

# M365 security, de mogelijkheden binnen uw licentie

Joeri Rotthier, Inetum-Realdolmen

# Joeri Rotthier



**Technical consultant**

Microsoft 365 Certified



Joeri.rotthier@inetum-realdolmen.world

## Office 365 E3

# Why move to M365?

- Office Apps
- OneDrive
- SharePoint Online
- Teams
- Exchange Online Plan 2



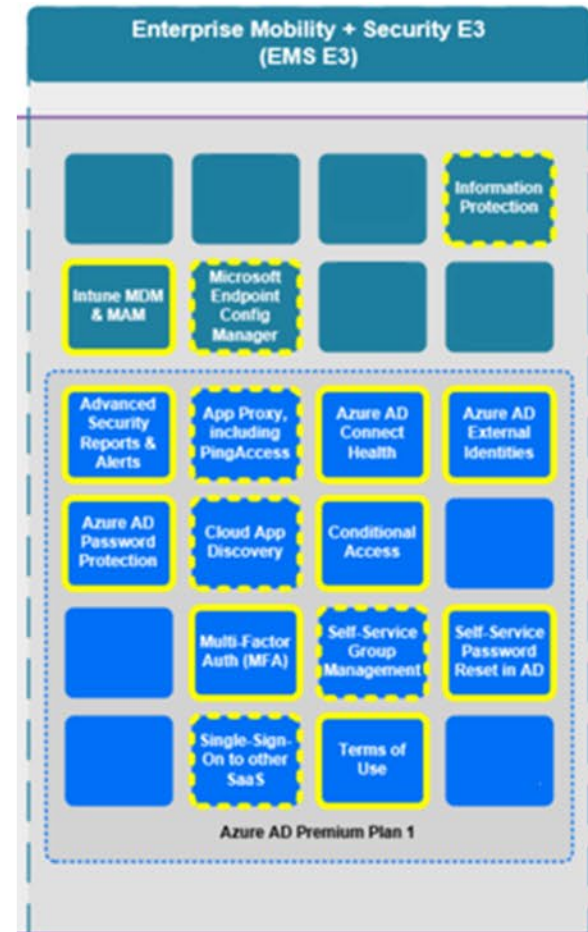


Microsoft 365 E3

# Enterprise Mobility and Security

Why most customers purchase this license?

- Azure AD P1
  - MFA
- Client Management
  - SCCM
  - Intune



Don't overlook these benefits!

- Azure AD P1
  - Conditional Access
  - External Identities
  - Password Protection
  - Self Service Password Reset
- Mobile Application Management
  - Application Configuration
  - Application Protection
- Information Protection

Microsoft 365 E3

# Risk-Based Controls



Microsoft Endpoint Manager helps ensure cross-platform device controls in your zero-trust strategy



Adapt in real-time to changes in device health



Leverage Microsoft 365 cloud to evaluate risks



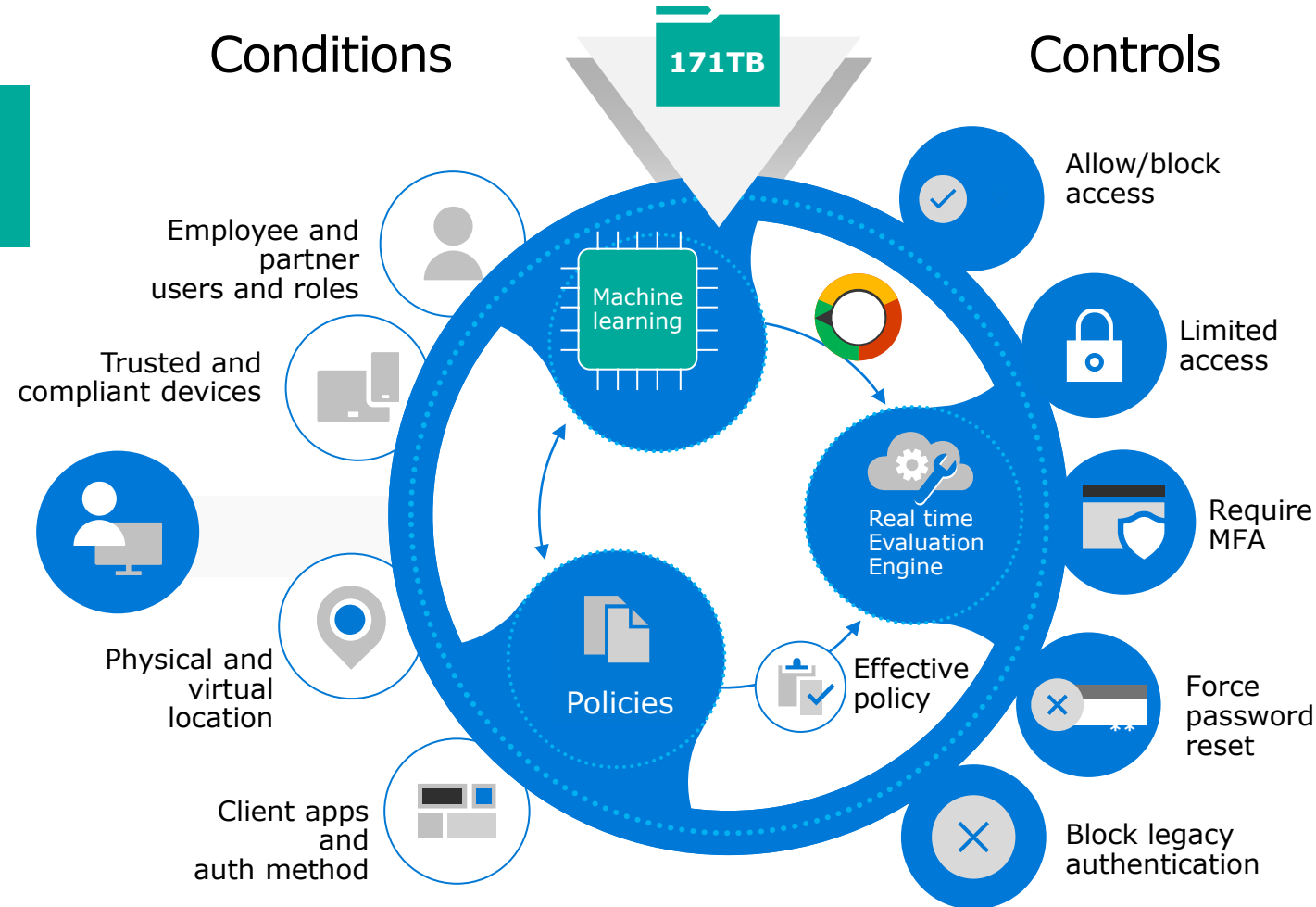
Protect Office365 data on unmanaged devices



Extend native platform security to meet all use cases



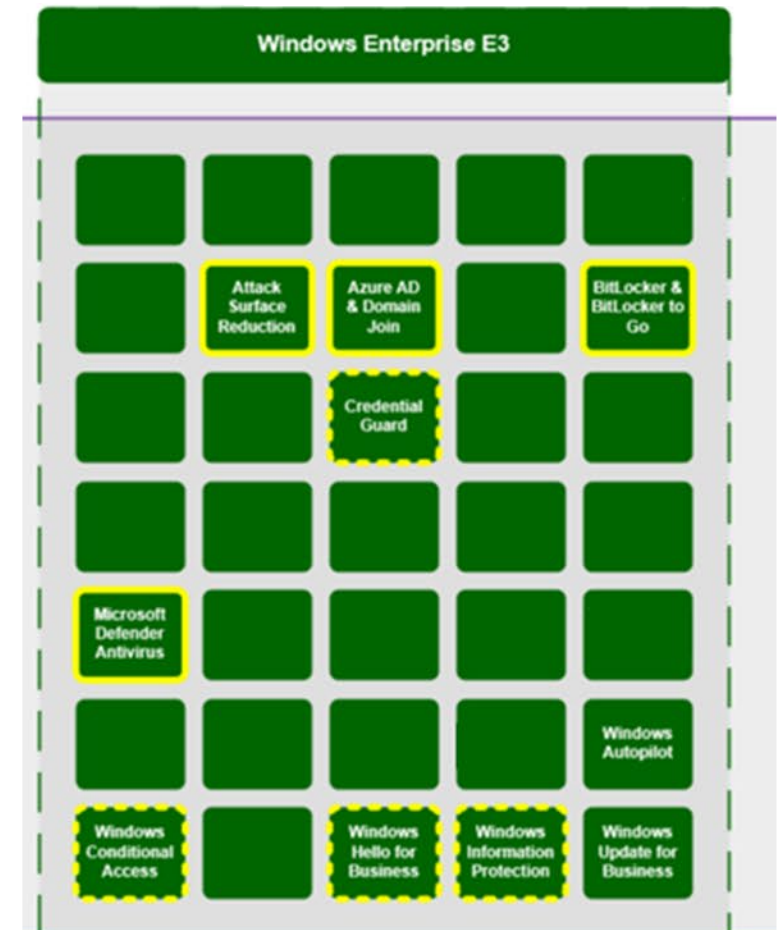
Factor in third party risk and compliance signaling



Microsoft 365 E3

# Windows Enterprise

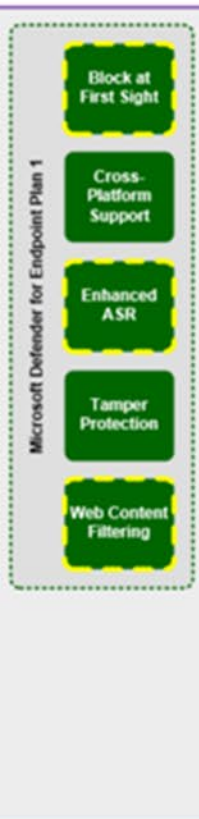
- Enterprise Upgrade License
- Azure AD & Hybrid Domain Join
- Windows Security
  - Managed by Intune
  - Hello for Business
  - Defender Antivirus



## Microsoft 365 E3

# Additional Security Benefits

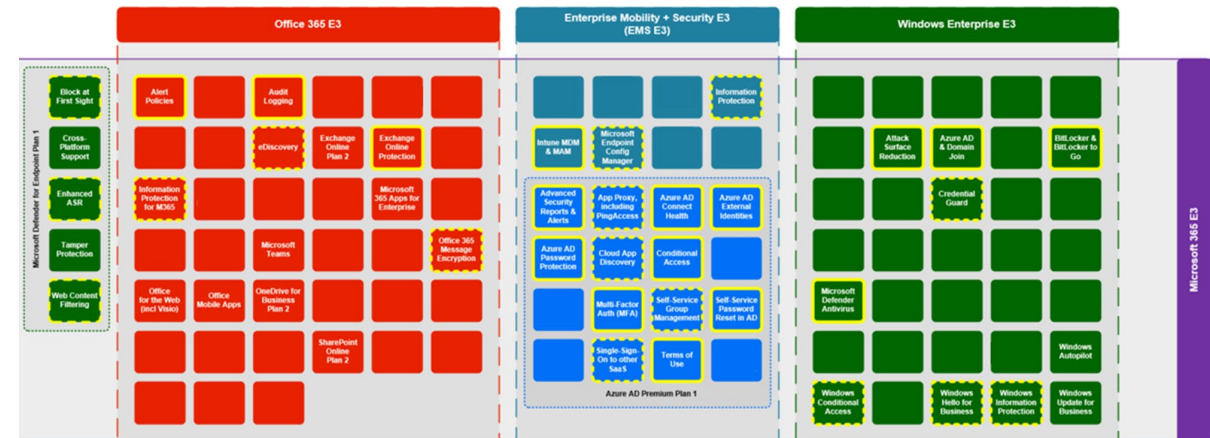
- Microsoft Defender for Endpoint Plan 1
  - Block at first sight
  - Cross Platform Support
  - Enhanced Attack Surface Reduction
  - Tamper Protection
  - Web Content filtering



## Microsoft 365

# Prioritize and Plan Features

- All possible security features should be evaluated and/or enabled, but...
  - Resources are limited
  - Activities, sequence, dependencies, and end-user impact must be considered
- In general: 80/20 principle
  - 80% or more OOTB or minor fine-tuning: Audit Logging, MFA, Conditional Access Policies, ...
  - 20% or less customized: Data Classification and DLP scenarios, business application-specific, ...



**Fundamental Must-Have Feature**  
Plan and Implement as Soon as Possible

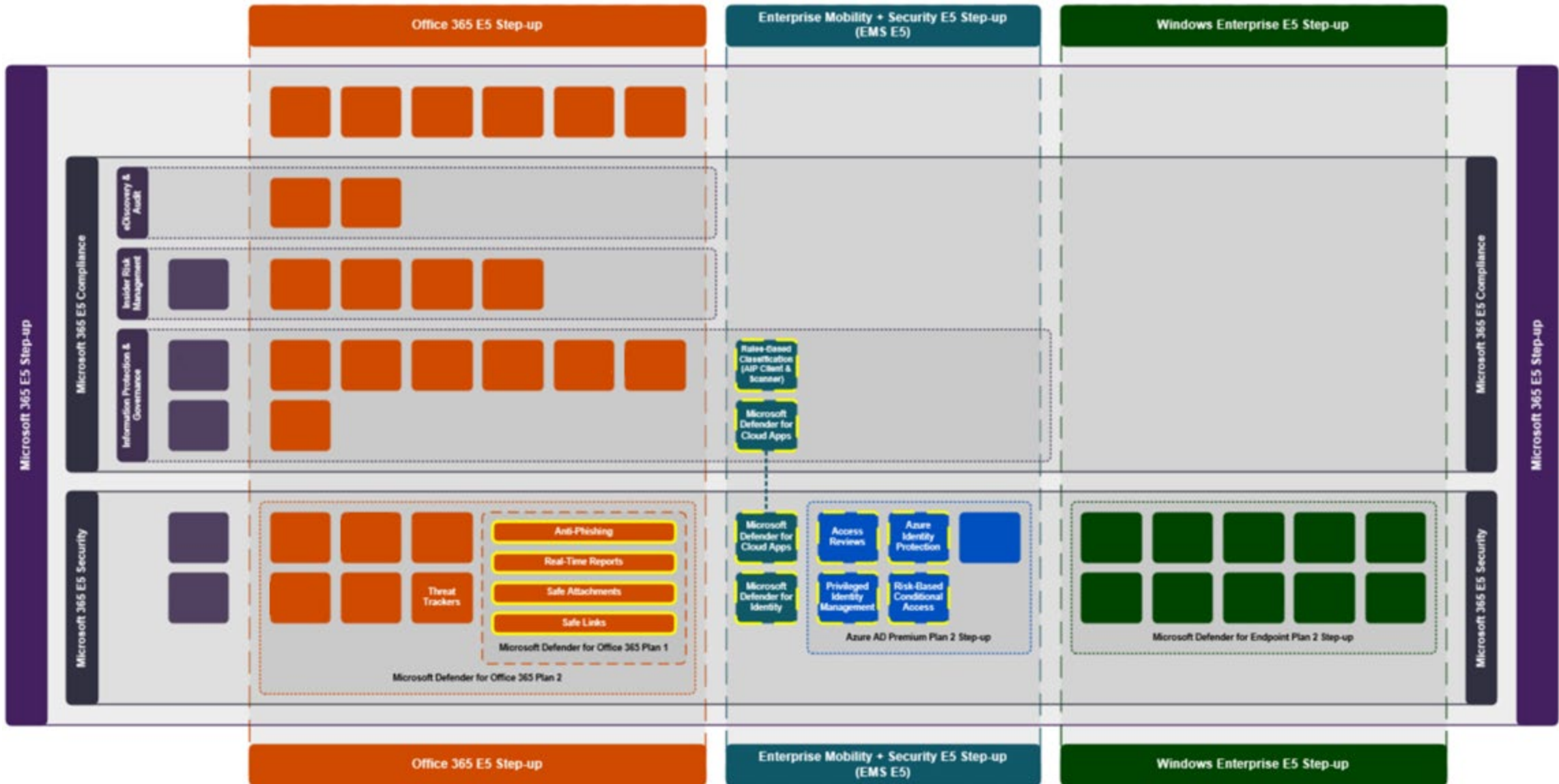
**Advanced Feature**  
Add to M365 Security Roadmap, Evaluate, Plan

80%

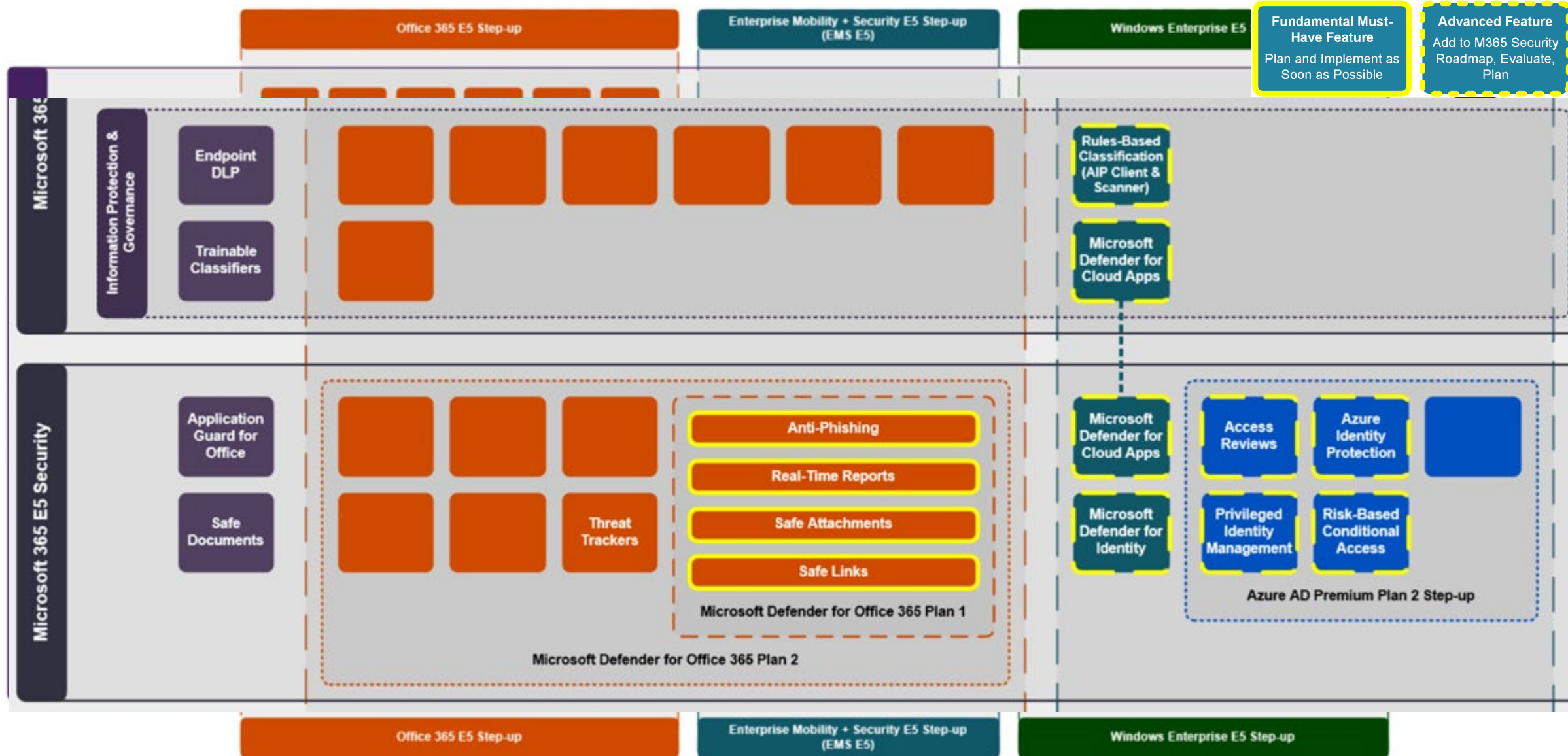
20%



# Microsoft 365 E5 Overview

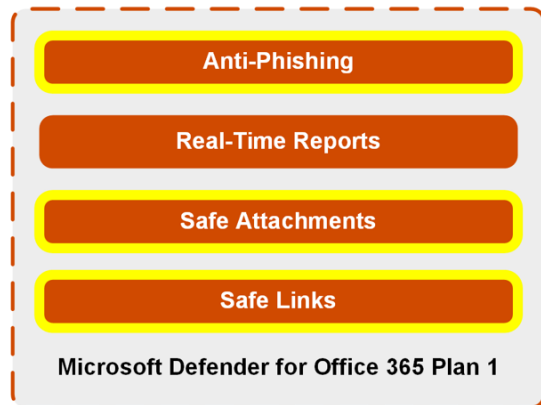


# Microsoft 365 E5 Overview



# Microsoft 365 Licensing

## Defender for Office 365 Plan 1



**Microsoft Defender for Office 365 Plan 1** provides a must-have features to protect against common attacks and malicious activity.

- Enhanced **Anti-Phishing** capabilities include **Anti-Impersonation** to protect from invoice phishing scenario, where an attacker impersonates an employee or one of your vendors, and requests payment of a fraudulent invoice.
- **Safe Attachments and Safe Links** provide additional layer of defense against common email attacks (sandboxing attachments and links)

**Microsoft Defender for Office 365 Plan 1 is an absolute must-have for all users** who will have an Exchange Online mailbox. This license provides a lot of concrete, usable functionality for a relatively low cost (1,41€ per user per month) and demonstratable security posture improvement.

Note: The Safe Links and Safe Attachments functionality also applies to Teams/SharePoint. Even if you already have a third-party mail gateway/scanning service, we still recommend **Defender for Office 365 Plan 1** to enhance/augment your security posture and defense-in-depth strategies.



# Q&A

**Volgende sessie:  
Uw datacenter in de public  
cloud: veiliger of net niet?**