Switching UEM providers?

Here's what you should know

Migrating to a new UEM isn't easy. Companies must be prepared for all contingencies. The following are the steps companies must adopt to seamlessly switch UEM providers.

IDENTIFY YOUR MOBILE DEVICE MANAGEMENT NEEDS

- The first step towards UEM migration is to review your organization's device management requirements.
- Evaluate your existing UEM solution and assess whether your current policies meet all the device and data security needs.
- Identify areas that need improvement, update your existing policies based on the results you receive, and list out the features you require from the new UEM.

DEFINE YOUR ENROLLMENT STRATEGY

- Determine how you are going to enroll your existing devices into the new UEM.
- Review your organizational requirements and identify the enrollment options your UEM solution supports.
- Ask questions like: Will you need to deploy devices to remote workers? Do you need to manage and secure employees' personal devices? Who is going to carry out the enrollment process – Is it the end-users, or the IT team?
- Once you've reviewed your options, determine the suitable enrollment methods.

BACKUP IMPORTANT DATA

- Migrating devices usually require an initial factory reset. Ensure you backup all the critical business data on to a cloud storage service before wiping them.
- Certain apps sync data on the local storage as opposed to on the cloud. Identify such apps in your inventory and perform the necessary actions to backup important data to the cloud.

IMPORT APPS, RESOURCES AND TOOLS

- Review your UEM app inventory and import apps and resources from your previous UEM solution to the new one.
- Identify your third-party integrations (Directory services, Apple Business Manager, Android Enterprise), and prepare them for transition to the new UEM.
- Take inventory of your profiles and settings, including custom scripts, configuration profiles, security certificates, and more, and transfer them to the new UEM.

PREPARE END-USERS FOR THE TRANSITION

- Admins must notify the end-users about the migration process, so they can plan accordingly.
- They must train the users for the migration process and provide them with necessary support documentation to become familiar with the new vendor.
- Users must be informed prior to critical actions such as device wipe, UEM enrollment/disenrollment, and more, and must be briefed on the notifications and warning messages they may receive during the migration process.

PERFORM A TEST ROLLOUT

- Test your policies and configurations with a small group of devices before officially rolling it out.
- Make sure you've accounted for all use-cases and variables by testing out your strategy multiple times on different configurations. This includes testing on different platforms, on BYOD devices, corporate devices, on older operating systems, newer operating systems, and such.
- Once all the potential issues have been ironed out, deploy your strategy on scale.

MITIGATE SPIKES IN NETWORK TRAFFIC

- When switching UEMs, admins may notice a huge spike in network traffic. This depends to a huge extent on the amount of apps, configuration profiles, and resources that admins have set up for download on end-user devices.
- Admins can reduce this surge in traffic by efficiently scheduling the enrollment process in organizational groups, and by limiting deployment to only the required apps and resources while offering the rest as self-service via corporate app stores.

RECEIVE USER FEEDBACK AND RESOLVE ISSUES

- Maintain a channel to gather regular reports from users and perform troubleshooting operations on potential issues that may arise before, during, and after UEM migration.
- Set up a dedicated support team to identify potential vulnerabilities and resolve issues ASAP. Conduct a survey after the migration to collect user feedback on the new UEM vendor.
- The UEM migration process can be marked successful only after resolving any such issues.