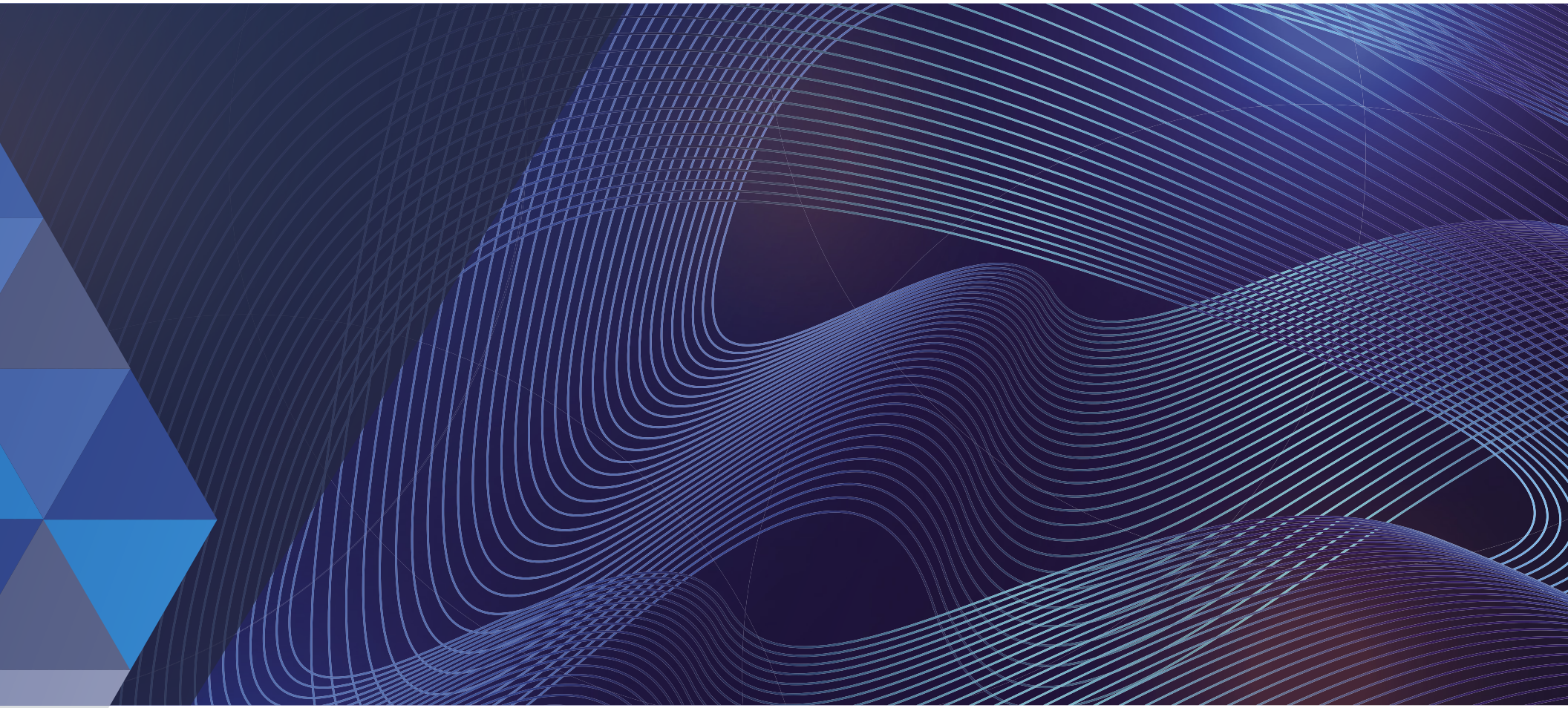
Kaseya®

EBOOK

MANAGING MOBILE DEVICES IN YOUR RMM



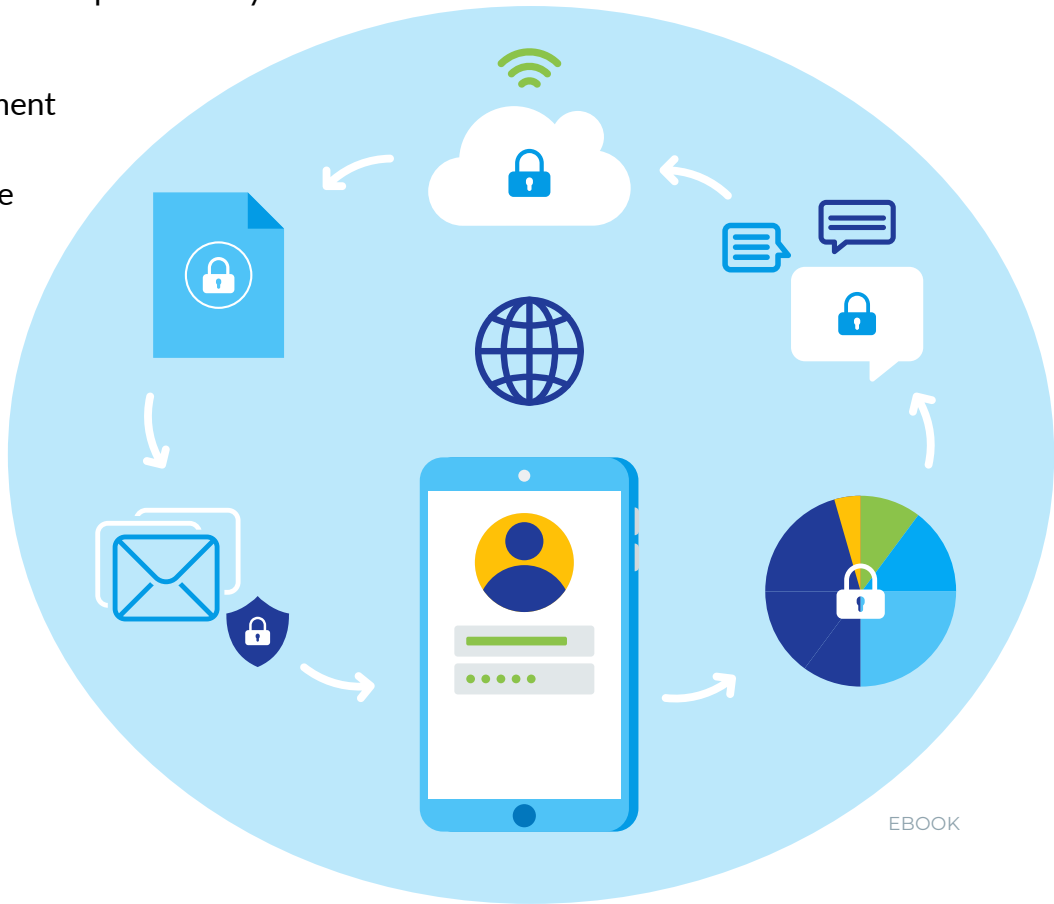
THE FUTURE OF BUSINESS IS MOBILE

These days, business happens anytime, anywhere. More than 90% of corporate employees use at least one mobile app for business while 60% of employees have seen an increase in their personal productivity as a direct result of department-specific apps. Even IT tasks can easily be handled through mobile apps like the Kaseya Fusion app. It goes without saying that mobile devices are clearly an important technology for businesses.

The increased use of mobile devices and apps for business brings with it the increased risk of a data breach or loss due to lost, stolen or hacked devices. In addition, it's becoming more critical to provide a streamlined process for your users to enroll and configure their mobile devices for business use. It's also important to make it easy for employees to get the business apps that will improve their productivity.

Your IT team needs to be able to act quickly to preserve the security of your data and systems with mobile device management (MDM) tools that allow them to set up mobile device usage restrictions and find, lock or wipe devices. They need to be able to maintain compliance with privacy regulations while also enabling employees to get the job done to keep your business humming along.

This makes MDM an important part of your IT services. Managing mobile devices in your remote monitoring and management (RMM) solution is the most efficient way to go about it since you already manage all your other devices (e.g., desktops, laptops and servers) there.



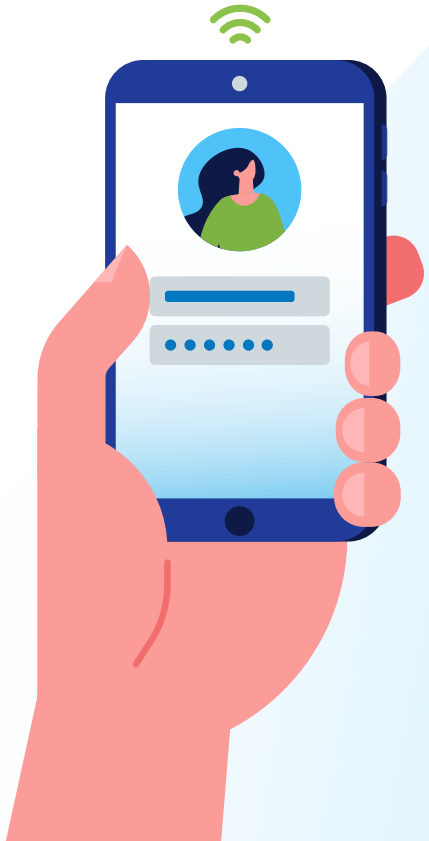
KEY MOBILE DEVICE MANAGEMENT FUNCTIONS

Managing mobile devices for business can be tricky. Your techs need to be able to control device functions and maintain strong security for any mobile device used for business. However, employees want the ability to perform business tasks on their personal devices. Plus, it can be a challenge to get new hires set up on company devices quickly. If a company regularly employs contractors or temps, that can add another layer of complexity to device management.

That's where bring-your-own-device (BYOD) policies come in to play. Many companies have opted to overcome those challenges by creating a set of standards that allows employees and contractors to safely use their own devices for business purposes. By establishing and enforcing BYOD policies, companies can ensure that devices that access business data are adequately protected, especially in industries with complex regulatory compliance needs.

Streamline workflows and reduce headaches for perennially overstretched IT teams by choosing the industry's only unified RMM that brings together all device management into a single product.

The essential features listed below constitute the key MDM functions that IT teams need for stress-free efficient management of both personally-owned and company-owned devices.



Painless Enrollment and Configuration

- Speedy, painless enrollment for phones, tablets and other mobile devices without long connection times or complex adjustments.
- Streamlined distribution and control of configuration profiles means that standard devices can be added and configured in minutes with a few simple clicks.
- Select an MDM solution that works seamlessly with all of Apple's solutions for device management including Apple Business Manager, Apple School Manager and Automated Device Enrollment. If personal devices are used, data separation keeps sensitive data safe and under control.
- Simplify device setup using Android zero-touch. Android Enterprise features let you fully manage company-owned devices or activate a work profile to easily manage business apps and separate data from the user's private space — for example, as part of a BYOD program.

Simple Profile Management

- Simple user template management allows you to configure and manage MDM settings, policies, profiles and apps for entire user groups.
- Rapidly define corporate email, Wi-Fi and VPN settings for individual users, groups or the entire enterprise and deliver over-the-air updates.
- Set up and secure smartphones and tablets in no time at all. Regardless of whether they are organization-owned or employee-owned mobile devices.
- Manage mobile devices and apps anytime, anywhere via the RMM UI.

Strong Data Security

- Easy integrations with security solutions enable IT teams to prevent unauthorized access with secure identity and access management tools.
- In the event of an intrusion or lost device, quickly locate, lock and wipe devices.
- Define passcode requirements and enforce encryption of corporate data
- Set up restrictions on the use of smartphone features such as the camera

Effective Maintenance of Privacy and Compliance

- Easily enforce policies that maintain separation of business and personal data.
- If you deploy an app, it becomes part of the secure business container and may only exchange data with other managed applications.
- Maintain compliance under most major regulations like SCC, CCPA, HIPAA and GDPR.
- Assign policies, certificates and apps easily and push MDM profiles over-the-air to the device.

Agile Mobile App Management

- Empower users (and save the IT team time) by letting them install trusted apps themselves.
- Get seamless provisioning and deployment of apps through a self-service user portal.
- Add recommended apps to a customized enterprise app store to make it easy to direct users to the right apps.
- Prevent unwanted app installation by clearly defining the menu of app choices.

MOBILE DEVICE MANAGEMENT IN YOUR RMM

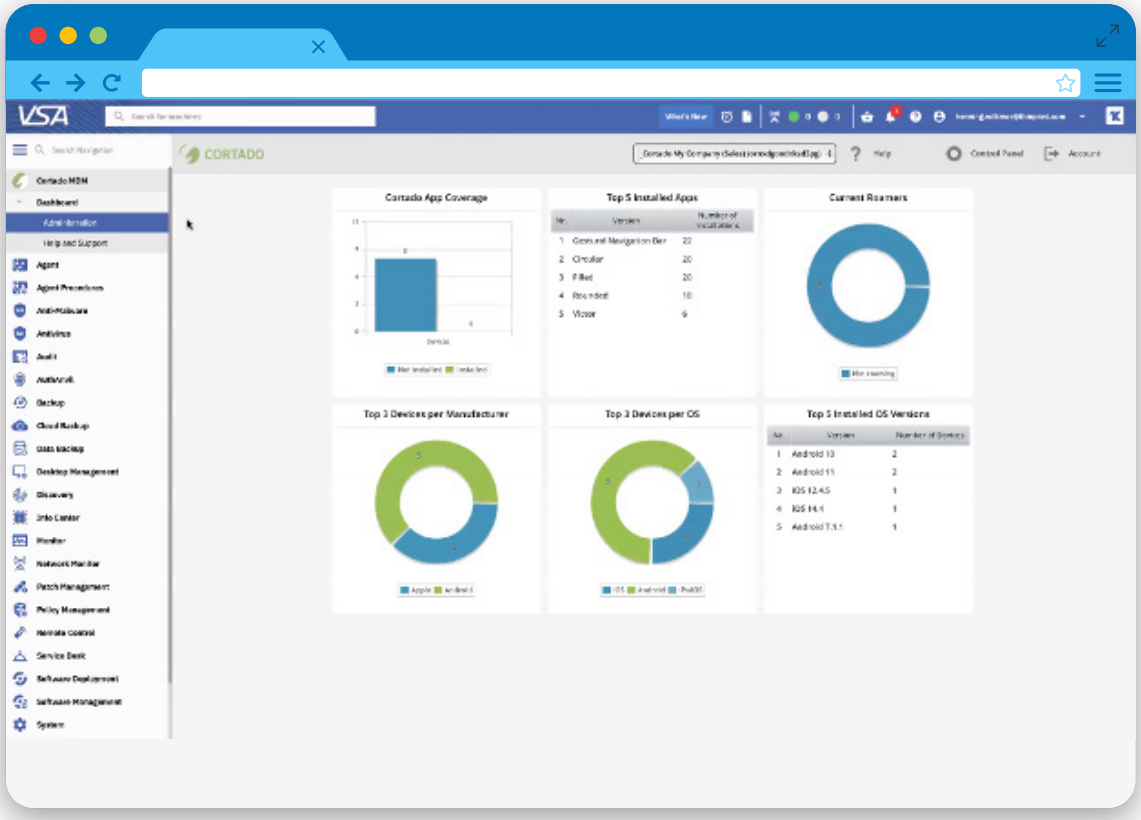
It's time to add dynamic MDM functionality to your RMM. Improve the efficiency of your techs and the security of your business data by enabling your IT staffers to manage all devices from one convenient place. This includes all your traditional endpoints—desktops, laptops, servers and network devices, as well as “Gen 2” devices such as mobile devices.

How It Works With Cortado and VSA

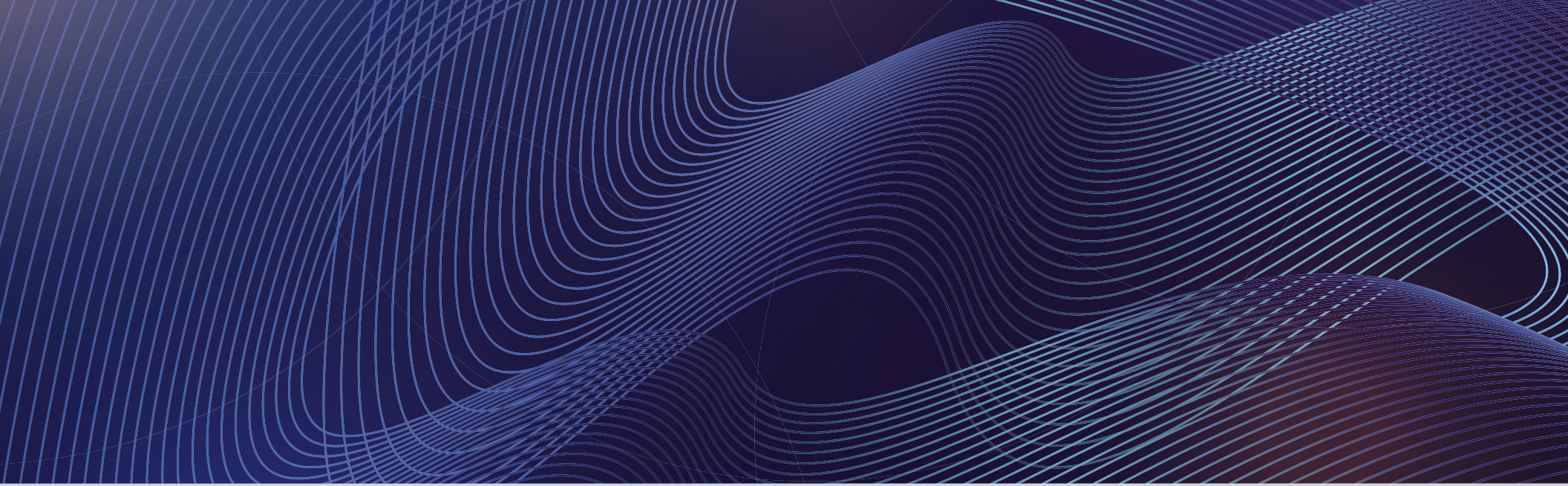
Empower your IT team to quickly handle mobile devices with Cortado MDM and Kaseya VSA, our unified remote monitoring and management solution. Using the Cortado module in the Kaseya Automation Exchange, your techs can easily set up and manage mobile devices in Kaseya VSA.

Just download and import the Cortado MDM module into VSA to enable your IT team to deftly manage mobile devices and keep your business running smoothly anytime, anywhere.

Book a Demo



Cortado MDM Dashboard in the Kaseya VSA UI



About Kaseya

Kaseya is the leading provider of complete IT management solutions for managed service providers (MSPs) and midsized enterprises. Through its open platform and customer-centric approach, Kaseya delivers best in breed technologies that allow organizations to efficiently manage and secure IT. Offered both on-premise and in the cloud, Kaseya solutions empower businesses to command all of IT centrally, easily manage remote and distributed environments, and automate across IT management functions. Kaseya solutions manage over 10 million endpoints worldwide.Headquartered in Dublin, Ireland, Kaseya is privately held with a presence in over 20 countries. To learn more, visit www.kaseya.com.

28062021