Apple device management and endpoint security for fully remote teams

WHITE PAPER

hexnode

Table of Contents

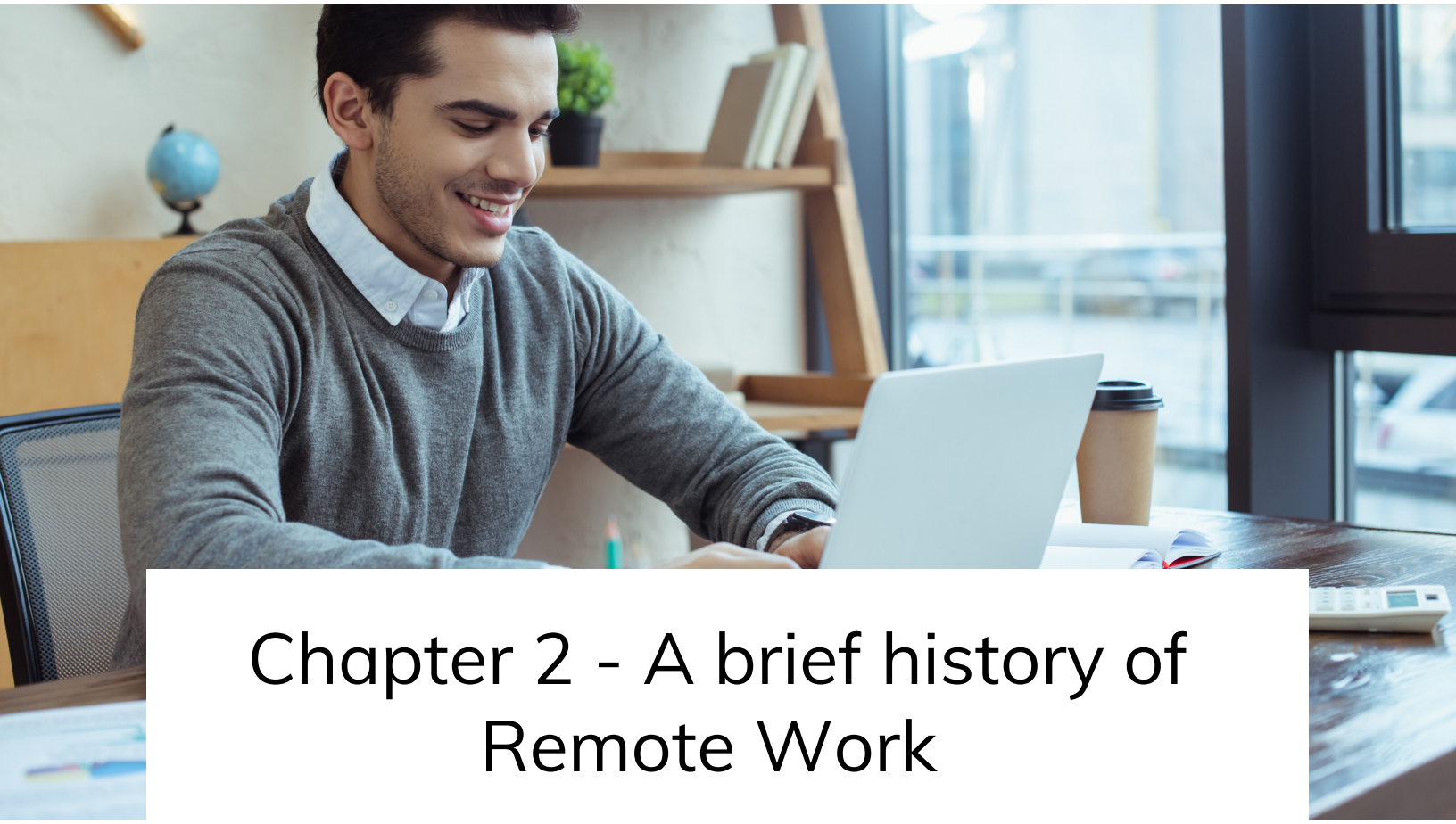
Introduction

The year 2020 saw a seismic shift into remote work. It seems like remote work is here to stay, even when the pandemic is over and we shift to our regular daily lives. Tim Cook, the Apple CEO, recently mentioned that he is impressed by remote work and that some aspects of the new work habits will remain after the pandemic. This echoes the sentiment of companies worldwide, as we have realized that we are able to do a multitude of tasks remotely. Remote work means that the devices with the users would be remote too, and so, remote device management is no longer an option for administrators. With the right tools and resources, it is a lot easier than it sounds. Let's delve into some important aspects of Apple remote device management and endpoint security with MDM.

Chapter 1 - Apple for Work

A mere decade ago, Apple devices were not preferred for enterprise usage at all as Apple did not cater to the enterprise market. Now, in 2021, Apple devices are top-rated for enterprise use. Whether they are personally owned devices or corporate assets, Apple devices have the highest share in the enterprise market. What makes Apple devices so attractive in the business world? The built-in security features, regular OS updates and fixes, ease of deployment and management – all play an important role. The premium design doesn't hurt either.

For bulk deployments, easy management, or even user satisfaction, Apple devices rank high as a popular choice. After switching from Windows to Mac, it was found that 97% of the users reported higher productivity. As a favorite among both admins and users alike, Apple devices play an important role in remote work. The IT admin has the responsibility of securing these remote endpoints and managing them while not compromising the compliance rules of the organization.



Chapter 2 - A brief history of Remote Work

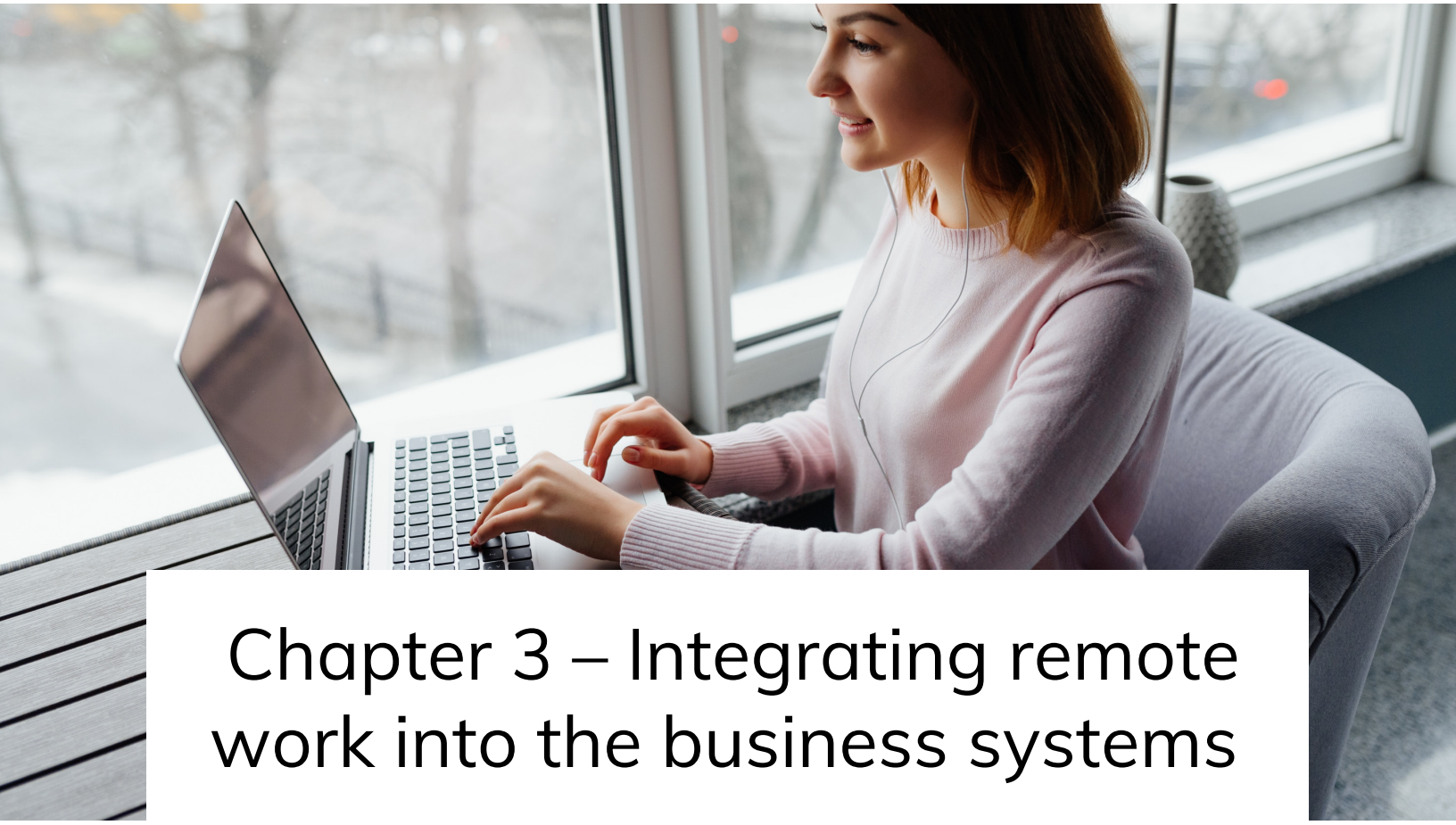
What do we mean by remote work? A remote worker literally works from anywhere outside the traditional office environment. They could be working from home, a library, or even a coffee shop in the opposite corner of the world. Working from home in itself is not a novel concept. In the days before the industrial revolution, working from home was the norm. The industrial revolution saw the shift of work from home to designated workspaces.

In 1983, the internet was born and paved the path for modern telecommuting. Continuous technological advancements and ownership of personal devices increased the relevance of remote work. In 1987, according to The Monitor, the number of remote workers in the US had reached 1.5 million. This number is huge, considering that WiFi was only invented in 1991. The numbers continued to increase gradually, until 2020 where remote work became a necessity rather than a choice. With the COVID-19 pandemic raging over our heads, the companies had to figure out a way to survive amidst all the chaos. Hundreds of millions of people from around the world worked from home.

Is the remote work here to stay?

Businesses that already had remote work support were amongst the least affected ones by the COVID-19 directives. Remote work is hailed as the “new normal” and it seems like it is not going anywhere anytime soon. Many companies have adopted remote work policies. Even companies that had no previous experience with remote work had to take some critical decisions and implement remote work to stay afloat.

What about work after the pandemic? While it would be unrealistic to say that everyone would be working remotely even after the pandemic, we can expect businesses to retain many aspects of remote work. Many employees enjoy working from home, and it has been proven that many tasks can be completed remotely. It will not come as too big a surprise if some companies opt to go fully remote.



Chapter 3 – Integrating remote work into the business systems

Working from home is of course a tough decision to make, but when the global pandemic pushes the stay home directives, businesses are left with no option but to embrace it quickly. The process is relatively easier for organizations that already had remote work policies and practices in place. However, for those who weren't supporting remote work ever before, this rollout is a hard nut to crack. They struggle to support new sorts of workflows and remote initiatives they have no idea of handling.

Most challenging things about working remotely

Establishing a proper remote work strategy with minimal interruption to business is quite a challenging task for enterprise IT. A careless mistake can slow down processes and open up the avenue for breaches. Sniffing Wi-Fi, unprotected devices, unsafe downloads - everything can create alarming security holes. So, each and every app and system need to be individually defended, and it's more likely that all the existing management tasks get augmented with a distributed workforce. Apart from the routine management tasks, the IT team has to find ways to handle tenfold additional chores.

Remote work challenges for IT:

- They have to manage endpoints at different locations and time zones remotely. They should establish full administrative controls and audit capabilities over the entire device.
- They have to manage workers and keep them accountable for remote-heavy operations.
- They have to enable remote collaboration for knowledge sharing and decision making.
- They have to educate employees on the new work procedures.
- They have to resolve all the issues related to virtual communication and ensure that the employees are never out of the loop.
- They have to do remote troubleshooting to handle technology hiccups.
- They have to track employee performance remotely.
- They have to maintain corporate security and remain compliant with general security standards and data privacy regulations.
- They have to provide remote access to information.
- Lack of face-to-face supervision demands additional supervision tools.
- They have to establish new rules of engagement.
- They have to allow a little privacy if it is expected by the employees, for instance, in the case of personal devices. They also have to ensure that easing privacy concerns never affect enterprise security.

Whether as a safety precaution or as a short term mandatory norm, remote work will be there for some more time and though we hope to return to something normal, the way we work will never be the same. Whatever the case, it is necessary to put adequate infrastructure to support businesses and employees working from home.

The essential remote work checklist

Setting up a successful prolonged remote work strategy might sound like a complicated task, but with the right foundation established, anyone can get started far more quickly. Foreseeing, analyzing and avoiding all the issues at the beginning itself can help businesses smoothly integrate remote work into their existing systems. Here are some considerations towards instituting an ideal remote work strategy for any business:

- **Keep an inventory of the devices that the company allow employees to take home for work**
  Knowing what all devices are leaving the office with the employees for remote

work is an essential first step. The organization should keep a list of company assets employees taking with them and make sure that they are in proper working conditions before allotting them for remote work.

- **Know what kind of device is ideal for remote work**
  This may solely depend on each of the company's work processes, the company's readiness to allow personal devices for work and the criticality of the tasks employees are handling. The company should have a clear idea of what type of devices should be allowed for each section of employees to work. Thoroughly understand the security aspects related to each kind of device before allocating personal, COBO, or COPE devices for remote work. Be sure that everyone has the right devices to fit their needs. Outright prohibiting personal use and going for COBO devices is the ideal way to go if you have huge security concerns. Anyways, whatever be the kind of device the organization has to support, be sure that the devices never represent uncontrolled risks to enterprise security.

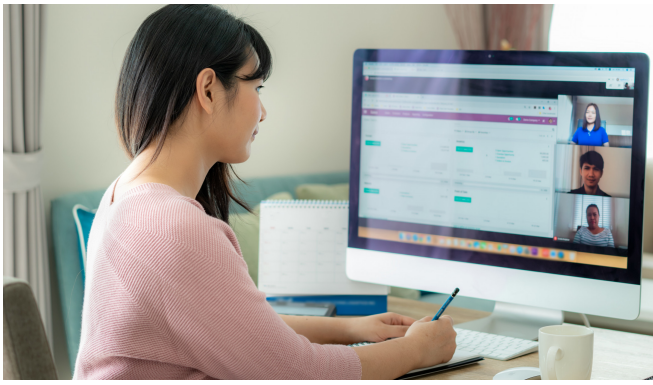
- **Onboard employee owned devices**
  Take utmost care if the organization is allowing personal devices for work. This step might have already been done by an organization that had prior support for BYOD policy. Before onboarding, carefully check the device for vulnerabilities and make sure that the device is apt for work purposes.

- **Provide access to essential resources**
  Give employees access to all apps and data necessary for work but be sure to limit access to anything unproductive. Restrict the use of any apps or content that may distract the employees during their working hours. Also, prevent access to unnecessary websites to make sure that the employees are never surfing the net and using social media during work hours.

- **Set up a line of communication and encourage virtual collaboration**
  Adopt a virtual collaboration tool to properly communicate with the employees working out of the office. A good setup to communicate back and forth is vital for discussing work, informing employees on essential matters, and ensuring that everyone is up to date with their work. And the employees being in self-isolation will be having important concerns to convey the employers back.

- **Ensure that employees are practicing proper security etiquette**
  Most basic security measures are more often overlooked. Be sure to keep employee habits secure and mandate strong password protection, data encryption, data backup, installation of anti-malware protection, prevent downloading applications, and all other methods to protect the devices and data from insider and outsider threats.

- **Remotely monitor employee activities**
  Track employee activities and monitor remotely to evaluate their performance. This strategy works well in keeping the workforce engaging and responsible all the time. Remote monitoring devices is also a good security practice to potentially stop any suspected cyber-attacks and other illegal activities.



- **Establish a management strategy**
  Opting for a UEM solution with remote management features is an ideal step towards managing your devices and users. UEM provides a centralized platform to secure endpoints and data across the entire business network and comply with regulations. They also provide options to configure devices hands-free with little to no involvement from the users.

- **Have an idea of what works well for your team**
  Keep track of what is working and what isn't working for your team's remote work operations. Everyone might not be equally productive while working remote rather than working with the team face-to-face. Be practical with what you can realize remotely but be sure to make necessary adjustments to accomplish everything possible to drive productivity as well as employee satisfaction.

Chapter 4 - Preparing Apple devices for remote work

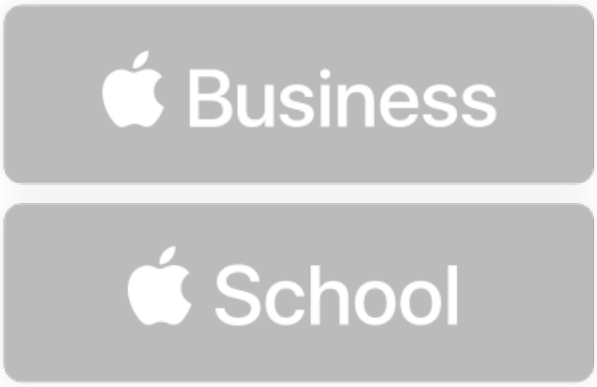
There is no dearth of methods to implement remote work. With the abundance of tools available, it is a task that can be implemented even by a beginner in device management. The distinguishing factor between a beginner and an expert would be how they realize remote work and the ease of device management. Fortunately, if your organization is already implementing a Mobile Device Management (MDM) solution for the Apple devices, the chances are that these devices are already ready for remote work.

Why should you use an MDM for Apple device management?

Remote or not, Apple device management is a cakewalk if you deploy the correct MDM solution. A Mobile device management solution like Hexnode allows you to configure and deploy devices on-the-air, update software and app settings, ensure compliance with the organizational policies, or even remotely wipe or lock the devices in the event that the devices are lost. There is little that the admin cannot do with the MDM integrated with tools like Apple Business Manager or Apple School Manager.

Getting Started

As the popular saying goes, well begun is half done. Apple provides all the right tools. All you need to do is exploit it to its maximum potential. The very first step is to integrate your Apple Business/School Manager account with your MDM solution. This helps in easy and no-touch device deployment. The admin can also easily distribute and install the applications remotely on the endpoints using the ABM/ASM integration.



Device Onboarding

There are different methods for onboarding an Apple device. If it is a corporate device going to be used by the remote workers, the recommended way to go about it is Automated device enrollment. Popularly known as the Device Enrollment Program (DEP), this Apple service allows you to enroll the Apple devices right out of the box without ever touching the device.

Steps to follow for Apple no-touch enrollment:

- Buy the business devices directly from Apple or an authorized reseller.
- Login to your Hexnode account. Integrate Apple DEP with Hexnode.
- Assign a default DEP configuration profile.
- Sign in to your ABM/ASM portal. Add the devices using their serial numbers.

Often, employees use their personal devices to access company resources. Securing these devices while respecting the privacy of the user is a fine balance. It would not be feasible to enroll these devices with Apple DEP. For such devices, it would be better to opt for User enrollment. The enrollment requests can be sent to the end user either via email or and SMS. The user can then enroll the device with the MDM using their own credentials. The administrators can create Managed Apple IDs in bulk for their employees. Unlike standard Apple IDs, the Managed Apple IDs are created solely for business/educational purposes. The IT administrator manages the services that can be accessed by Managed Apple IDs. By turning on federated authentication, the end-users will be able to use their existing Microsoft Azure AD credentials as Managed Apple IDs.

Content management

For remote work, content management is very important for proper and complete device management. There are two types of applications: App Store apps and non-App Store apps. Deploying App Store apps is easy with an Apple Business Manager or an Apple School Manager account integrated with Hexnode. First and foremost, the apps to be distributed have to be purchased from “Apps and Books” by signing into your ABM/ASM account. These purchased apps would show up for assignment in your Hexnode portal. These apps would get silently installed on the target devices. The non-App Store apps or enterprise apps are often custom apps developed by the organization. These apps can be uploaded and deployed using the MDM solution.

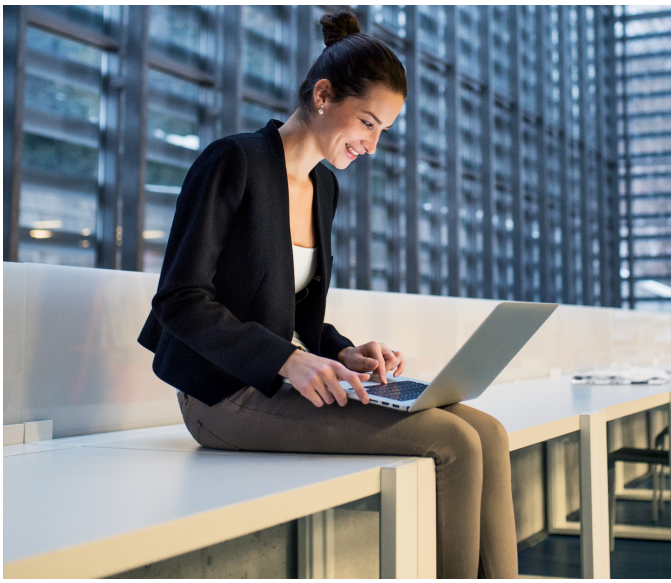
**An interesting feature: App Catalogs

Even within an organization, different departments would have different needs. They would be using different apps. It would be a waste of resources and storage if we were to install the apps on every device without any filter. One way to prevent this is to push a customized App Catalog to the users. The end-user can decide on which apps to install and which to not. Using App Catalogs instead of directly pushing the apps would also establish trust between the end-user and the IT admin. It also builds the user’s self-reliance.

Configuring the settings

A remote worker still has to work. To work properly and efficiently, the right tools and services should be available. Using the MDM solution, you can remotely assign the corporate email account and all the services associated with it, including contacts and calendar. Configuring Exchange ActiveSync accounts on the Apple devices would give secure access to all emails and attachments. It would also sync all the emails, contacts, calendars, and other accounts between the Exchange server and the device even in the absence of a network connection.

OS updates management



Apple releases regular OS and software updates. Not all updates are necessary, while some may be crucial. It would not be very smart to trust the end-user to make the decision on whether to update or not. Using Hexnode MDM, the admin has the following options:

- Notify the user that the software update is available and trust the user to make the decision.
- Download the software update without installing it.
- Forcibly download the update and install it directly after download. If the update was previously downloaded, the installation would begin automatically.
- Download the software update and install it at a later period of time. Apple OS updates can be delayed for up to 90 days.

Security management

Organizations can enforce various security policies to safeguard the endpoints and the data residing on them. With an MDM, different security restrictions can be pre-configured and mass deployed to a group of endpoints dynamically if they seem incompliant with any prevailing regulations. Set extensive and restrictive management policies to combine in-built security tools with MDM security features and push strong measures towards security, including:

- Enforcing strong passwords.
- Encrypting data at rest and in transit and mandating the use of in-built full disk encryption tools like FileVault on Macs.
- Restricting device functionalities like camera, app downloads, iCloud services, copy-pasting, taking screenshots, etc.
- Preventing unwanted browsing and setting up web filters to restricts access to malicious or improper websites.
- Enabling firewalls and mandate the use of VPNs.
- Enforcing MFA authentication to possibly protect work accounts.
- Pushing Apple Business Container restrictions to separate work data from personal data on employee owned devices.
- Controlling, delaying and blocking app and software upgrades.
- Tracking the device's compliance status and automatically removing jailbroken devices if detected.

- Preventing third party access to lost, stolen or misplaced devices by remotely locking, wiping, and tracking the device location. Enabling lost mode to help the device automatically initiate a complete or corporate wipe to save sensitive data.
- Restricting unwanted apps and features by locking down the device to purpose specific kiosk modes.

Device troubleshooting

MDM never let any of the devices become a blind spot in your corporate network. Organizations can always keep track of the geographic locations on the devices and prevent employees from manually turning off the location services. MDM has options to allow monitoring the activities on the endpoints remotely. This feature is particularly handy in situations where employees report malfunctioning devices. Combining the capabilities of remote monitoring and control, the organizations can quickly troubleshoot problematic devices without the employees needing to meet the IT in person, which is impossible too in the current situation. Remote management features with MDM saves a significant amount of downtime as firsthand diagnostics, troubleshooting, and servicing can be done over the air using the remote monitoring and control capabilities.

Offboard devices

It is critical to immediately disconnect any device which doesn't meet up to the corporate standards. MDM provides options to set automatic offboarding to any device non-compliant or inactive device. The IT can remotely offboard any such device marked as non-complaint from the management portal. In a similar way, any device that is no longer in use can also be identified by the enterprise IT and disenrolled from the MDM portal on demand. When an employee working with his personal device leaves the organization, it is essential to offboard the employee device and wipe all sorts of corporate resources from the device to make sure that the corporate data is not accessed or misused data. Upon disenrollment, all the MDM pushed apps and data will automatically get eradicated (provided that option was checked during the app deployment) and for a safer side, the organization can implement a corporate wipe on the device before offboarding.

Mitsogo Inc., Unites States (HQ), 111 Pine St #1225,
San Fransisco, CA 94111
Tel: Intl +1-415-636-7555, Fax: Intl +1-415-646-4151