Scalefusion

Android MDM

Mastering Control, Security, and Productivity

An Ebook for IT Administrators

What’s Inside?

Scalefusion

Why read this Ebook?

How many mobile users do you think there are worldwide? Take a wild guess! Well, will you be surprised to know that there are around 7.33 billion mobile (as of 2023) users worldwide? Seven billion, as in nine zeroes after seven! Yes, NINE! And out of these, there are about 3.6 billion Android users.

Now, with these astonishing numbers, it is absolutely imperative to have a robust mobile device management solution for your Android device fleet. In today’s fast-paced world, where the number of mobile devices is skyrocketing, the security threat landscape is also expanding exponentially. Well, you must have heard about a saying that prevention is ALWAYS better than cure. So, to ensure the utmost safety and protection of your Android devices from potential threats and vulnerabilities while maximizing IT productivity, the ultimate solution lies in adopting a Mobile Device Management (MDM) solution.

An MDM solution emerges as the perfect solution, ensuring not only the safeguarding of your Android devices but also for the empowerment of your IT infrastructure. In this dynamic landscape, the symbiotic partnership between technology and security becomes a cornerstone for continued success. If you're currently reading this, you're likely in search of an improved system for the management, control and security of the Android devices used in your business. In our comprehensive Ebook, we will explore the evolution of device management, the rapid growth of Android device management, the ways in which Android MDM can enhance your business, and the benefits you get from it.

Let's dive right in!

Scalefusion

Challenges of Modern-Day Businesses

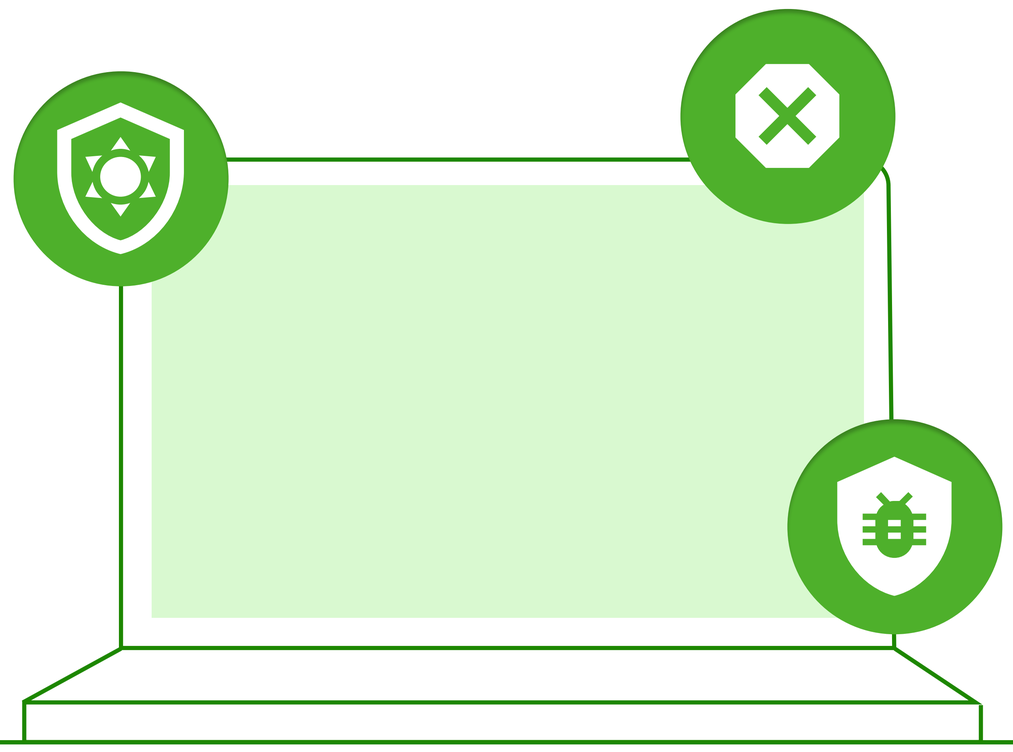
Today's IT operations face numerous challenges, ranging from cybersecurity and digital transformation to cloud migration, automation, analytics and data management. One crucial aspect is ensuring that the fleet of Android devices used by employees remotely is functioning optimally, with enhanced security measures and supporting maximum productivity.

In the past, when everyone worked in the same building with the protection of a secure firewall, IT faced fewer difficulties in identifying devices used for work, checking their software versions, addressing patching needs for software updates and security enhancements, and assessing the stability of devices. Additionally, calculating the cost of a device in terms of downtime, as well as resolving any necessary repairs, was simpler.

However, in our current remote business landscape, employees often access corporate networks using their own devices or they use company devices during remote work. This adds to the IT team's challenge of managing performance and ensuring the best value for money from hardware. Device have become mission-critical in remote business settings. If a laptop malfunctions, the impact on user productivity can result in significant financial losses, amounting to hundreds of dollars per user, per hour, or even more.

In the era of cloud computing, mobile technologies, and user-centric environments, IT teams must also address emerging challenges. These include identifying vulnerable device to known threats, gaining increased visibility into remote devices and streamlining management overheads associated with maintenance, tech support and operating system updates.

Modern IT Ops teams need to strike a delicate balance between accommodating mobility and collaboration demands while ensuring robust security and manageability.



Scalefusion

Introduction to Android Device Management

Since the launch of the HTC Dream in September 2008, the first Android phone, the Android operating system, has continuously remained in the spotlight. And even now, after fifteen-odd years, Android accounts for 70.9% of the mobile operating market share worldwide.

The versatility of the Android operating system has been clearly demonstrated through its ability to power a diverse range of devices. Whether it's smartphones, tablets, or even televisions and watches, Android offers wide device diversity.

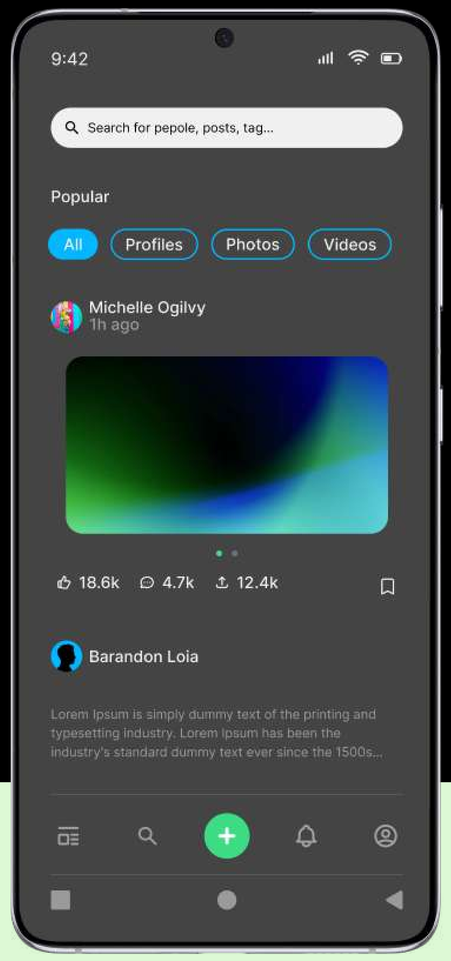
However, as the adoption of Android devices in corporate environments has grown, so have the challenges associated with managing these devices effectively. This is where Android device management comes in to save the day. Android device management involves a range of powerful tools and practices that enable businesses to securely and remotely oversee their Android devices.

Android device management provides businesses with the ability to enforce policies, deploy applications, and ensure data protection across their Android device fleet. It also enables organizations to make their devices business-ready for diverse use cases.

Scalefusion

Android Device Management Modes

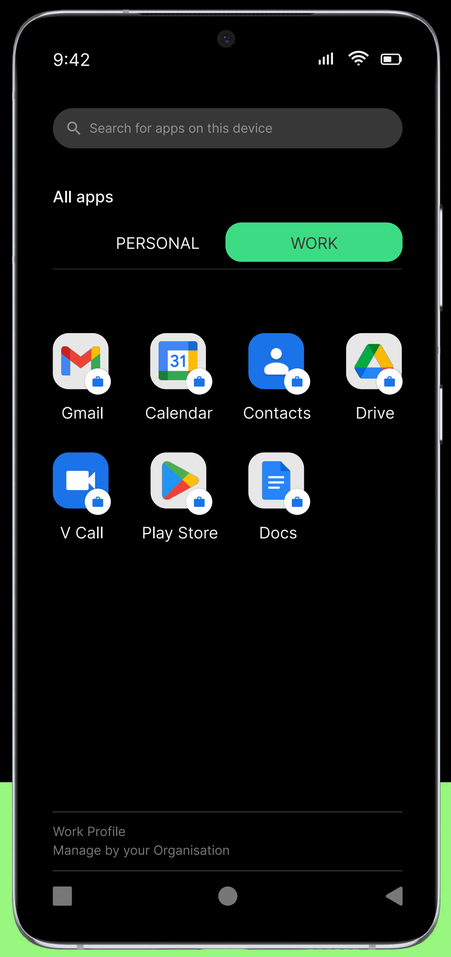
Before we delve into the powerful features that an Android device management solution offers, let’s first have a look at the various device management modes available within an MDM.



1

Corporate-Owned, Personally Enabled (COPE)

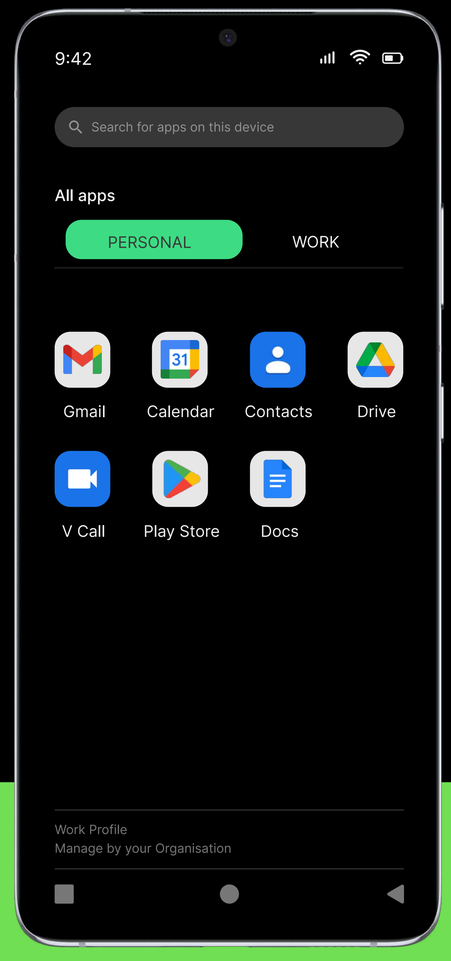
COPE allows organizations to provide employees with corporate-owned devices while still allowing some degree of personal use. IT administrators can create containers on the device, separating the Android work profile from the personal one. This approach strikes a balance between security and employee privacy.



2

Company-Owned, Business Only (COBO)

COBO refers to devices owned by the company and controlled entirely by the IT department. These devices are typically used for specific work-related tasks and have limited access to personal apps and content. COBO offers the highest level of security and control, making it ideal for industries with strict data protection requirements.



3

Bring Your Own Device (BYOD)

BYOD, or bring your own device, is a widely adopted model in enterprises. When employees are allowed to bring their smartphones and mobile devices into the corporate network, they are supporting BYOD. This saves inventory costs and enables organizations to provide business resources on employees' personal devices.

Scalefusion

COPE Mode: The Perfect Balance of Work and Play

Over the last few years, Android has been making regular amendments to the device management ecosystem as a whole, considering the evolving needs of businesses and, more importantly, its employees.

With BYOD enrollment, IT admins can segregate work and personal apps on managed employee devices into separate containers. And while BYOD is great, it might not be the right fit for several organizations. Especially for knowledge workers, organizations must offer flexibility with devices used while also ensuring that the corporate data on those devices is secured.

This is where Company Owned, Personally Enabled Mode comes into play. In COPE mode, employees can use their work devices for personal tasks without compromising security. It's a win-win situation where employees enjoy the flexibility and employers maintain control.

This mode combines work profile benefits with extra security, allowing IT administrators to enforce strict company policies on the whole device while keeping personal data and apps separate and private for users.

Seamless Business Operations with Company-Owned, Business Only (COBO)

This device management mode enables complete control over the devices. It is intended for managing devices owned by the organization. Unlike other management modes, such as work profiles, COBO mode enables organizations to exert control over every aspect of the device, from its applications to its security protocols. It's like being the captain of your device ship.

What sets COBO apart is its arsenal of extended capabilities. In COBO mode, you can fine-tune device settings, enforce security policies with the precision of a laser beam, and optimize device performance.

In a world full of cyber threats, COBO mode is your digital fortress. It can encrypt your devices, set up strong security policies, and even wipe data remotely if things go south. Your data is locked up like a treasure chest, and only you have the key.

Scalefusion

Managing Bring Your Own Device (BYOD) in the Workplace

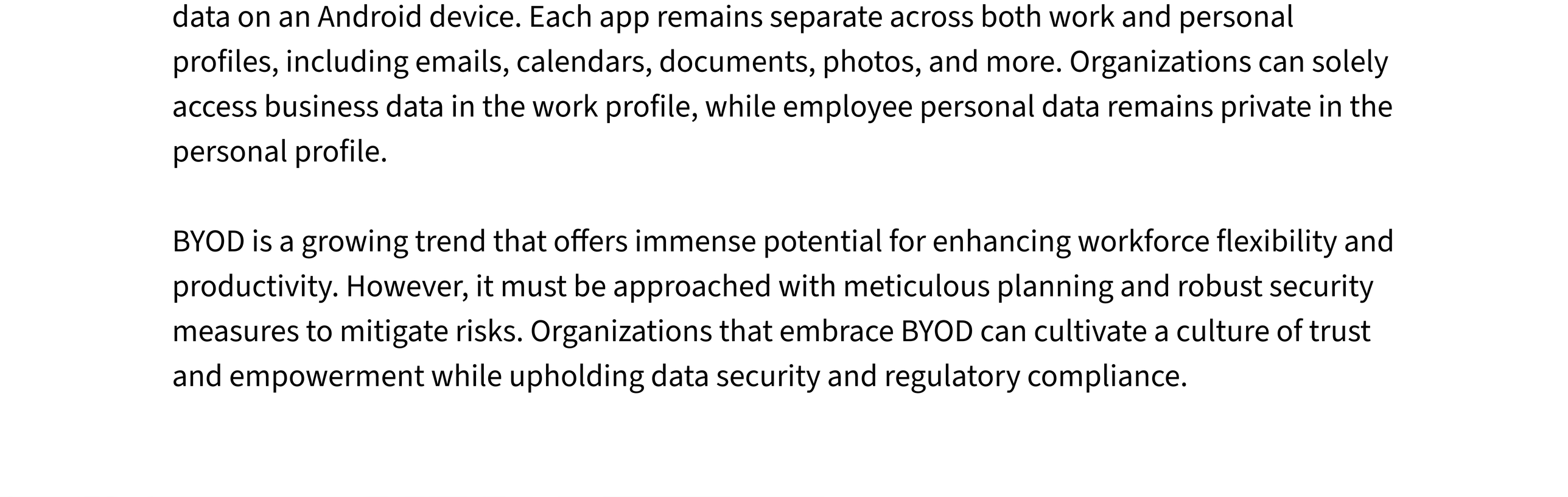
The opportunity to embrace personal devices for work purposes is an enticing proposition that appeals to both employers and employees. Employers are freed from the responsibility of providing work devices, allowing them to cut down on expenses. On the other hand, employees are already well-acquainted with their own devices, enabling them to perform work-related tasks with remarkable efficiency.

Nevertheless, there is a crucial aspect to implementing a successful BYOD policy in the workplace. When introducing personal devices, and potentially personal data, into the corporate environment, IT must address the concerns of data leakage and user privacy.

To ensure the protection of devices and data, IT teams commonly rely on an device management solution that can securely onboard, manage, monitor, and safeguard corporate devices and data.

With Scalefusion UEM for BYOD, you have the ability to segregate personal and corporate data on an Android device. Each app remains separate across both work and personal profiles, including emails, calendars, documents, photos, and more. Organizations can solely access business data in the work profile, while employee personal data remains private in the personal profile.

BYOD is a growing trend that offers immense potential for enhancing workforce flexibility and productivity. However, it must be approached with meticulous planning and robust security measures to mitigate risks. Organizations that embrace BYOD can cultivate a culture of trust and empowerment while upholding data security and regulatory compliance.



Scalefusion

Ways Android MDM Can Boost Your Business

Seamless Device Enrollment Options

Transform Your Devices into Purpose-Built Kiosks

Application Management across Disparate Devices at Scale

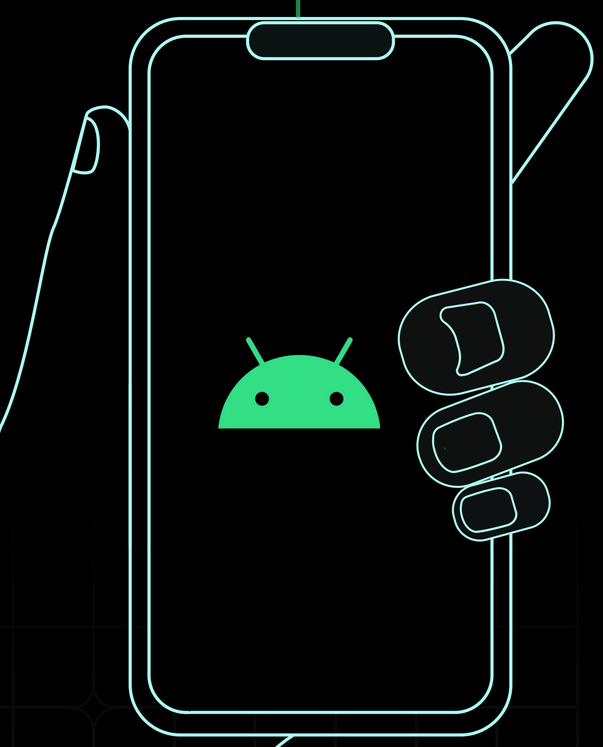
Remotely Control Devices & Troubleshoot Errors

Enhance Your Security Posture

Content Management On the Go

Shared Devices

Location Tracking & Geofencing



Scalefusion

Ways Android UEM Can Boost your Business

Seamless Device Enrollment Options

With the growing number of Android devices in an organization, the first and foremost need comes a seamless enrollment option. In this regard, Scalefusion offers an array of streamlined enrollment options tailored for Android devices:

- **Zero-touch Enrollment:**

Scalefusion provides Zero-touch enrollment methods, including compatibility with Samsung Knox and Android. Rather than individually provisioning devices, you can engage in bulk enrollment, distributing fully managed devices to end users. End users can get a managed device out of the box immediately and start using it for the intended purpose.

- **IMEI-Based Enrollment:**

In just a few simple steps, administrators can upload a CSV file containing IMEI numbers for the devices earmarked for enrollment. This effortless process ensures that a multitude of devices can be enrolled swiftly.

- **QR Code Enrollment:**

Scalefusion offers a seamless QR code enrollment process, allowing users to easily verify their identity by scanning a QR code. This user-friendly and intuitive approach accelerates the enrollment procedure and guarantees a smooth transition to device usage.

- **Email/SMS Enrollment:**

Users are granted the convenience of email or SMS-based enrollment, wherein they receive enrollment credentials via these channels. This ensures secure authentication and an effortless entry point into the enrollment process.

- **Serial Number-Based Enrollment:**

To facilitate the seamless integration of numerous devices, IT administrators can effortlessly upload a CSV file containing serial numbers for large-scale Android device enrollment. This innovative approach closely aligns with IMEI-based enrollment, enabling swift and efficient inclusion of multiple devices.

The ever-expanding array of Android devices within organizations necessitates a sophisticated and flexible enrollment strategy. Scalefusion provides a wide variety of enrollment options to meet this requirement, making it easy to quickly and efficiently integrate devices into an organization's operational framework.

Scalefusion

Transform Your Devices into Purpose-Built Kiosks

In today's digital age, customers have high expectations when it comes to accessibility. They want everything at their fingertips with just a few clicks or taps. Businesses must prioritize seamless customer experience with every interaction. This is where kiosks come into play, unlocking a world of possibilities by offering curated content, interactive interfaces, and targeted applications However, it is crucial to protect customer-facing kiosks from unauthorized access, tampering, and other security threats, especially in retail and hospitality environments.

That's where Scalefusion Kiosk Mode can be a game-changer. With this powerful solution, you can easily transform any of your Android devices into purpose-built kiosks.

By setting a device into kiosk mode using Scalefusion Android Kiosk Software, you can control and restrict access to specific applications and websites, resulting in a focused user experience with enhanced security. There are two types of Kiosk Mode—Single App and Multiple App. Single App Mode means setting an app as the default and making it run all the time on the device. The application set as default takes over even if the device reboots or restarts. On the other hand, Multiple App Mode allows you to select the required apps that will run on the devices. Not only this, but in kiosk mode, you have the capability to control the screen orientation, brightness and hardware keys.

The best part is that achieving all this is incredibly simple with Scalefusion—just a few clicks on the dashboard is all it takes.

Scalefusion

Application Management across Disparate Devices at Scale

What is device management without app management? A mobile device such as Android relies on apps, and it is crucial for administrators to have control over the installation process. With Scalefusion, admins not only have a say but also have the power to decide what gets installed and what doesn't. That’s right, with Scalefusion Application Management, you have the power to permit or restrict specific applications on managed devices, effectively safeguarding users from accessing potentially hazardous or undesirable apps.

Furthermore, you have the flexibility to pre-set app permissions and configurations. Additionally, you can effortlessly install or uninstall applications without any end-user involvement. IT admins can also push their in-house native app through the Enterprise Store.

Content Management On the Go

In today's connected world, employees need constant access to vital enterprise information, no matter where they are or what device they're using. The ability to tap into real-time data fuels quicker and more precise business decisions. As businesses embrace a mobile-first culture, the trend of telecommuting is on the rise, making it essential for remote and mobile employees to have instant access to important company data and documents.

With Scalefusion Content Management, you have the power to effortlessly deliver various files via Scalefusion FileDock. You simply push the FileDock app onto the managed devices and publish content to it, such as documents, images, videos, and more. You can experience the automatic download of these files from the server to the device, eliminating the need for any prompts or permissions. Additionally, you can remotely delete these files, ensuring the utmost security of the device, even in compromising situations.

Enterprises lean on content management as a cornerstone for elevating employee productivity and convenience. It's not just about information accessibility; it's about empowering individuals to work efficiently, irrespective of their location or the device they hold.

Scalefusion

Enhance Your Security Posture

As cybercrimes become vicious, a single security breach can jeopardize the years of hard work you've put into securing your data. While having a security wall is a good start, having a fortified fortress is even better.

With Scalefusion Android device management, businesses have the power to enforce robust security policies across all their managed devices. This includes implementing password requirements, enabling encryption, and establishing access control rules to safeguard sensitive data.

- **Passcode Policies**

When it comes to enterprise mobility or remote working, allowing employees to work outside of the office comes with its own advantages and challenges. One of the biggest challenges businesses worry about is corporate data breaches. A study suggests that 81% of company data breaches are caused by poor passwords. To address this issue, enterprises establish a passcode policy that consists of guidelines to ensure employees create strong and reliable passwords. With the help of Scalefusion UEM, businesses can remotely configure and enforce Passcode Policies on their Android devices. This not only saves valuable IT time but also eliminates the need for manual configuration of passcode policies on numerous devices.

- **Peripheral Control**

Picture a scenario where an unsuspecting employee plugs in a seemingly harmless USB drive into his/her Android device, completely unaware that this innocent-looking drive is actually a Trojan horse housing malicious software capable of infiltrating the entire network. With Scalefusion Peripheral Control, you gain the power to regulate and control all external devices that interact with your device. This includes a wide array of peripherals such as keyboards, printers, barcode scanners, and more. By restricting users from connecting any unauthorized external device to your Android, you can ensure the utmost safety and security for your valuable device.

- **Control Wi-Fi Access**

The convenience of wireless connectivity comes with its fair share of security challenges. Unregulated Wi-Fi access can pave the way for unauthorized users, data breaches, and network vulnerabilities. Scalefusion helps organizations curb this with its network management feature. With this cutting-edge feature, administrators can effortlessly configure devices to automatically connect to pre-approved Wi-Fi networks. By doing so, the risk of network attacks and data breaches is significantly reduced. Plus, here's the best part—the device is seamlessly connected to the secure network without the user even needing to know the password.

- **Certificate Management**

With Scalefusion MDM, you have the incredible ability to revolutionize the deployment of digital certificates on your organization's devices. With Scalefusion Certificate Management, IT admins can simply provision digital identities onto devices without requiring any action from the end users. This means authenticating devices accessing your organization's Wi-Fi network by pushing digital identity certificates through a certificate payload to all managed Android devices.

- **Conditional Email Access**

In the age of ubiquitous connectivity, email remains a cornerstone of modern communication, serving as a conduit for business interactions, collaboration, and information sharing. Yet, in a world where data security is paramount, unrestricted email access can pose risks. Scalefusion’s Conditional Email Access (CEA) is a policy that enables your IT admins to restrict user access to corporate mailboxes if users fail to enroll their devices in the organization's UEM solution. By adopting this approach, organizations empower themselves to strike a balance between unrestricted communication and safeguarding sensitive data.

- ## Shared Devices

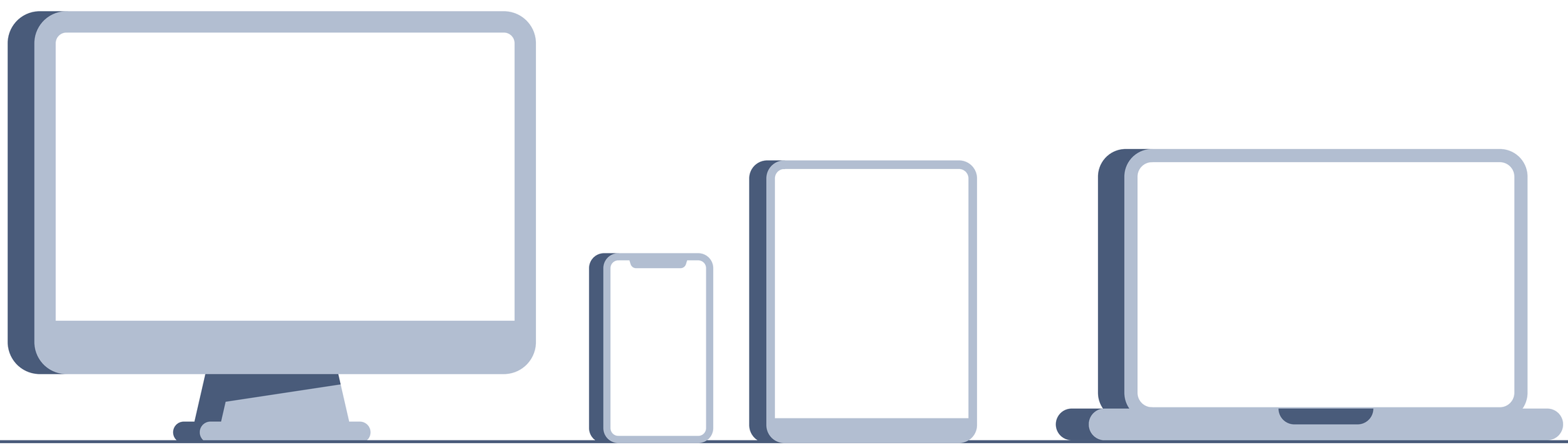
The transformation of IT operations across businesses and industries is out there to be seen.
Let’s be honest. Navigating the complexities of IT operations isn’t the smoothest sail. Sysadmins encounter a multitude of requests every day. From network bugs to a pit of IT tickets—there’s so much to do with a minimal time span. And not only this, IT admins must manage a whole lot of device inventory.

To reduce the current mammoth device inventory that IT admins must manage, shared work devices are the only way out of this maze of IT operations.

Scalefusion enables the sharing of company-owned Android devices amongst employees working in different shifts.

The primary purpose of shared devices is to significantly reduce the costs that companies incur when procuring new devices for their employees or customers. For instance, instead of overseeing 30 separate devices for a team of 30 individuals, shared devices can bring the managed device count down to 15 (when shared between two people) or even 10 (when shared among three). And that's just for one team. You can imagine the impact across the board!

The reduction in cognitive load achieved through shared device management translates to fewer troubleshooting issues, a decreased influx of support tickets, reduced maintenance, and saved time and effort by half.



- **Remotely Control Devices & Troubleshoot Errors**

Remote control, just as the name suggests, empowers you with the ability to effortlessly control and manage your Android devices from anywhere in the world. No matter the geographical distance between the IT team and an employee, remote control bridges the gap and allows for seamless device management. You might be wondering, how is this possible if the IT guy can't physically see the screen of the employee's device? Well, with remote control, you not only have the power to control the device, but you can also gain real-time access to the employee's screen, providing you with a complete visual understanding of their device and enabling you to navigate and troubleshoot remotely with ease. Scalefusion allows you to remotely access Android devices and troubleshoot them, decreasing device downtime. Administrators can detect and fix issues from the comfort of their home or office as they can remotely operate Android devices from PCs. Beyond sheer convenience, remote access significantly reduces IT support and maintenance costs.

- **Location Tracking & Geofencing**

The rise of mobile technologies has completely transformed the way businesses operate. Gone are the days when employees were bound to traditional office spaces, as they can now work remotely to meet the real-time demands of the business. Take frontline workers and field forces, for instance, who often find themselves working from warehouses, construction sites, and retail stores. To ensure optimal efficiency and accuracy, companies equip them with cutting-edge smart devices such as tablets, RFID scanners, and barcode scanners. While enterprise mobility undoubtedly boosts productivity, it is of utmost importance for companies to keep track of these devices used by their remote workforce.

Not only that, if a device used by a remote employee falls into the wrong hands, it could potentially lead to the disclosure of your company's sensitive information, dealing a devastating blow to your business.

With Scalefusion's Location Tracking, you can effortlessly monitor the physical whereabouts of your devices, while with Geofencing, you can define a virtual fence around a geographic location and get alerts when a mobile device enters (or exits) the fenced periphery.

As more and more industries heavily rely on remote devices to handle their ever-increasing workload and assignments, the need to monitor, secure and manage these devices becomes absolutely critical.

Scalefusion

Android Enterprise Security: Scalefusion as a Gold Partner

Google and Android teamed up to recognize MDM solution providers as Silver and Gold Partners based on their technical expertise and robust feature offerings. Any solution provider that has received these badges is an Android Enterprise Recommended Solution, and you can rest assured that they have gone through robust assessments and are validated by the Android Enterprise Team.

Some of the key benefits of using an Android-validated Enterprise solution are:

Robust Feature Set

Any solution receives the Silver/Gold badge only after having a predefined set of features under its armor, which means that you get the maximum device management features and security options with these solutions.

Reliability

Android Enterprise Silver/ Gold partners have undergone extensive training and assessments from the Android team, making them a reliable solution. They have demonstrated excellence in customer support and market success and implemented Android Enterprise technical products and features.

Technical Support

Working with a Silver/Gold partner ensures you will not be left hanging if and when you need technical support. The partners are tested on their technical expertise and are trained by Android before receiving their badge. You can rely on them for your technical requirements and focus on your business goals.

Scalefusion proudly stands as a Gold Partner, a testament to its technical expertise and robust feature offerings. With this badge of honor, you can trust that Scalefusion is committed to providing you with top-tier device management solutions that meet and exceed the highest industry standards. Your devices are in the hands of a recognized and esteemed partner.

Scalefusion

Benefits of an MDM Solution for Android Devices

Now that we have discussed the incredible features of an Android device management solution let's delve into the numerous benefits it brings to your organization.

Ability to Manage a Growing Device Fleet from a Centralized Solution

As your organization grows and your device fleet expands, managing Android devices can become increasingly complex. With an Android management solution, you gain scalability and centralized management capabilities, allowing you to efficiently oversee and monitor a multitude of devices from a single, convenient console.

Enhanced User Experience

An Android management solution empowers your organization to configure devices according to specific user requirements, ensuring a consistent and personalized user experience. IT admins can customize settings, app configurations, and access permissions to enhance user satisfaction and productivity. They can thus take complete control over how and why Android devices are used.

Save Costs

While implementing an Android management solution may involve initial costs, it can lead to significant long-term savings. Effective device management optimizes device usage, reducing the burden on IT support and streamlining workflows. Centralized management and automated routine tasks improve operational efficiency, minimize manual effort, and mitigate the risk of costly errors.

Editor’s Note

And there you have it—we've journeyed through the world of device management for Android, uncovering how it can revolutionize the way your organization operates. From untangling complexities to safeguarding your data, the possibilities are exciting and endless.

But hey, amidst this landscape of options, there's one name that truly stands out—**Scalefusion**. Think of it as your tech-savvy sidekick, your go-to for all things device management. With a hint of magic and a whole lot of innovation, Scalefusion takes your device management game to a whole new level.

Now, the best part? Scalefusion isn't just trusted by your next-door neighbor (although they might love it too!). Industry leaders across the globe rely on Scalefusion UEM to effectively secure and manage corporate devices.And what’s the best way to get a taste of all that Scalefusion’s got to offer? Sign up for a free trial! Enjoy the bliss of easy and efficient device management and security for 14 days.

Scalefusion

Seamlessly Manage Your Android Devices with Scalefusion

Book a Demo

Sign up for Free

Know someone who might benefit from this Ebook?

Share it across!