Team Challenge

During the team challenge, attendees working as a team will attempt to deliver a Proof of Concept (PoC) for a real-world scenario and will be challenged in two significant ways. From a technical perspective, attendees will need to both design, scope and implement the PoC. From a soft-skills perspective, attendees will need to pitch the vision for their PoC, explain and defend their design and present their final solution. The teams of attendees will have their presentation and deliverables evaluated by a panel of judges, with recognition being awarded at the end of each day of the event (best PoC pitch, best design, best implementation, etc.) with an overall award for the best solution.

# Scenario for the Proof of Concept (PoC)

Best for Your Organics Company (B4U) manufactures and sells non-toxic cosmetics that also minimize their impact on the environment. They have grown their business into a billion-dollar business by leveraging the network sales model. In network sales, B4U involves non-employee consultants (also called contractors) to sell their products in a person to person way. Best for Your Organics Company is looking to expand their consultant model to contain Basic Consultants and Platinum Consultants. Basic Consultants have a low cost to enter the business and low monthly expenses. Any Consultant can select to become a Premium Consultant under the new model by paying higher monthly fees. In return they will receive discounts, early access to new products and an enhanced set of software tools to support their business.

Each consultant runs their own small-scale version of the business, including purchasing product inventory, performing product demonstrations, marketing on social media, handling sales both “on the spot” during in-person events and by driving clients to their personalized B4U website, recruiting and nurturing and building a team of consultants beneath them to help scale their personal organization’s sales force. Consultants start off as individuals but may end up growing their organizations to 100s or 1,000s of consultants beneath them. Some organizations are narrow and deep, with only a few legs directly reporting to the original consultant but having many consultants in the chain below the. Other organizations are wide and shallow, having 10’s to 100’s of direct reports, each only a few levels deep.

They originally purchased Office 365 E5 and completed a migration to the service. However, they have recently upgraded to Microsoft 365 E5 for their 500 full time employees and need a plan to improve the security of their devices and data. Part of this initiative was due to an increase in mobile and remote work of these 500 users. Due to this, they have the following initiatives to implement:

1. They need to prevent sensitive information such as Personally Identifiable Information (PII) and financial information from being shared outside their Microsoft 365 environment.
2. They want to ensure that employees can’t download files from SharePoint to computers that aren’t owned by the company.
3. When employees are working from personally owned mobile devices, all corporate data should remain secure and users shouldn’t be allowed to use their mobile device to share the data with just anyone.
4. When employees are working from corporate owned devices (both Windows 10 and mobile devices) the company should maintain complete control over the entire device
5. Leverage multifactor authentication to reduce potential security breaches

# Current state of B4U

* All computers are running Windows 10, joined to AD, and hybrid joined to Azure AD
* Mobile devices owned by the company are all Android Devices
* Mobile devices owned by employees may be iOS or Android
* Employees can use home computer to access Microsoft 365, however, they shouldn’t be allowed to download any files from Microsoft 365
* Data that contains PII and Financial information is currently stored in SharePoint Microsoft 365
* Assume B4U has Microsoft 365 E5 licenses already purchased and assigned to all 500 users.

# Your Challenge

B4U clearly has a lot of big ideas to improve the security of their data and protect against data leaks. However, they need help implementing these ideas and a strategy for how it can be accomplished.

The final solution must meet the following requirements:

* Full management of company owned Windows 10 devices, including remote wipe capabilities
* Full management of company owned Android devices, including remote wipe capabilities and blocking things such as backup to the Google cloud and installing non-approved apps
* Limited, web based only access to Microsoft 365 (SharePoint) from any non-company owned PCs
* If sign-in risk is deemed highly suspicious, require MFA
* Employee-owned mobile devices can access corporate data; however, it must be limited to only certain company approved apps (you can’t copy/paste from email into a text message, and corporate data should be backed up to Google Cloud or iCloud). Users can still install apps and maintain control over their personal data without fear of corporate control over personal data on their personal devices. It must just not mix with corporate data.
* Data that contains PII and financial information should be labeled and blocked from being shared with to any external user or email address, including any personal email address of employees.
* Email attachments must not be able to be saved to devices that aren’t company owned (they need to stay within the company’s ability to control and monitor)
* While people are free to converse in Teams, they shouldn’t be able to share PII within a conversation in Teams.

Your task is to determine the Microsoft 365 features and functionality that must be implemented in order to achieve the requirements. Define services, policies, conditions, and settings that need to be used to achieve all these reequipments should be defined.

Good luck!

# Resources to help you get started

The following resources have been made available to help you quickly get started with your PoC:

|  |  |  |
| --- | --- | --- |
| Item | Description | Location |
| Article Link | Microsoft Endpoint Manager documentation | <https://docs.microsoft.com/en-us/mem/> |
| Article Link | Microsoft Intune Device Management | <https://docs.microsoft.com/en-us/intune/remote-actions/device-management> |
| Article Link | Microsoft Intune app management | <https://docs.microsoft.com/en-us/intune/apps/app-management> |
| Article Link | Azure AD Conditional Access | <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/> |
| Article Link | Conditional Access: Session | <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session> |