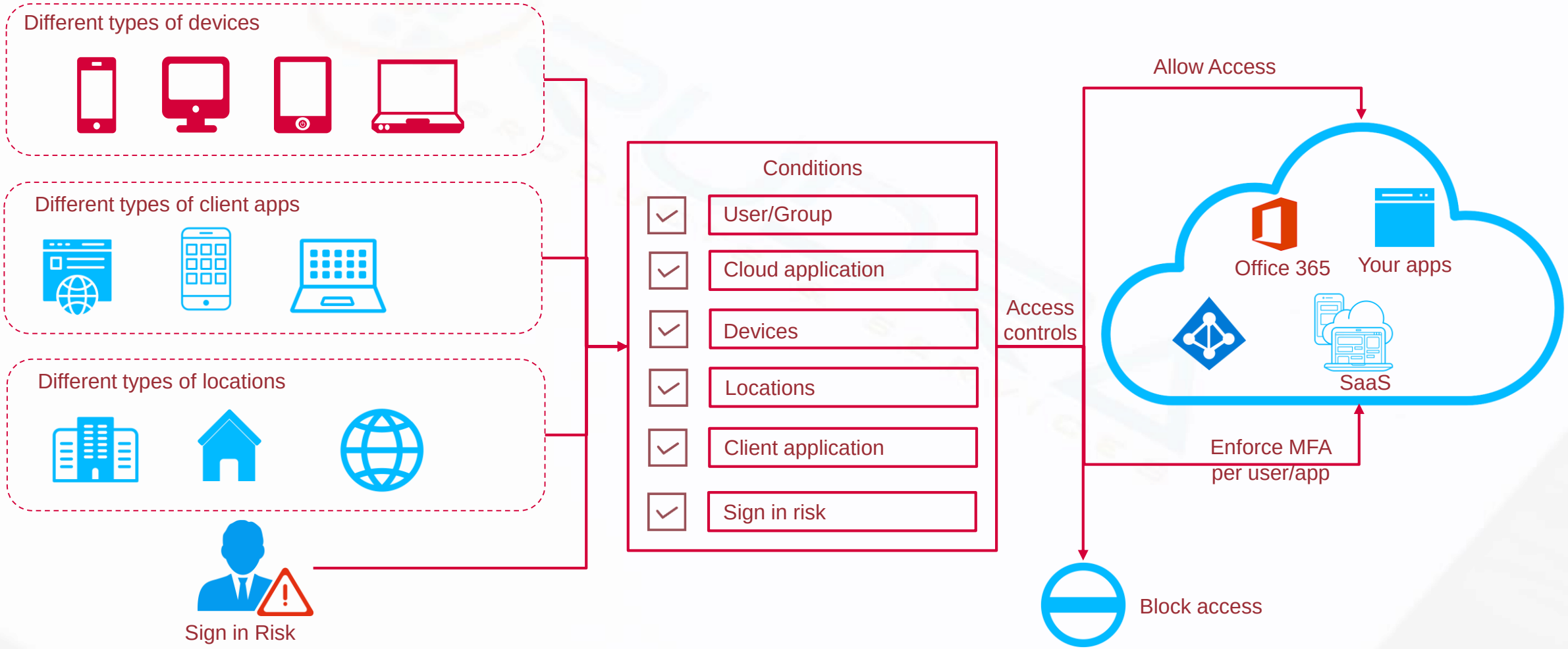
Introduction to Conditional access

What is Conditional access?

Conditional access is a capability of Azure Active Directory using which you can implement automated access control decisions for accessing your cloud apps that are based on conditions.



Conditional access key points

How conditional access policies applied?

- All policies are enforced in two phases:
  - In the first phase, all policies are evaluated and all access controls that aren't satisfied are collected.
  - In the second phase, you are prompted to satisfy the requirements you haven't met. If one of the policies blocks access, you are blocked and not prompted to satisfy other policy controls.

What you should be careful about?

- For all users, all cloud apps:
  - Block access
  - Require compliant device
  - Require domain join

Plan your conditional access deployment

- **Draft policies**
  - With a conditional access policy, you define a response (**do this**) to an access condition (**when this happens**). Define every conditional access policy you want to implement using this planning model.
- **Plan polices**
  - What outcomes you want to achieve?
  - Block access, Require MFA, Require managed access, Require approved client apps
- **Test policies**
  - You should evaluate your policy using the What if tool
  - Apply a policy to a small set of users and verify it behaves as expected.
  - Apply a policy to all users only if necessary.