WHITE PAPER

CHOOSING MOBILE LAUNCHER OR KIOSK MODE FOR WORKFORCE DEVICES

BlueFletch

INTRODUCTION

Android workforce devices provide organizations with the accessibility and functionality employees need to maintain an efficient workplace. These devices are crucial to developing productivity in dynamic environments like retail warehouses and delivery platforms.

As the use of shared Android devices continues to evolve, so has the need for increased functionality. Software solutions are constantly adapting to better interfaces or customizable management tools. In the hands of field and frontline employees, shared devices give end-users the best working experience and have become more critical than ever.

Kiosk mode and Enterprise Launchers are two approaches that enable organizations to lock down mobile workforce devices to increase employee productivity, enhance security, and prevent device misuse.

This whitepaper analyzes both solutions to help an organization make an informed decision about whether or not these mechanisms will benefit their company.

KIOSK MODE

OVERVIEW

Kiosk Mode is an Android software configuration that locks a mobile device into a specific application or set of applications for specified functionality. Devices set to kiosk mode are limited to the locked application(s) and cannot access any apps, settings, or device functions outside the set application. Kiosk Mode protects data by restricting unauthorized access to other applications or settings on the device.

An organization may leverage this mechanism for various purposes, including improved security and streamlined functionality for mobile devices. In retail, Kiosk mode typically functions for customer-facing devices, terminals, and kiosks for services such as self-checkout, price scanning, and stock checking. It is advantageous for organizations seeking to utilize single or multi-app devices without worrying about device security.

WHY CHOOSE KIOSK MODE ON MOBILE DEVICES?

Kiosk mode may be most beneficial for security and functionality purposes on customer-facing or employee-shared devices. In retail spaces utilizing self-checkout kiosks, and dedicated devices for customer support, kiosk mode is a safe option for improving the user experience.

Additionally, in environments where employees rely on multiple applications on shared devices, kiosk mode can be a more straightforward solution to providing a better user experience.

KIOSK MODE FUNCTIONALITY

Single vs. Multi Applications

Kiosk Mode offers two modes, single-application mode and multi-application mode. Both variants offer the same functionality but with a differing number of accessible applications.

Single Application Mode – Locks a device into one function or application, restricting access to all other apps, settings, and services on the device. Anything outside the locked app is inaccessible, protecting data while maintaining functionality. This mode is particularly beneficial for retail kiosks and devices dedicated to a single purpose.

Multi-Application Mode – Limits a device to two (or more) applications, allowing users to alternate between the approved applications but denying access to anything else. Like single application mode, a user or bad actor can not access anything outside the approved application set. This feature is useful when an end-user may need to use various applications in a dynamic scenario. This functionality is perfect for retail employees to protect device data while giving employees access to the tools they need.

Use Cases

As organizations focus on user engagement, the ease of Kiosk devices has found its way into day-to-day operations. Kiosks are becoming increasingly

crucial for businesses as they allow enterprises to provide single-use devices to mobile field workers and customers. Examples of single-app use include data entry, payment collection, and advertisement display.

Kiosk mode provides a diverse range of use cases across the retail environment, including:

- **Self Checkout –** In the wake of the COVID-19 pandemic, self-checkout kiosks have become more prevalent. Many customers enjoy using a kiosk device to scan, bag, and pay for their items while reducing interpersonal interaction. Kiosk devices service customers while maintaining security by limiting device use to checkout functionalities.

- **Ordering –** Outside the retail space, kiosks have become helpful for ordering food inside a fast food or takeout restaurant. Popular chains such as McDonald's already implement large touchscreen kiosks that access their menu and allow customers to place orders and pay without approaching the counter.

- **Product Scanning –** Retailers like Target and Walmart have scanning devices littered about their stores to let customers price-check items. Kiosk mode ensures that these devices function within the boundaries of their assigned functionalities while giving customers a sense of control over their shopping experience.

- **Parking –** Some parking garages offer contactless check-in and check-out parking kiosks at large shopping malls or event centers. These terminals allow customers to pay for parking and validate tickets for streamlined parking.

Implementing Kiosk Mode in the Field

Android devices can use kiosk mode by configuring them as dedicated devices (formerly called Corporate-Owned Single-Use or COSU). These devices can be left unattended and/or used for critical tasks as an organization fully manages them to prevent misuse. The company owns fully managed devices for work purposes.

There are two ways to deploy Android Kiosk devices to the field.

Employee-Facing Devices

Kiosk mode can be useful for shared device environments where employees need access to a few specific applications for their daily tasks. Kiosk mode eliminates the need to scroll through a collection of workplace applications and re-enter login information between apps. Any employee can grab a locked-down device and get to work.

Android provides a set of APIs that allow IT admins to lock down enterprise devices to a whitelisted set of applications that can run in full-screen (application pinning), which keeps the user from closing or switching to another application. These shared devices rotate between users after a shift, and there is no personal/work profile separation for dedicated device policies. Retail store associates, warehouse workers, field technicians, and delivery workers are the types of employees using a dedicated Android Kiosk device with a whitelisted set of applications.

Customer-Facing Devices

Sometimes customers do not want to bother store employees, and sometimes people don't feel comfortable approaching associates for assistance at checkout or within the store.

Kiosk-enabled devices that service customer needs, like price checkers and checkout kiosks, allow customers to have the shopping experience they want.

Not only do kiosk devices enable customers, but they also free up employees' time spent aiding customers. Employees have more time to focus on other pressing tasks and generate a better shopping environment.

A dedicated customer-facing Android device is the most common use case for Kiosk Mode. Android's APIs allow a device to pin an application in full-screen mode and provide lockdown options to the IT admin to enforce, such as:

BlueFletch

- A single application in full-screen mode
- Blocking all paths to settings
- Disabling status bar
- Hiding Home and Recent App buttons
- Turning off incoming calls
- Always awake device
- Disable automatic over-the-air (OTA) updates

Locking unattended devices is crucial since an untrained user base (the customer) uses them. Without having the lockdown APIs available in Android, the device could be left in an unusable state or used for nefarious reasons. All of which are missed opportunities for engagement or business activity.

LIMITATIONS OF KIOSK MODE

Kiosk Mode is a convenient solution for company-owned dedicated devices in the enterprise. Dynamic environments can benefit greatly from the ease and security functionality of kiosk-mode-enabled devices. However, as with any software solution, nothing is a perfect fit for every situation.

Imperfect Technology – the rise in popularity of kiosk-mode customer devices has contributed to large lines. Since untrained customers use these devices, lines may be longer as inexperienced customers fail to use devices properly. Also, kiosks have been known to be buggy and have issues with payment or scanning. If employees are not around to assist, these devices may cause distress or further inconvenience among customers.

Employee Concerns

Kiosk devices genuinely shine in the customer-facing sector. For organizations looking to create a more customizable user experience for their employees, kiosk mode may have more drawbacks than advantages. For example, kiosk mode can be limiting in dynamic environments where employees require access to device settings and subsets of different applications.

Since its primary function is to lock down a device, end-users may be restricted when leveraging devices across various tasks. Additionally, kiosk mode may not provide the user experience that a customized launcher can.

Kiosks may be a frustrating workaround for employees who depend on versatile device functions, tools, and accessories in their daily responsibilities.

KEY TAKEAWAYS

As organizations leverage mobile technology, Android Kiosks will continue to play a role in modernizing how employees work and customers interact with brands. Android holds more than 75% of the global market share and given its ease of use, level of customization, and support from OEMs, Android devices have become the enterprise mobility standard.

Kiosk mode is an increasingly accessible and valuable tool for organizations in the retail space. Consider leveraging kiosk technology for appropriate situations for increased customer and employee satisfaction.

MOBILE LAUNCHERS

Launchers are home screens on Android devices that control application access and on-screen device functionalities. These user interfaces (UI) are customizable and allow organizations to choose the best experience for their end users.

Companies control which applications are accessible in the enterprise by dividing access between specified roles. These allocated access points allow companies to manage which tools are available to certain employees. In addition to providing a customized experience, launchers run on a session-based functionality, limiting device access to approved users.

Launcher security protects individuals from accessing sensitive information or applications outside their approved permissions. Within a session, users can use every one of their approved applications, dynamically controlling their experience.

Launchers are a standard feature for all Android devices. Each vendor (Samsung, Motorola, HTC) in the consumer market has a launcher variant. Launchers come fit with customization features to

BlueFletch

allow enterprises to curate the end-user experience. However, organizations are not limited to using the default out-of-the-box launcher.

Organizations can replace an Android device's launcher with aftermarket or specialized launchers. Popular options include the Nova Launcher, Blackberry launcher, Smart Launcher, Action launcher, and BlueFletch Enterprise. Each variety of launchers caters to a different user experience, optimizing efficiency and organizational productivity.

LAUNCHER HISTORY

Launchers began as a way for Android users to have more control over their user interface. Customizing home screen layouts, colors, and functionalities allows users to bring their personality to their smartphones. But as Android devices become more popular in the enterprise, the launcher is a valuable tool in securing shared devices while giving employees access to applications and functionalities their roles require and give employees the power they need to drive productivity. With access to workplace applications and features like NFC authentication, SSO, scanners, and other accessories, Android devices provide a dynamic experience.

As these devices continue to evolve, so does the launcher software.This means having advanced customization capabilities, and control over device settings. With devices costing upwards of a thousand dollars, these features are essential. Why Choose a Launcher?

CUSTOMIZATION

An organization's ability to customize and control shared device capabilities is crucial to providing the best end-user experience. Launchers create a perfect environment for an organization to manage user permissions, access, and interfaces by utilizing many customization options.

A shared device is critical to daily tasks in dynamic workplaces. They provide employees with the tools they need to service customers or nurture the flow in a warehouse. However, not every employee works the same, and some roles may require a unique set of applications or functionalities that another role may not. Launchers ensure every employee gets their hands on the applications they need.

SECURE DEVICES

There are more secure launcher versions than the default launcher provided by the vendor. An organization's data is safer with a more secure launcher that hardens and locks down devices. Features available in a secure launcher include: controlling setting access, controlling notifications access, requiring PIN/password for device access, and controlling what applications users can access.

SINGLE-SIGN-ON (SSO)

SSO grants users access to all workplace applications with a single set of credentials. A launcher outfitted with SSO generates a secure session, allowing users to use their approved apps with a single login.

SSO sessions also minimize failed login attempts and wasted time by letting users switch between apps without having to re-authenticate. A recent study found that the average login time is 42.3 seconds, resulting in hundreds of dollars lost yearly. SSO can save an organization upwards of $800 per device per year.

SSO is a more secure alternative to traditional passwords.SSO only grants users access to their pre-approved applications, not even employees can access information beyond what an organization lets them access. Additionally, once a secure session expires or a user logs out, that device is only accessible with valid credentials. For more information on how SSO saves organizations money, refer to this article.

Other benefits include:

Login Accountability – An organization can see who accessed a device last and generate a list of login attempts. This can reduce the percentage of lost devices as end-users know they are accountable.

Forgotten Passwords – Forgotten passwords plague the enterprise. In an organization that requires a laundry list of login credentials for all its workplace applications, users are more likely to forget their

BlueFletch

passwords. With one set of credentials, users can access every application without worrying about forgetting. Additionally, the reduction in lost passwords also reduces the number of password resets done by the helpdesk.

Benefits

The customizable launcher is the most beneficial solution for work environments with a range of dedicated roles. The launcher provides offerings for customization across an entire device fleet, but it also allows an organization to customize the UI for each user. Taking advantage of these tools proves to boost device effectiveness while empowering end-users.

SESSION-BASED ACCESS

Launchers are customizable, session-based interfaces where users access role-based applications. Instead of isolating a user to one application (or a subset of applications), a launcher dynamically controls the user experience across every application. An organization can choose any number of applications per user, role, or device. These applications are only available to the users who fit an organization's predetermined criteria (i.e., position or access level).

A session begins when a user enters their login credentials. Their credentials unlock the pre-approved applications necessary for their role. Users can access every authorized application within a valid session and seamlessly switch between these apps without reauthentication. Session-based access also allows shared devices to rotate without needing to reset or adjust settings. Once one user logs off, the following user to log in will be able to access their approved applications, and there is no need to worry about wrongful access.

ROLE-BASED ACCESS

The launcher makes delegating access simply by providing organizations the means to customize application access on a role-based level. When users enter the system, an organization can assign a subset of applications based on their roles and responsibilities. These applications can be organized from the backend, so any user assigned to a specific role will automatically gain access to the necessary applications.

This way, managers, and users working in a warehouse can use the same shared devices without worrying about losing access to their applications. Keeping access organized is one of the many ways launchers can keep end-users productive and satisfied.

CUSTOM SETTINGS OR RESTRICTING ACCESS

One of the most significant advantages of an Android launcher is the variety of options available on the platform. However, without a secure launcher solution, employees may change settings to improve their UI or accidentally render a device unusable. Some scenarios include:

Network Changes – Users could connect devices to unsecure public networks that compromise the security of an entire organization.

Installing Apps – Employees may install inappropriate applications that could become dangerous or carry viruses. Furthermore, without settings to limit application use, employees could download games and apps that limit productivity.

Uninstalling Apps – An employee may sometimes uninstall applications crucial to daily operations. In an environment where shared devices all have the same apps, this could create issues for employees in other roles who need access to said applications. Due to the highly customizable nature of the launcher, an organization can avoid these mistakes by controlling the settings and locking them away from users. Launchers allow an organization to:

Restrict Settings Access – Deny users the ability to see or change their device settings.

Restore Defaults – Some settings, like screen brightness or Bluetooth, may be available to users. When a user has changed these settings, an organization can build a process that allows a device to return to specified default settings upon logout.

Monitor Changes – Track what changes and monitor updates to ensure users get the best experience.

BlueFletch

THREE SCENARIOS FOR LAUNCHERS
While every Android device has its own launcher, an organization typically follows one of these three paths.

The Default Launcher
The out-of-box experience may be the quickest and simplest solution for an organization without investing time or money in an aftermarket launcher. Most manufacturers include an out-of-the-box launcher such as the Zebra Enterprise Home Screen, The Honeywell Launcher, or the Datalogic Lockdown launcher. Manufacturers do not consistently optimize launchers for the diverse use cases of different enterprise environments.

While convenience is a driving factor, it should never be the main focus. Default launchers do not have advanced support for SSO (single-sign-on) and shared multi-user scenarios. Default launchers are typically capable of launching applications while locking down other device features.

This may prove to be a roadblock for organizations needing a more dynamic user experience. Additionally, the lack of advanced support for security features, such as SSO, does not allow organizations to upgrade their security standards.

The Proprietary Launcher
Organizations may decide to develop a proprietary launcher. In-house development can seem like an advantage over outside development; however, the future costs and maintenance associated with maintaining launcher support can be overwhelming. Providing ongoing support for new Android versions and allocating resources to bug fixes or major security updates is costly. Lack of attention given to continued launcher support can leave devices vulnerable to breaches.

The Customizable Launcher
Organizations with complex needs often turn to customizable launchers. The flexibility of having a customizable launcher is essential to providing value in a dynamic environment. Curated application access and more control of device functionality give organizations a wide range of versatility. These launchers support SSO, blend multiple legacy and third-party applications, or provide additional device control and compliance.

These Launchers offer a gamut of security features to protect company data, streamline and improve the login process, and personalize unique user roles. Organizations with dynamic work environments needing an adaptable and dependable software solution should consider a custom launcher.

CONCLUSION

Launchers are an excellent way to accelerate the employee experience by giving users the tools they need with a functional and streamlined user interface. For an organization looking to boost productivity, increase security and customize the user experience, launchers may be the ideal solution.

THE BLUEFLETCH ENTERPRISE LAUNCHER

The BlueFletch Enterprise Launcher is a highly secure and customizable home screen replacement for Android workforce devices that ties into all major Identity Providers and provides a quick login experience using single sign-on.

Improved User Experience
Seamless Single Sign-On – Eliminate the need for users to remember and repeatedly enter their usernames and passwords for each application. With BlueFletch SSO, users can use one set of login credentials to get immediate access to all their business apps in under 5 seconds.

Modern Re-Authentication – Employees can re-authenticate using NFC, FaceRec, Fingerprint Biometrics, Barcode, and PIN to instantly access devices and apps instead of fumbling with passwords.

Strengthened Device Security
Multi-Layered Device and User Security – BlueFletch Enterprise Launcher provides an added layer of security and integration that goes above and beyond.

BlueFletch

Application Control – Manage application access on an individual or role-based level, and give employees access to the applications they need. Also, restrict access to settings and unapproved applications to increase security and limit vulnerabilities.

Identity Provider Support – Integrates into all major Identity Providers (e.g., Azure AD, Okta, SailPoint, Ping), allowing consistent enterprise security out-of-the-box.

Configurable Logout Events – Trigger logout based on custom events such as device cradled, no detected motion, and timer per role.

Clear Cached Data Upon Logout – Take control over device data by clearing running apps, destroying session tokens, and removing cookies upon logout to keep sensitive data secure.

Reduce Device Loss

Capture Login/Logout Events – With check-in/check-out data, see which users currently have what device and when they last used them to maintain device accountability.

Device Finder and Battery Alerts – Built-in configuration tools to find missing devices using network access points and dispatch audible alerts. A battery threshold keeps devices from going missing. The BlueFletch finder tool provides real-time mapping and location data for all company-owned devices. Leverage finder to locate misplaced devices with AR support for dynamic locationing within the field.

Detailed Login and User Data – Feed login and usage data into any backend data services to support end-to-end visibility of device usage.

The BlueFletch Enterprise Launcher is a premium solution for organizations looking to improve the user experience, strengthen device security, and access actionable data.

SUMMARY

KEY TAKEAWAY:
Launchers hold an advantage over Kiosk mode for their range of dynamic use cases and customizable functionality. Launchers provide much more flexibility for organizations to curate the best user experience while also maintaining device security.

Kiosk mode is a far more restrictive option and does not hold a candle to the versatility of Launcher. Kiosk Mode is ideal for point-of-sale terminals and other devices whose use cases are limited to one or two applications.

Launcher's ability to control application access, device settings and improve upon security options make it perfect for dynamic work environments.

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