Microsoft Entra ID Access Management Capabilities

Vlad Catrinescu

Microsoft MVP | Independent Consultant

@vladcatrinescu | VladTalksTech.com | YouTube.com/@VladTalksTech

Overview

Role-based access control

Microsoft Entra Conditional Access

Security defaults in Microsoft Entra ID

Introduction to Role-based Access Control

Role-based Access Control

A role is a set of pre-packaged permissions for one or multiple applications

- Entra ID
- Microsoft 365
- Power Platform
- And more

Entra ID has multiple built in roles

- Users can be assigned one or more roles

The Global Administrator

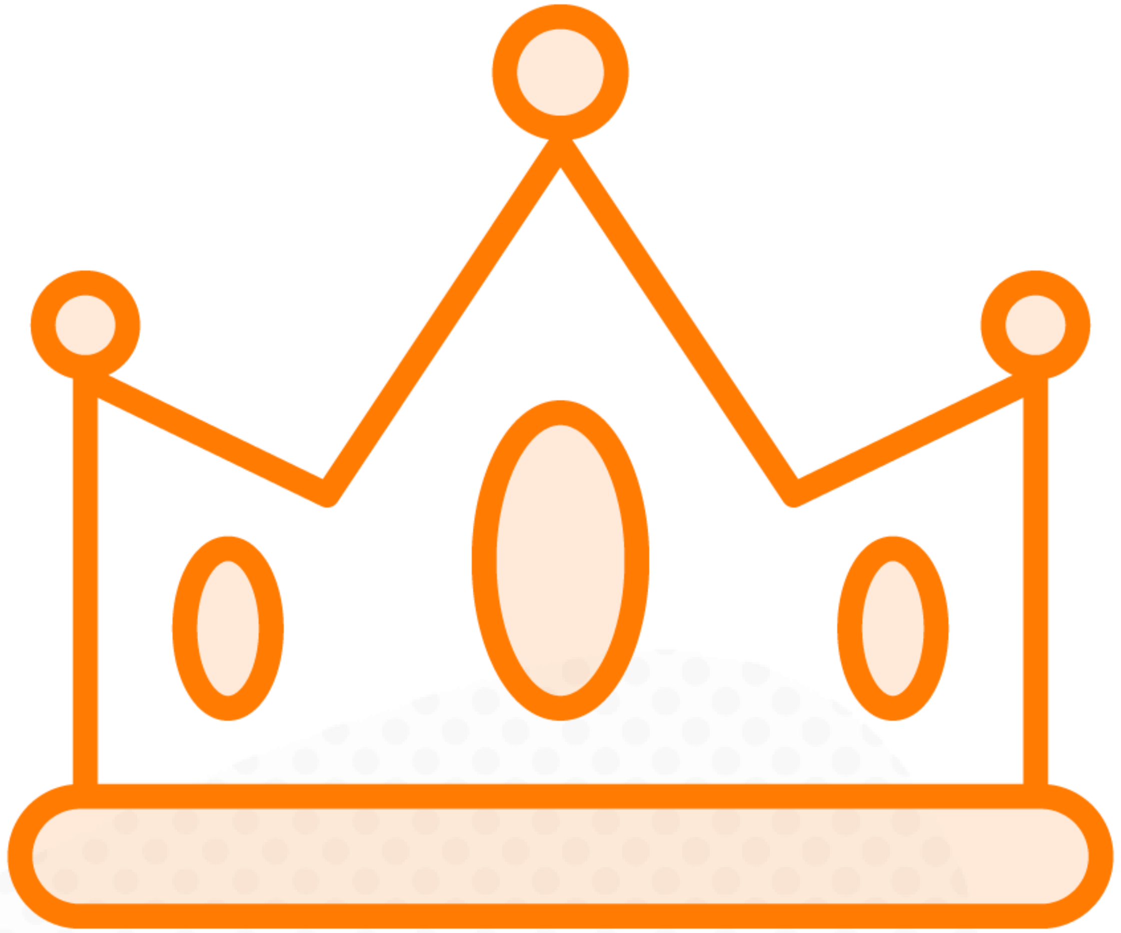
Global administrator has full control over the tenant

- Users
- Licenses
- Billing
- Etc.

Global admin doesn’t give you access to content directly

- But gives you the ability to grant yourself access

Limit the number of administrators with this role



Application Administrative Roles

SharePoint admin

Microsoft Teams admin

Exchange admin

Power Platform admin

Search admin

Fabric admin

Multiple Roles per Application

Applications can have multiple roles

Microsoft Teams

- Teams service administrator
- Teams communication administrator
- Teams devices administrator

Microsoft Search

- Search admin
- Search editor

User and License Management Roles

User admin

Resets user passwords, creates and manages users and groups, including filters, manages service requests, and monitors service health

License admin

Assigns and removes licenses from users and edits their usage location

Helpdesk admin

Reset password, force users to sign out, manage service requests, Monitor service health

Billing admin

Makes purchases, manages subscriptions, manages service requests, and monitors service health

Multiple Reader Roles

Global reader

- Read access to everything in the tenant including admin centers

Message center reader

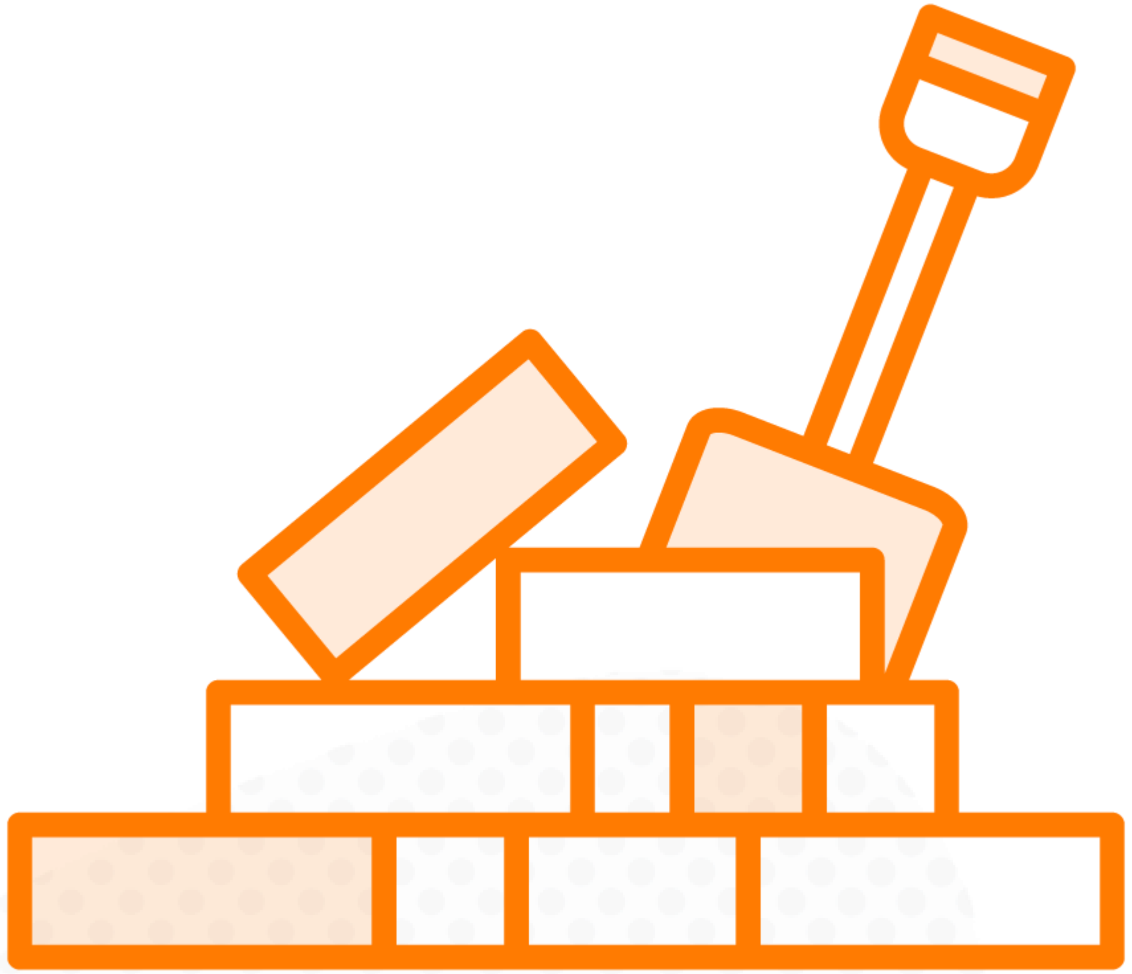
Security reader

Reports reader

Custom Roles

Entra ID allows you to create custom roles

Useful if pre-built roles don't meet needs of the organization



Best Practices

Only grant the access user need

- Just Enough Access (JEA)
  - What’s the least privileged role I can assign for this admin to do their job

Limit the number of global administrators

- Check your current global admins and see if any can be assigned less powerful roles

Microsoft Entra Built-in Roles

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

Demo

Overview of available roles

Analyzing role permissions

Microsoft Entra Conditional Access

Microsoft Entra Conditional Access

Additional layer of security between authentication and authorization

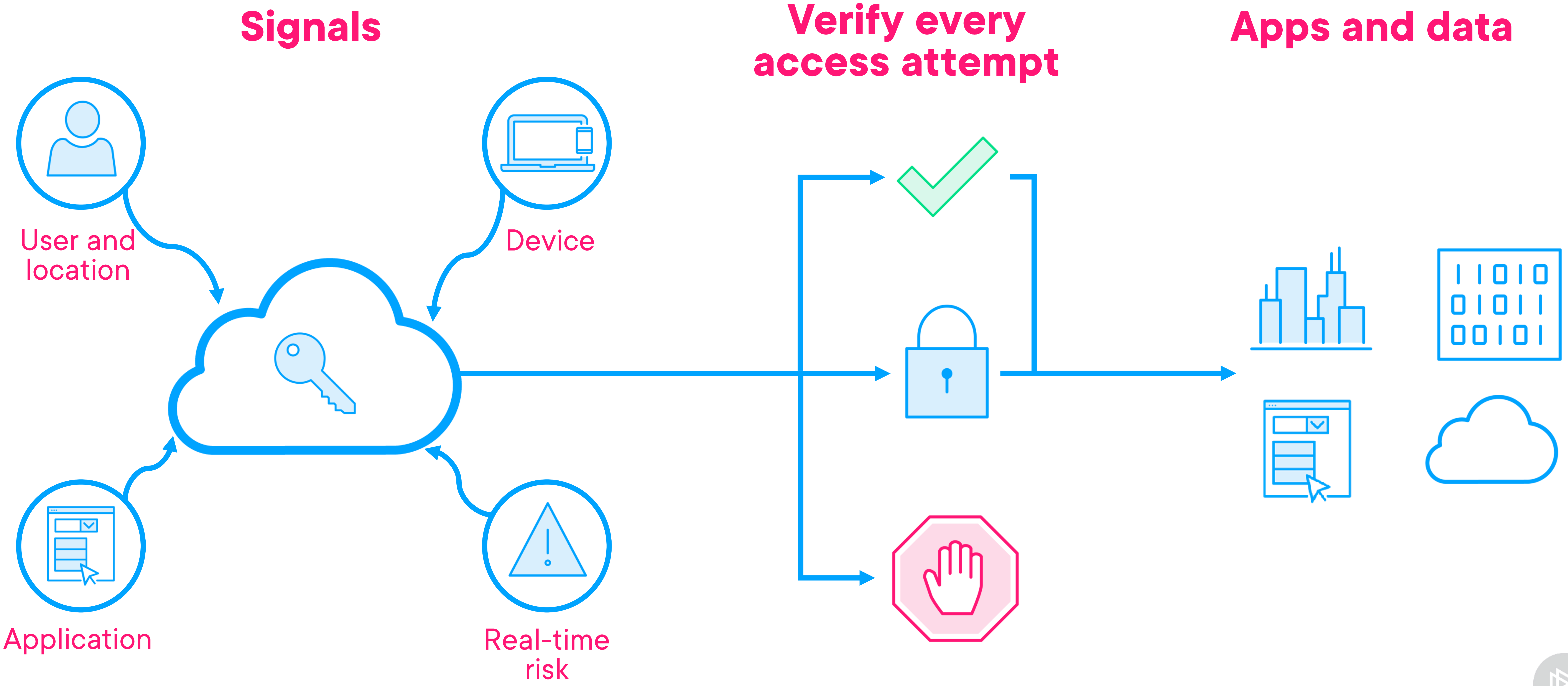
Conditional access policies evaluate every access attempt and decide if

- Grant access
- Block access
- Require one or more conditions to be met
  - Require MFA
  - Require device to be marked as compliant

Conditional access is implemented trough policies created by each organization

- Can be applied to users or applications

Microsoft Entra Conditional Access



Signals

Verify every access attempt

Apps and data

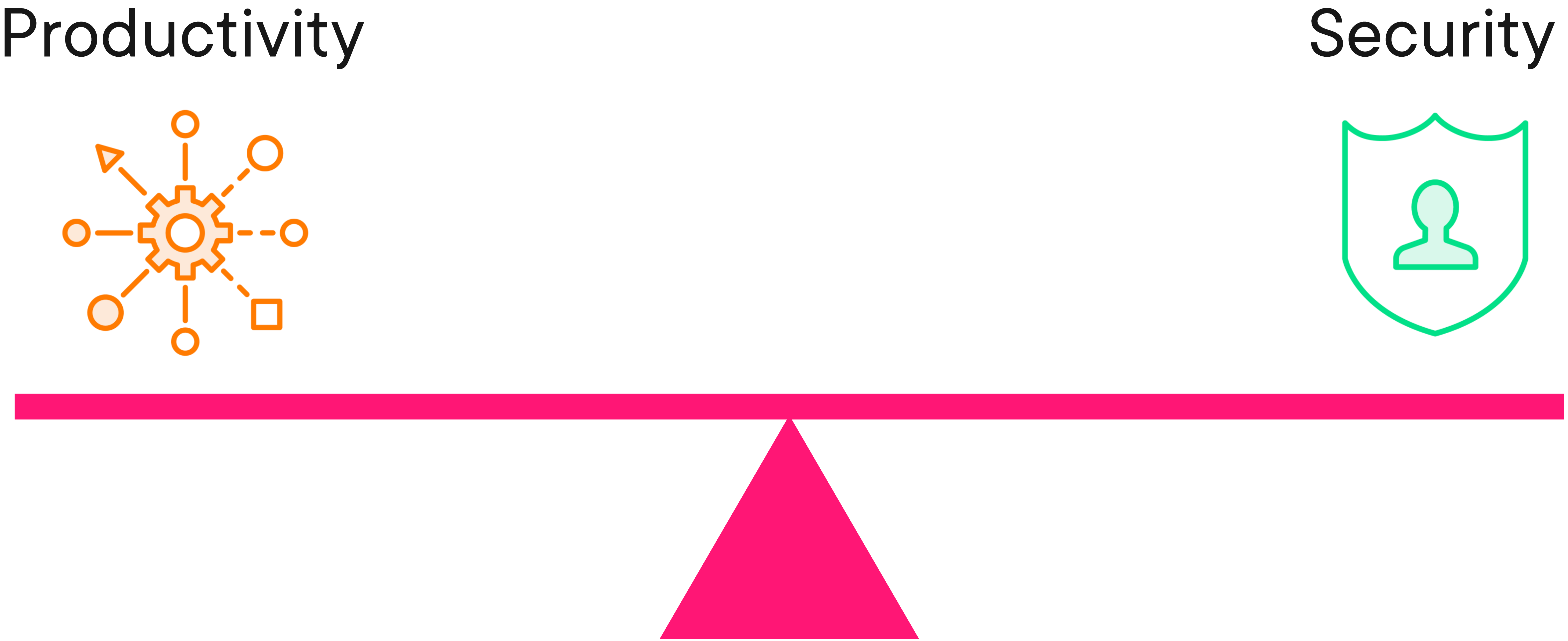
User and location

Device

Application

Real-time risk

Conditional Access Allows You to Find a Balance



Productivity

Security

Conditional Access Signals

User or group membership

Location
(Based on IP)

Device

Application

Real-time sign-in risk detection

User risk

Example Conditional Access Policies

If a user wants to access SharePoint Online from a trusted network after authenticating on a compliant device

- Grant access

If a user wants to access a collaboration SharePoint site from an untrusted network

- Prompt MFA

Any user that logs in that has an administrative role

- Prompt MFA

Example Conditional Access Policies

A user authenticates at home on a managed device and trusted network and browses the intranet

- Allowed
  - Same user tries to access the SharePoint site where employee files are stored
    - Ask for MFA prompt

A user tries to access SharePoint Online from another country

- Block access

Demo

Microsoft Entra Conditional Access

Security Defaults

Security Defaults

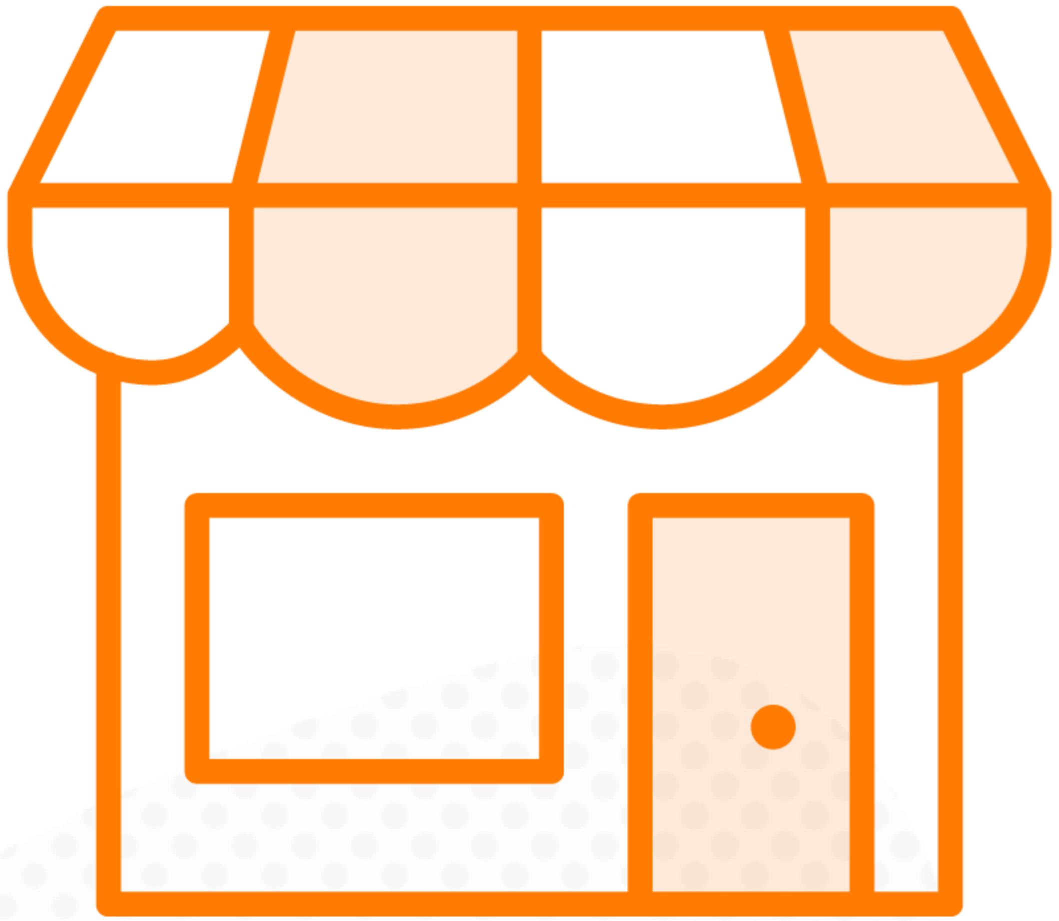
Security defaults are an easy way to enable security mechanisms recommended by Microsoft

- Requiring all users to register for multi-factor authentication
- Requiring administrators to perform multi-factor authentication
- Blocking legacy authentication protocols
- Requiring users to perform multi-factor authentication when necessary
- Protecting privileged activities like access to the Azure portal

Who’s It For?

Targeted at organizations that do not have premium Entra ID licenses or limited IT

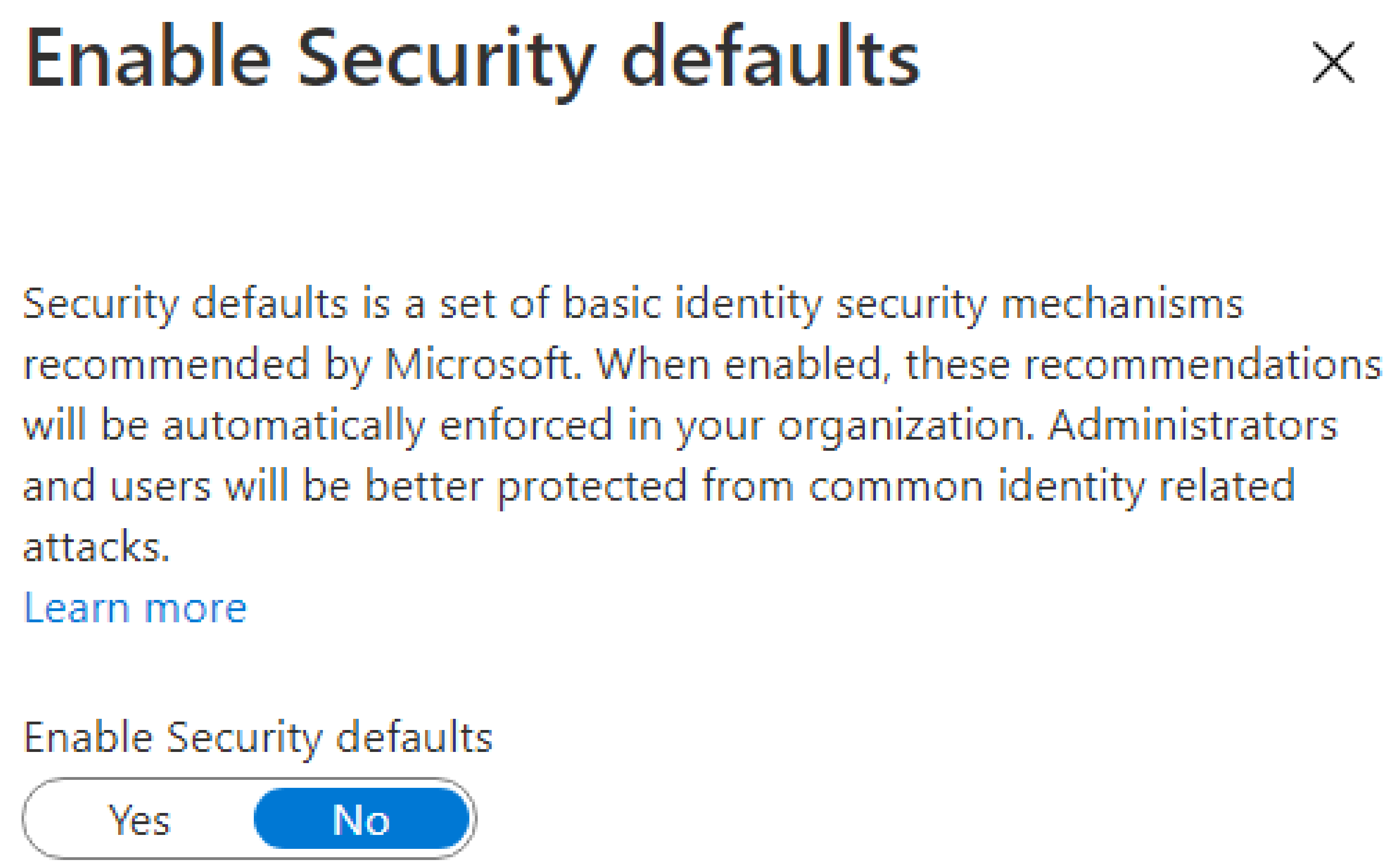
Organizations with premium Entra ID licenses or advanced requirements should use Conditional Access



One click enable

Microsoft has already enabled them on newly created tenants

- Most existing tenants will automatically get it unless they opt out



Enable Security defaults

Security defaults is a set of basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity related attacks.

Learn more

Enable Security defaults

Yes [✓ No]

Module Conclusion

Role-based access control

- Pre-packaged permissions for one or multiple applications
- Multiple Entra ID and application roles
- Custom roles

Microsoft Entra Conditional Access

- Additional layer of security between authentication and authorization
- Helps you find balance between productivity and security

Security defaults

- One click experience to enable recommended security mechanisms
- Built for orgs without premium Entra ID

Up Next:

Microsoft Entra ID Identity Protection and Governance Capabilities