Enterprise Device Finder uses precise geolocation using Wi-Fi 6 to locate devices on a map.

Organizations have access to a map of their environment to track down devices. These maps are customized to a store or workplace's layout, making precise locationing accurate and easy. Additionally, the device finder can use AR integrations alongside a device's camera for an augmented reality experience. Digital markers point out a device's location, so a user can find it whether it's sitting on a shelf or hiding somewhere in the warehouse.

Device Finder also hosts an advanced check-in and check-out functionality. BlueFletch captures a list of every user who logs into a device, the time of their login/log out, and the device's precise location. Device finder can trigger an audible sound or alarm on a device as well.

***Protecting Data***

At the center of device security is the protection of company data.

According to the Identity Theft Resource Center, there were 1,864 data breaches in 2021. These breaches span enterprises of all sizes and seriously threaten enterprise security. Lost devices are the main component of data breach incidents, as unprotected and unencrypted devices can access sensitive information, including:

- **Client data such as financial records, bank information, and confidential transactions.**
- **Employee financial information, addresses, and personal data (SSN, phone numbers, etc.).**
- **Customer information, such as credit card numbers and sensitive personal data stored on customer accounts.**
- **Proprietary enterprise information relating to stores, inventory, orders, traffic and more**

Leaking such information threatens not only the integrity of an organization but the individuals who support the company's mission. It is of the utmost importance to protect shared devices from falling into the wrong hands.

***BlueFletch Enterprise Security Protocols***
BlueFletch has a set of features to protect devices in case of a lost or stolen device. If a device leaves a company network or geofence, BlueFletch will lock it down until it returns. Once within the organization, BlueFletch re-enables its feature set again. For a worst-case scenario, BlueFletch has a timed feature that wipes all device data after a specific time. Even though the loss of a device is costly, it is far more reasonable than the loss of sensitive data.

### 3. Reduced Support Costs

Companies spend thousands of dollars annually on device fleet support costs and associated management software. Therefore, management teams are always looking for the best way to secure devices within the confines of an approved budget.

***The BlueFletch Support Agent***
The BlueFletch Support Agent is an Android application and background service that collects and displays real-time device-specific data to manage better and support device ecosystems.

The focus of the Support Agent is to collect as much device data as possible to maintain a healthy support structure. Instead of relying on the MDM to create actionable data, the endpoint generates accurate data reports. Support Agent leverages device data to develop a richer understanding of what is happening within a device. This gives IT support teams the edge they need to troubleshoot a single device or run a query across the entire fleet.

***Actionable Data with Support Agent***
One of thE advantages of the BlueFletch Support Agent is the output of analytical data. An organization does not have to pull information from its MDMs database; it can seamlessly access device data directly from their BlueFletch portal. Support Agent's dashboards identify and organize information to curate an accessible environment for organizations to better manage devices. An organization also can route its data through an existing analytic tool such as Splunk or Power BI. This may be an advantage when searching for additional reports, as BlueFletch does not limit an organization.

Application information is vital when managing a company-owned device fleet. With BlueFletch, an organization can see data on the applications used most and why. BlueFletch helps them survey their user base and generate an efficient environment for end users. In addition to application data, the Support Agent also provides information about which peripherals are in use and which user groups use what applications. Further filtering such data aids in maintaining a productive workforce.

Support Agent analytics reduces support costs by having actionable data readily available. Helpdesk teams no longer have to outsource support or wait for data from their existing MDMs to troubleshoot and resolve device issues. Putting data in the hands of an organization creates a more advanced management solution.

### 4. Improved End User Experience on Devices

BlueFletch Enterprise puts Android devices first and is designed for shared device environments. Many existing MDMs work best on single-user devices; however, BlueFletch supports device fleets of all sizes. By putting Android first, BlueFletch curates an ideal user experience for Android users.

BlueFletch user experience features include:

- **Widgets**
- **Notifications**
- **App Switchers**
- **Contextual Search**
- **Highly Configurable look and feel**
- **Chat**

### Polishing Enterprise Devices

BlueFletch's goal is to create an engaging, user-friendly experience that makes using company-owned devices feel personal and efficient.

BlueFletch

BlueFletch brings many of the functionalities found on consumer devices to the enterprise. This will help users feel more at home when using a device in the workplace. BlueFletch aims to make the shared-device experience just as interactive as consumer devices.

Some of the ways BlueFletch generates a better user interface include the following:

- **Notifications, icons, and widgets showing recent notifications or emails from a device's home screen.**
- **Users can quickly switch applications and search their system for files and tools.**

Shared device users deserve to have a polished, sharp look and feel to their devices. Primarily when they rely on these devices for daily responsibilities, a device should be one a user wants to use and feel as if it belongs to them, making it easy to use and efficient for their work tasks.

### BlueFletch Chat

Enterprise users traditionally leveraged walkie-talkies and portable VoIP phones to provide communication. However, the prevalence of company-owned workforce mobile devices drives the popularity of communication tools such as Microsoft Teams and Slack. These applications provide a hub for instant messaging, video calls, and other forms of digital communication. Users can share multimedia attachments and remain connected throughout the workday.

Many people have become adept at asynchronous forms of communication. Bringing this technology to company-owned workforce devices is only natural. Applications like Slack are tools many people are more comfortable using. These tools are excellent for corporate enterprise users but are not designed for frontline and field workers. The features found within applications like Microsoft teams better suit employees in back offices where the workday happens mainly on the computer.

BlueFletch bridges the gap between field workers and shared device communication with BlueFletch Enterprise Chat.

BlueFletch Enterprise Chat is built to make communication with shared workforce devices easy. It is specifically designed to provide asynchronous communication across the enterprise where applications like Microsoft Teams don't meet the needs of frontline employees.

BlueFletch Chat allows for communication to occur directly within the BlueFletch Launcher. There is no need for a third-party application. BlueFletch chat is purpose-built for field scenarios, offering end-users the functionality that works best with their job. Chat offers role and site-based chat for specific functionalities. Our chat supports direct messaging, video, and audio communication.

Some of the standout features of BlueFletch Chat include:

- **Asynchronous Communication**
  - Texting is the primary feature of BlueFletch Chat. Send and receive text messages directly in the chat application. Chat supports multimedia attachments (videos, images, etc.) for a more dynamic communication experience. Users can also send walkie-like voice messages for those times when sending a text isn't sufficient but having a call is too much.
- **Video Calling**
  - Users can perform FaceTime-like video calls from their devices. This allows for synchronous video communication with coworkers across the enterprise.
- **Voice Calling**
  - Just like any other mobile phone, BlueFletch Chat supports voice calling.
- **Presence**
  - See who is currently logged on to their device within a facility. This improves response time and accountability as users can see who may be available for a conversation or to aid with an urgent matter.
- **Configurable Roles**
  - An organization can assign roles to individual users, granting access to pre-authorized chat

channels to meet the needs of an employee hierarchy. For example, a manager can configure a rule allowing employees to only message their team members.

- **Data Security**
    - BlueFletch Chat is GDPR compliant, as it cleans all user data at the end of a session. Chat wipes all message history and chat details at the end of the user's shift.
- **Securing Devices**
    - BlueFletch Chat leverages WebRTC for direct device-to-device communication. This prevents audio and video calls from ever leaving your facility, resulting in not just a faster experience but a more secure communication experience as well.

## Key Takeaways

BlueFletch Enterprise upgrades authentication, security, and user experience. With an ever growing library of features, organizations can feel safe knowing BlueFletch is working hard to give users and management alike the experience they need. BlueFletch Enterprise reshapes the integrity of an organization's security posture, securing workforce devices while simultaneously boosting user productivity and the overall shared device experience.

If an organization is interested in a demo of BlueFletch Enterprise or would like to ask more questions, please feel free to reach out at info@bluefletch.com.

## 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. BlueFletch Enterprise provides a customized launcher, SSO, Support and Analytics, and MDM/EMM for Android workforce devices. BlueFletch Enterprise is currently the only solution that provides full FIDO support for shared Android Workforce devices.

BlueFletch Enterprise helps ensure an organization's digital transformation or management initiatives are effective and secure.

BlueFletch