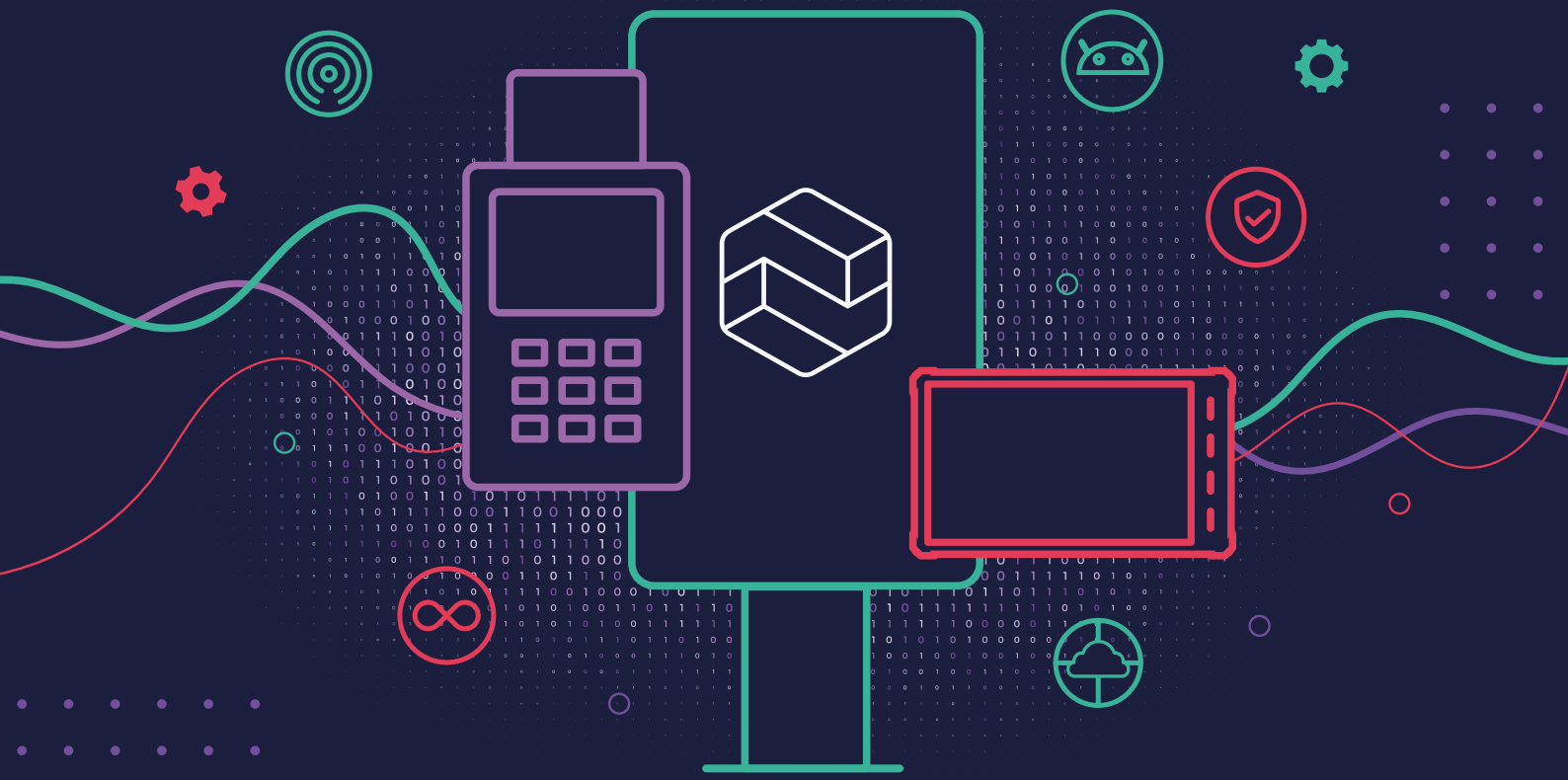
esper

TCO Considerations for

Dedicated Device Management vs. Traditional MDM Solutions



TCO Considerations for

Dedicated Device Management vs. Traditional MDM Solutions

Overview

Most total cost of ownership (TCO) analyses for device fleet mobility focus exclusively on **workplace smartphone scenarios via bring your own device (BYOD) or corporate-owned, personally-enabled (COPE) scenarios, rather than the mission-critical, revenue-generating single-purpose devices** that make up the majority of today's corporate fleets. As a result, IT and product ops professionals often struggle to estimate the true total cost of ownership of fleets for device-dependent businesses.

A comprehensive analysis of costs demonstrates that the capital expenditure (CapEx) and operational expenditure (OpEx) costs associated with dedicated Android devices are much different than CapEx and OpEx for workplace smartphones. **For example, studies show the single highest cost factor involved in BYOD and COPE smartphone programs is data connectivity, which is rarely true for single-purpose Android devices such as kiosks, point-of-sale, or interactive signage.** On the other hand, mission-critical, single-purpose devices often have much higher operational and maintenance requirements than employee-enabled smartphones.

To build a comprehensive TCO analysis, comprising both OpEx and CapEx, organizations need to look beyond monthly recurring connectivity costs and per device software subscription costs (generally, organizations pay a subscription fee between $3-15 per device per month).

In this guide, we take a look at the following list of factors to consider when comparing platforms that are purpose-built to manage device fleets to traditional mobile device management (MDM platforms) to understand: time to market and launch delays, maintenance and remediation, security incidents, product flexibility, and scaling.

As touchscreen device fleets are increasingly important to business strategy and differentiation in the market, all of these considerations grow in importance.

Many of the additional costs associated with operating a dedicated device fleet are associated with IT Operations staffing. As a result, **organizations should consider talent availability when considering the impact of traditional MDM on an Android product roadmap.** Nationwide, there is a noted talent shortage of individuals with Android device lab expertise, especially when it comes to nontraditional or purpose-built hardware. Depending on your region and total compensation packages, you may face significant delays in filling open positions.

In this guide, we break down each of these factors, enabling you to more accurately calculate the total cost of ownership (TCO), and as a result, make smarter decisions about how to plan, operate, and manage your device fleet.

In this guide, we break down each of these factors, enabling you to more accurately calculate the total cost of ownership (TCO), and as a result, make smarter decisions about how to plan, operate, and manage your device fleet.

Excecutive Summary

While many IT and product ops leaders believe that traditional MDM solutions can deliver lower TCO for Android devices, the true cost output varies significantly according to hardware choices and use case. MDM can deliver a lower cost output than manual management methods for BYOD use cases, but it does not have the same effect for single-purpose devices such as kiosks, point-of-sale systems, medical devices, ruggedized hardware, tablets, and interactive signage. **MDM solutions, due to their roots in BYOD and enterprise phones, along with the need to be a one-size-fits-all tool, lack the key features and customization necessary for a rapidly changing dedicated device fleet.**

Based on experience with thousands of customers across many industries, from hospitality and restaurants, to education, retail, healthcare, and logistics, using an agile platform based on a Developer Operations (DevOps) approach can lower OpEx by 60% or more compared to traditional MDM solutions in single-purpose device scenarios. By examining all the factors that lead to savings with deploying and managing single-purpose Android devices and apps, **organizations can gain a deeper understanding of the TCO differences between traditional MDM and purpose-built fleet management tools.**

Defenitions

Traditional MDM

Mobile device management is a category of technology that manages policy, inventory, security, service, and apps for smartphones and tablets. MDM originated in the early 2000s, built to address BYOD use cases. **As a result, MDM tools were never intended as a solution for dedicated device fleets** where the end-user experience is correlated to company revenue. The MDM DNA is to protect the company from employee devices. **In the MDM paradigm, the company is first, while devices are considered to be a risk that must be mitigated.**

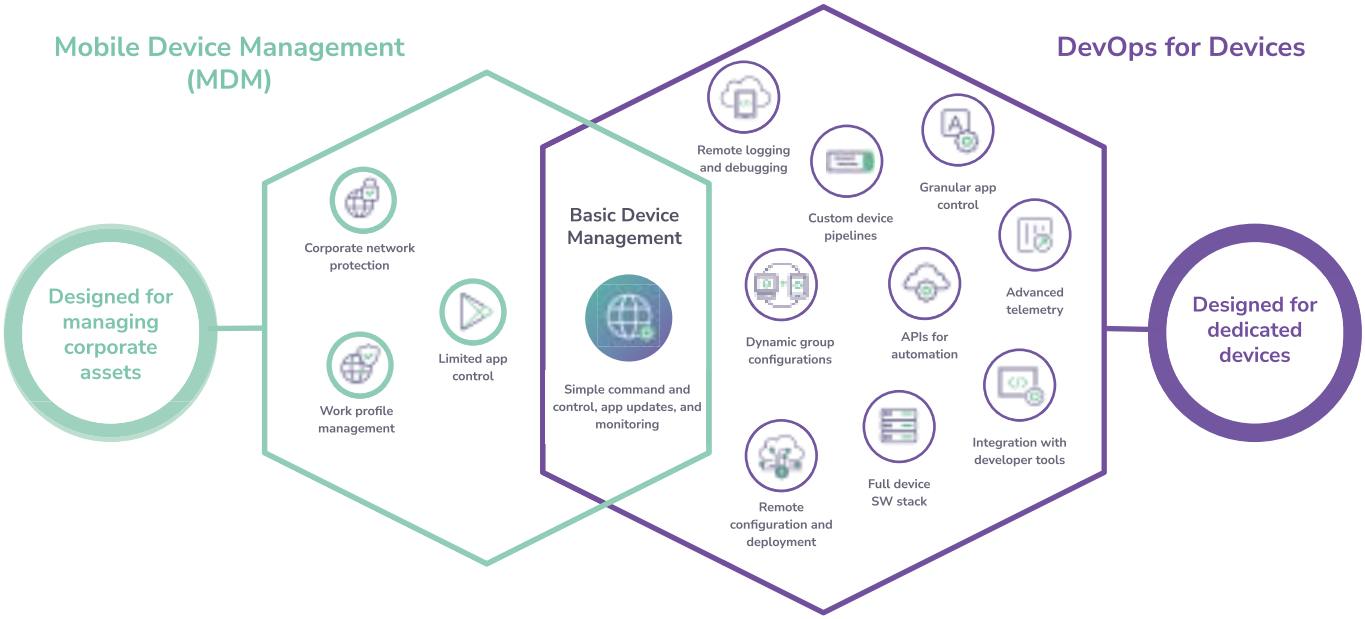
A traditional MDM solution may be related to technologies such as mobile application management (MAM), unified endpoint management (UEM) or enterprise mobility management (EMM). For the purposes of this analysis, the traditional MDM category includes both cloud-based solutions and homegrown mobility management applications.

Dedicated Device Management

Dedicated Device Management is an emerging category of technology that describes an infrastructure for managing both traditional and non-traditional device deployment and app management, including support for kiosks, point-of-sale, telehealth devices, smart fitness equipment, and more. Its emergence is a response to the growing importance of dedicated devices to modern business strategy. A 2022 study by 451 Research **found that 89% of companies consider their dedicated device fleets to be a critical tool for differentiating their services and customer experiences.** Because consumers expect continuous improvement, frequent updates, and always-on stability, DevOps principles are core to dedicated device management solutions. As a result, these offerings can be called DevOps for Devices (or DevOps for Dedicated Devices) solutions.

Dedicated device management solutions create a responsive connection between fleet devices and the cloud, allowing IT operations to monitor, update, and remediate the total state of device health. A Dedicated Device management solution encompasses device configurations, hardware, firmware, operating system, applications, and more. **Contrasted against the MDM paradigm, the end-user is first, while devices are considered to be a mission critical company asset.**

A Dedicated Device management solution has capabilities that allow you to operate on a fleet (or subdivided fleet) holistically, **so teams can worry less about device management and infrastructure, and spend more time on the product.** Dedicated Device management platforms are also equipped with additional features to support a full lifecycle approach to mobility, including automation tools, deployment pipelines, and a complete software development kit (SDK).



Factors to Consider in Building a TCO Analysis

Device Deployment Timelines

TL;DR: How much do you value speedy time to market? Consider the cost of slower device deployment downtime when trying to adapt a one-size-fits-all MDM approach to bespoke dedicated device fleet use cases.

Your organization's average time to deployment can impact both device fleet cost considerations and user satisfaction. Android deployment delays can carry both hard and soft cost factors due to a loss of potential revenue or damaged customer trust. These costs are only increasing as a result of the COVID-19 pandemic, which accelerated the business importance of single purpose devices, such as revenue-driving self service ordering and payment terminals. Data shows that customers are demanding more self service options—73% of customers now prefer self-service options such as kiosks, unattended point-of-sale, or interactive digital signage to face-to-face interactions with a human customer service representative, according to Aspect research. **A single unattended payment device likely has a higher potential ROI than ever before. Conversely, the cost (lost revenue) of any delay to device deployment is also higher than ever before.**

While deployment timeline factors can vary significantly according to your traditional MDM and business requirements, it's important to consider the following factors when comparing traditional MDM to Dedicated Device Management with DevOps in terms of cost:

Off-the-shelf or purpose-built device procurement time frames

Shipping time from OEM to HQ

Shipping time from HQ to deployment site

Application and license procurement intervals

Integration testing

Application testing

Staging and kitting

Remote site deployment

Depending on the deployment approach taken, sourcing and provisioning Android hardware via traditional MDM can take months or longer due to the challenges associated with testing devices for interoperability and on-site provisioning requirements. Furthermore, if you're limited to specific hardware models or configurations, procurement timelines can grow exponentially. **As a result, with many traditional MDMs, you get locked into specific off-the-shelf device models, and you require a team of Android experts to accommodate anything different.**

With a Dedicated Device management solution, you will still likely need to partner with and build relationships with OEMs and ODMs to design and build your hardware, but you benefit from greater flexibility, and as a result, lower costs to accommodate any variation or model changes. **And, with a Dedicated Device management solution that offers remote provisioning, you can ship devices straight from the manufacturer to the intended point of use.** With pre-set device configuration, all the end-user needs to do is boot up the device, reducing time to value and increasing user satisfaction.

Maintenance and Remediation

TL;DR: Consider CapEx and OpEx costs such as support subscriptions, field support, revenue and brand losses due to device downtime, and device replacement costs due to tampering or theft when determining whether a BYOD-focused MDM solution is appropriate for managing a dedicated device fleet.

In addition to monthly subscription pricing, monthly maintenance costs for Android devices and apps can be around 15-20% for workplace smartphones. But, the maintenance costs for single-purpose devices can be much higher than the OpEx common to BYOD or COPE scenarios.

Single-purpose devices often have much more stringent security and privacy requirements to prevent end user misuse. Cutting corners on mobile security can double the risks of a security incident, according to Verizon Research. Sacrificing security for time savings can be incredibly costly, especially considering the global average cost of data breach recovery is $3.92 million.

Single-purpose devices such as kiosks or point-of-sale are generally operated at a separate location from the organization's headquarters and IT operations staff and are more likely to involve non-traditional or purpose-built hardware that's not necessarily built for remote maintenance or remediation, increasing the need for on-site repairs.

Factors that significantly impact both OpEx and CapEx when using traditional MDM to manage single-purpose, dedicated Android device fleets, include:

Post-sales support subscription from device or MDM manufacturer

On-site support to perform regular or ad hac maintenance

24 x 7 on call support

Testing application or peripheral compatibility prior to upgrades

Revenue and reputational losses due to device downtime

Productivity losses due to employee or customer device misuse

Physical losses due to devices tampering or theft

Replacement device shipping costs

TIme and resource commitment needed to track upgrade requirement

The latest data shows that Android has become the dominant OS for dedicated devices. Even then, today's fleets often represent a broad mixture of device models, device manufacturers, and Operating System (OS) versions, such as Android 11, Android 12, Android 13, etc. Each model and manufacturer can have a unique schedule for patches and upgrades. **Staying on top of these changes is resource intensive for IT operations staff, and it is typically more cost-effective to outsource if possible.** Finally, non-traditional hardware upgrades can be surprisingly challenging, and in some cases, require technicians to physically unscrew a case or device components before security patches can even be applied. **Trying to manually maintain a fleet using traditional MDM is often unpredictable,** leading to remote device downtime and security risks. With dedicated device management's advanced remote capabilities, maintenance, troubleshooting, and remediation can be done remotely, saving significant support resources while reducing device downtime.

New Use Case & Application Adoption

TL;DR: Consider the value of having an agile device strategy so that you can capitalize on opportunities and reduce costs including on-site visits to physically change or update devices, failed deployment results, and poor visibility into performance.

The pandemic created a "new normal" for consumers worldwide. Consumer-facing organizations face new levels of demand for self-service and unattended mobile solutions. Business agility has always been critical, but it matters more than ever with the shift in customer expectations over the last few years.

Research by McKinsey confirms organizations with a faster operational response time to new use cases achieve 30-50% superior measures of efficiency. The most agile organizations also appreciate 10-30% better customer satisfaction scores. And finally, the same study shows that agile organizations have 10-20% better financial performance than their counterparts.

The ability to rapidly adopt new use cases, especially remotely, has not traditionally been a part of TCO analyses for Android mobility. But, the idea of use case adoption and opportunity loss has clear value in the post-pandemic world. Shekel Brainweigh research indicates that **87% of global consumers now prefer digital self service.**

Beyond use cases, it's increasingly important for organizations to drive efficiencies by increasing device flexibility, often by repurposing devices to run different applications at different times. Many single-purpose Android devices are locked to Android kiosk mode, a configuration state that limits end user access to download apps, make calls, or browse the internet. Locking users to one or more enterprise apps can protect productivity and privacy and mitigate the chances of misuse. But, secure and effective application deployment can be a challenge without sufficiently advanced tooling to support Android kiosk mode.

Traditional approaches to mobile application management are ineffective for modern Android mobility roadmaps. End users often don't need unfettered access to download social media apps via Play Store, especially since consumer apps can carry security and productivity risks. In addition, many traditional MDM solutions require that devices are powered on before app updates can be pushed to production, which is unreasonable for many global fleets.

IT operations pros should shift their mindset from traditional mobile app management to edge content delivery. Content delivery networks create a powerful connection between the cloud and edge device by frequently caching updates to ensure end users have access to the latest app versions and device content.

While the OpEx and CapEx costs of traditional MDM vary by use case, they can include:

Speed and efficacy of purpose-built hardware design

Compatibility testing between cloud tools, and peripheral hardware

Testing deployment performace according to use case

Opportunity cost(s) of failed use case deployments

On-site visits to physically update device application content

Waiting for devices to come online before pushing app updates

Minimal cloud lab testing tools to gauge real-world performance before deployment

Failed or mixed deployment results leading to loss of uptime or satisfaction

Poor visibility into app performance or success in production

With traditional MDM, organizations run the risk of waiting months or even years before being able to expand to new use cases. If a purpose-built hardware project fails or organizations order hardware that is not compatible with the traditional MDM, new components of the product roadmap can be significantly delayed, resulting in lost revenue opportunities and poor end-user experiences.

In contrast, a dedicated device management solution can significantly streamline the deployment process by offering validated devices, validated peripherals, and cloud test tools that are backwards compatible with developer and QA environments. According to a 2022 study by 451 Research, speeding up time to market was the top reason why respondents desire to apply a dedicated device management with DevOps approach to the development of device applications (followed by improving quality of user experience, lowering overall costs, and increasing organizational agility).

Scalability

TL;DR: Consider both OpEx savings associated with workflow automation, OTA updates at scale, and CapEx savings associated with device reuse and repurposing.

Historically, mobility had a 1-to-1 ratio for devices to employees. In the early 2000s, each member of the senior leadership team was equipped with a Blackberry. A decade ago personal smartphones became a commonplace tool for both workplace and non-work usage scenarios, which led to the advent of the BYOD movement. Today, the ratio has shifted dramatically. **Connected devices significantly outnumber contributors at most organizations**. IDC predicts there will be 41.6 billion smart, connected edge devices by 2025.

Traditional MDM tools simply weren't architected to handle the demands of a large-scale fleet. And, trying to use a traditional MDM solution to manage a fleet of 10,000 or 100,000 devices can create serious efficiency and security problems. It's crucial to consider whether your current mobile device management solution can scale to meet your Android roadmap, or whether you'll absorb risks such as performance degradation or inefficiency. Cost factors associated with using traditional MDM while scaling can include:

Limitation on reusing or repurposing device provisioning templates

The inability to reuse a single provisioning template for multiple device types

Limited or nonexistent ability to remotely provision devices using IMEI or other factors

Minimal remote, over-the-air deployment and provisioning tools

Noexistent device group commands or nested device groups

Poor ability to create programmatic actions, alerts or reporting

A lack of APIs for custom - built, cloud-connected solutions

In contrast, a Dedicated Device DevOps tool is **built to scale from 100 to 10,000 to 100,000 devices and beyond without adding to the IT operations burden.** It offers full cloud GUI features as APIs for custom development scenarios and sophisticated, nested groups to support programmatic or streamlined actions at the single device, device group, or sub-group level.

Key Takeaways for Business Line Leaders

The last few years have accelerated a trend that was already in the making - a pivot to digital experiences and dedicated devices to meet customer expectations and drive revenue growth. The reduction of inefficient operating costs (OpEx), improvement and predictability of capital expenditures (CapEx), and increasing ROI expectations from dedicated device fleets are but a few of the benefits tied to a dedicated device management strategy. **The good news is that these costs are controllable.**

Organizational costs are directly impacted for a myriad of reasons attributed to the expanding scale and complexity of dedicated device fleets. Staffing your IT department at the same rate as your growing fleet to constantly troubleshoot and maintain devices is inefficient and expensive. Device interoperability, testing requirements, deployment roadblocks, and device hardware limitations exponentially increase the time to market and create significant missed revenue opportunities. Creating the experiences customers expect are limited by **MDM tools with a "one-size-fits-all" platform that simply weren't built to support dedicated device fleets.**

The costs associated with development, deployment, and maintenance of dedicated device fleet infrastructure are the costs easiest to control with a dedicated device management solution. And notably, **this not only saves your organization financial resources, but also unlocks the potential of your existing teams by freeing them from monotonous, low-impact tasks that should be remotely managed, monitored, and fixed by a platform.** As a result, you can reprioritize them to focus on product and customer experiences, while actually being able to quickly build and support those experiences.

A Dedicated Device DevOps solution can reduce OpEx by 60% or more as compared to traditional MDM solutions while improving overall financial performance up to 20%; improve the time to market for mission-critical devices that deliver front-line services; and allow for the seamless expansion and scale of your dedicated device fleet by choosing a tool custom-built for the job.

Key Takeaways for Technical Leaders

IT Operations teams face increasing pressure and burden as the shift to digital-first experiences has not only accelerated but been thrust front-and-center to meet the changing technical landscape. This has increased the resources necessary to troubleshoot devices in-field, underscored an emphasis on the critical need for remote access and monitoring, and revealed failure-points in the hardware supply chain that ultimately constrain business and IT strategy.

At the heart of these challenges is the recognition that MDMs were built to service legacy BYOD use cases, not to support dedicated device fleets. As such, these "one-size-fits-all" solutions only address some of what a dedicated device fleet manager requires from such a platform to be successful. **Limitations on customized user-experiences, manual device deployment, lack of insight into fleet status or health, and inability to troubleshoot any device remotely are but a few of the barriers constraining your fleet potential.** And the common denominator across each of these is the lack of a flexible, scaleable, reliable and automated tool custom-built for dedicated device fleet management.

With device fleets growing exponentially and the need for dedicated devices to play an increasingly key differentiating role in customer experiences, the risks only increase as fleet complexity and scale grow. A dedicated device management solution addresses these pain-points by removing the most manually intensive tasks and providing **truly granular control of the entire fleet, automating provisioning and device deployment through pipelines, and allowing for configuration of bespoke fleets into groups and sub-groups with transferable device configurations.**

A dedicated device management approach not only eliminates most of the primary pain-points in your day-to-day role, but also opens up avenues of innovation by making it much easier to deploy solutions quickly with a device-agnostic approach.

Conclusion

Dedicated Device Management with DevOps Lowers TCO, Increases Revenue Opportunities

A thorough analysis of all cost components shows why dedicated device management solutions can lower OpEx and even CapEx compared to traditional MDM solutions. In order to fully understand the cost of MDM solutions built for smartphones, **organizations must look beyond the per device subscription price to understand the greater context and related factors, including the significant provisioning, maintenance, and remediation requirements needed to secure remote, single-purpose devices.**

Traditional MDM tools have value for select scenarios, including both corporate and employee-owned smartphones, but when organizations attempt to adapt and scale these tools to manage kiosks, point-of-sale, interactive signage, or other dedicated-device fleets, they encounter significant efficiency and orchestration challenges. In practice, many organizations find they are unable to integrate non-traditional hardware or use cases with their existing tools and have little visibility into the health or performance of field devices.

Global food-chain Saves Millions

A global food-chain looked to transform their technology stack to meet the new challenges of rapid food delivery, self-service ordering, and increased demand in drive-thru orders. To execute this transformation effectively, save on OpEx costs, and extend the life of their devices, they looked to an Android DevOps platform to control their entire device fleet, deploy application updates over the air, and remotely troubleshoot and debug. **By using Android DevOps, they reduced device deployment time by 380% and saved $15 million in OpEx across their thousands of stores.**

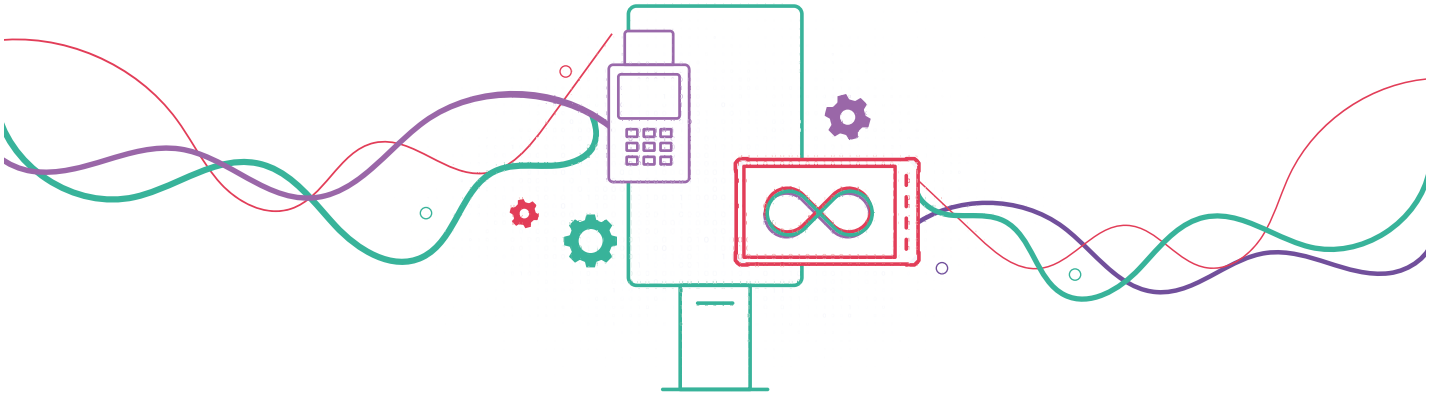
In-Store Kiosk Solution Reduced OpEx by 30%

A provider of in-store kiosks that capture shopper feedback in a fun and interactive way struggled with device management. Devices frequently went offline, software crashed, and they had to send support into the field to provision, manage, and troubleshoot, resulting in high operating costs.

Using Android DevOps, they were able to quickly and easily provision devices in as little as three days—importantly, with the ability to monitor and fix issues remotely. **They were also able to deliver a better customer experience with reduced device downtime, and reduced their operations costs by 30% because they no longer had to go into the field to deploy and fix their devices.**

C-Store Chain Accelerates Time to Market for New Self-Serve Kiosks

Parker's Kitchen is a fast-growing convenience store in the Southern United States. Their leadership team set a goal of getting 40% of customer purchases through self-serve kiosks. They wanted no-touch remote device deployment, management, monitoring, and maintenance, as well as telemetry for real time data analytics so they could improve the customer experience with a customer loyalty program. With an Android DevOps platform built into their hardware solution, **they remotely deployed custom self-serve devices with Kiosk Mode in just two months and experience ongoing savings of 60% in OpEx per store.**



Want to explore how you can reduce the total cost of ownership for your dedicated device fleet?

Request a consultation with Esper's Android experts

About Esper

Esper is the world's first device platform built specifically for the reliability and precision required of modern dedicated device fleets. We're compatible with both traditional and nontraditional hardware, GMS-certified and AOSP (non-GMS) hardware, and Android OS versions 4.4+ to provide comprehensive support for both off-the-shelf and purpose-built solutions that span retail, hospitality, education, healthcare, fitness, and more.

Traditional MDM has its value, but Esper is the first tool built to simplify the challenges of scaling a single-purpose fleet. We have validated and provisioned more than 1400 Android device models from 100+ OEM/ODM and manufacturing support to streamline deployments. Our user-friendly cloud GUI features are offered as Android management APIs, all of which is backed by best-of-class customer support.

Visit **esper.io/signup** today to get started.