Introduction to Azure AD Privileged Identity Management (PIM)

Introduction

Azure Active Directory (Azure AD) Privileged Identity Management (PIM) is a service that enables you to manage, control, and monitor access to important resources in your organization.

Using PIM, you can manage both AD roles and Resource roles

Using PIM

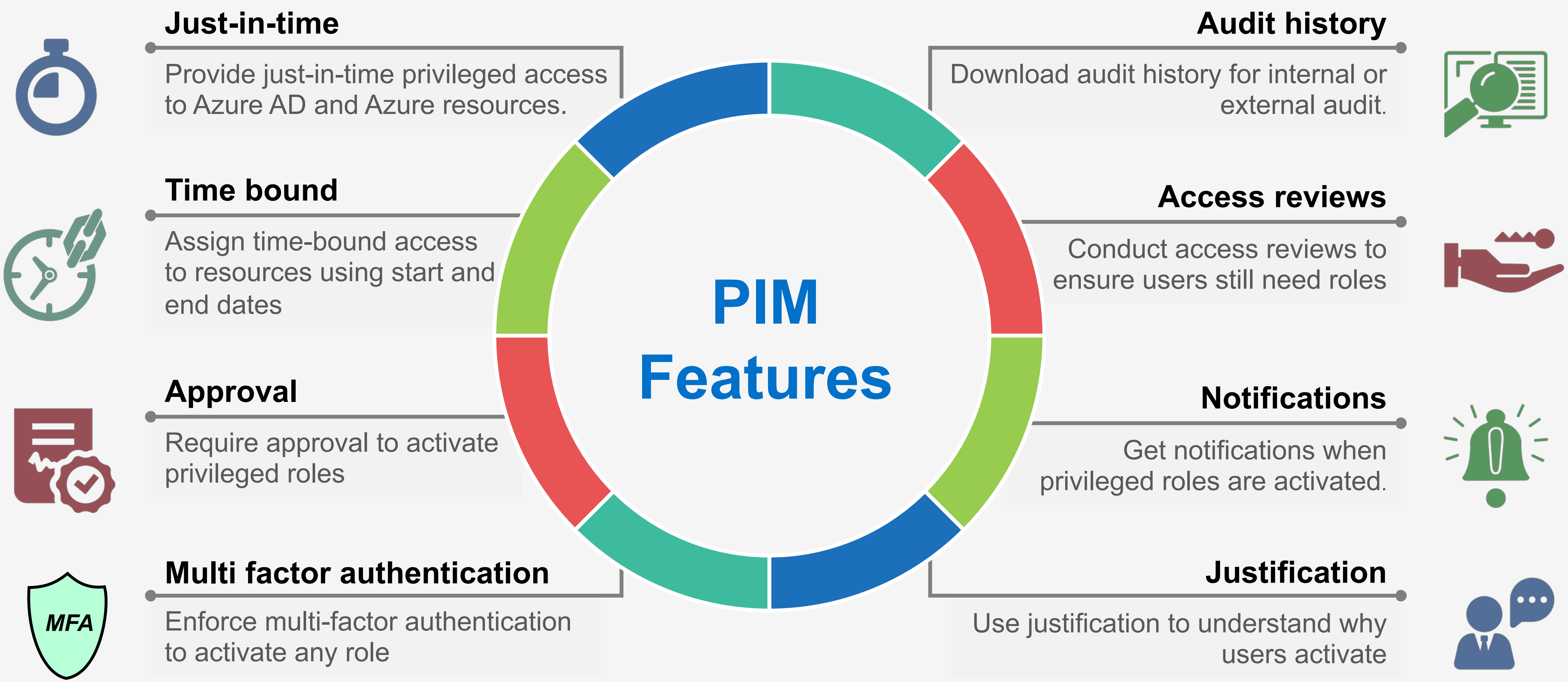
- Manage risk - Secure your organization by enforcing the principle of least privilege access and just-in-time access.

- Address compliance and governance - Deploying PIM creates an environment for on-going identity governance.

- Reduce costs - Reduce costs by eliminating inefficiencies, human error, and security issues by deploying PIM correctly.

Features of Privileged Identity Management

RUDRA
PRODUCTS & SERVICES



PIM Features

Just-in-time

Provide just-in-time privileged access to Azure AD and Azure resources.

Time bound

Assign time-bound access to resources using start and end dates

Approval

Require approval to activate privileged roles

Multi factor authentication

Enforce multi-factor authentication to activate any role

Audit history

Download audit history for internal or external audit.

Access reviews

Conduct access reviews to ensure users still need roles

Notifications

Get notifications when privileged roles are activated.

Justification

Use justification to understand why users activate

Implementation steps of PIM

RUDRA
PRODUCTS & SERVICES

Enable PIM

To enable PIM, you first need to provide consent. First person to enable PIM will be automatically assigned with Security Administrator and Privileged role Administrator.

Access Review

Role assignments become "stale" when users have privileged access that they don't need anymore. In order to reduce the risk, carry out frequent access reviews

Protect Role Assignment

Eligible users assigned to PIM must elevate to use the privileges granted by the role.

Monitor & Alerts

Utilize PIM's built-in alerting functionality to better safeguard your tenant. Set up recurring access reviews to regularly audit you organisation's privileges identities