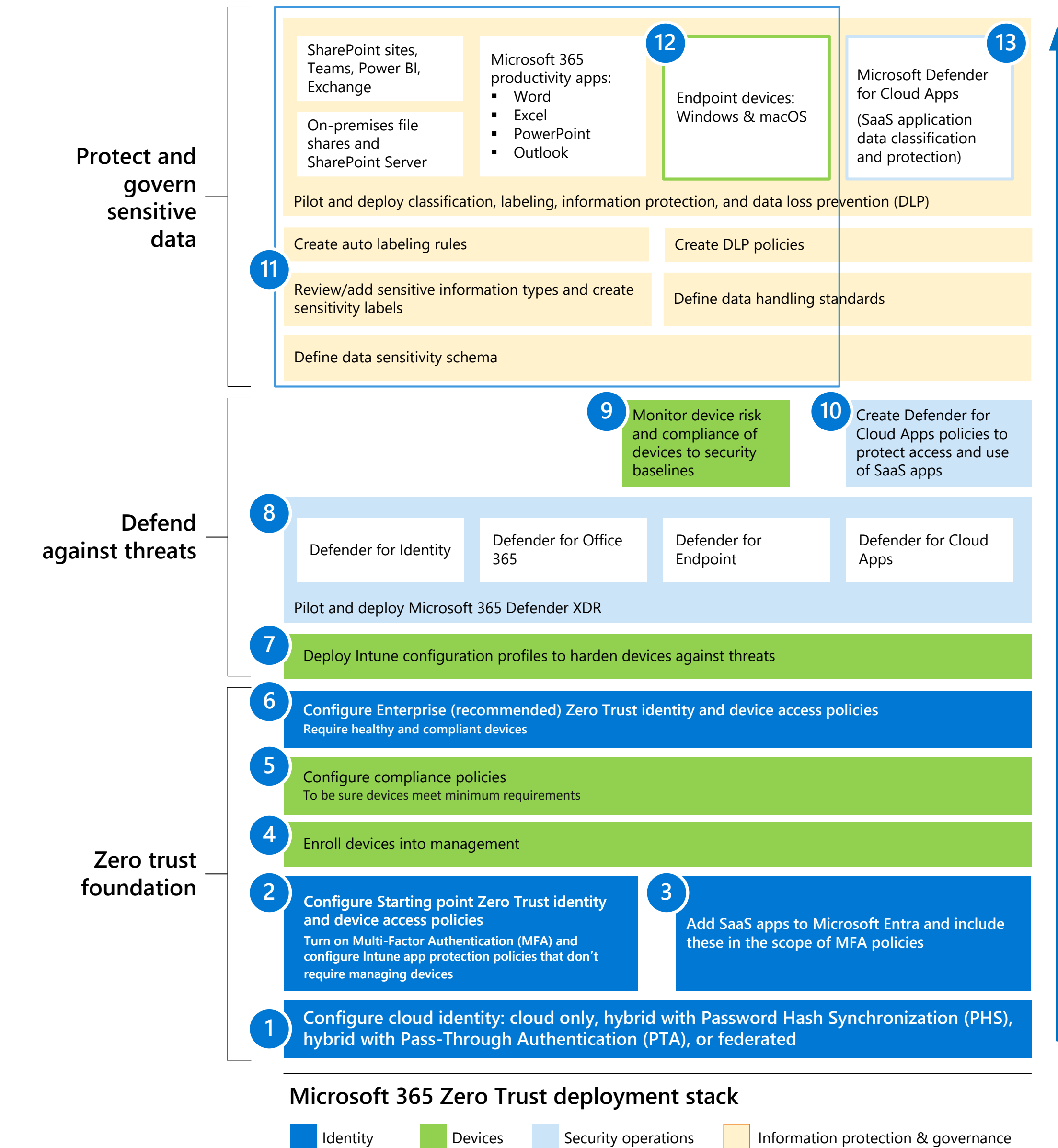# Zero Trust deployment plan with Microsoft 365

A **clickable** deployment plan in the Zero Trust universe

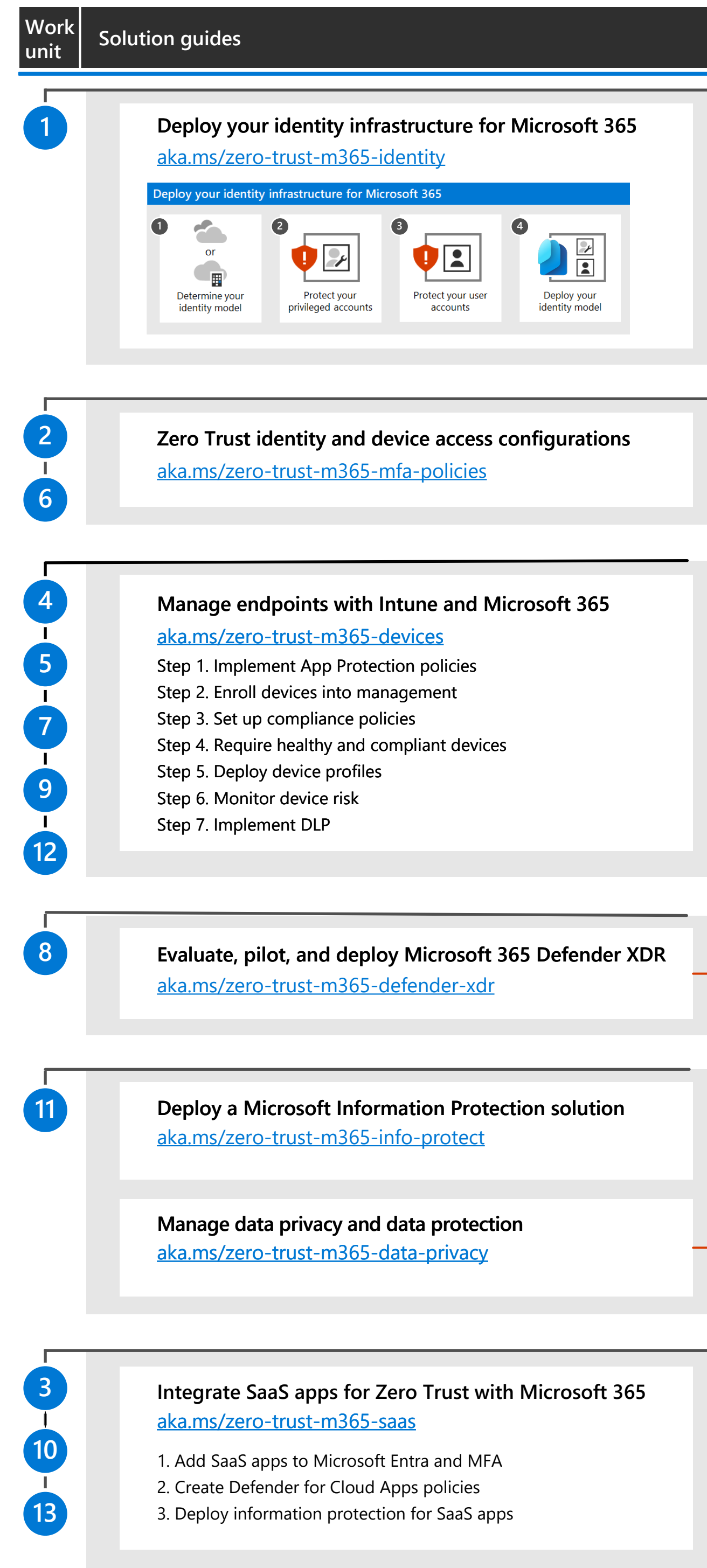## Deploying Zero Trust using Microsoft 365 capabilities

This poster represents the work of deploying Zero Trust capabilities with Microsoft 365. This work is broken into **units of work** that can be configured together, starting from the bottom and working to the top to ensure that prerequisite work is complete.

This Microsoft 365 Zero Trust deployment stack illustrates the recommended units of work. Read more here — aka.ms/zero-trust-m365.

Protect and govern sensitive data

- **12**
  - SharePoint sites, Teams, Power BI, Exchange
  - On-premises file shares and SharePoint Server
  - Microsoft 365 productivity apps:
    - Word
    - Excel
    - PowerPoint
    - Outlook
  - Endpoint devices: Windows & macOS
  - Microsoft Defender for Cloud Apps (SaaS application data classification and protection)

- **11** Pilot and deploy classification, labeling, information protection, and data loss prevention (DLP)
  - Create auto labeling rules
  - Create DLP policies
  - Review/add sensitive information types and create sensitivity labels
  - Define data handling standards
  - Define data sensitivity schema

Defend against threats

- **9** Monitor device risk and compliance of devices to security baselines
- **10** Create Defender for Cloud Apps policies to protect access and use of SaaS apps
- **8**
  - Defender for Identity
  - Defender for Office 365
  - Defender for Endpoint
  - Defender for Cloud Apps
  - Pilot and deploy Microsoft 365 Defender XDR
- **7** Deploy Intune configuration profiles to harden devices against threats

Zero trust foundation

- **6** Configure Enterprise (recommended) Zero Trust identity and device access policies — Require healthy and compliant devices
- **5** Configure compliance policies — To be sure devices meet minimum requirements
- **4** Enroll devices into management
- **2** Configure Starting point Zero Trust identity and device access policies — Turn on Multi-Factor Authentication (MFA) and configure Intune app protection policies that don't require managing devices
- **3** Add SaaS apps to Microsoft Entra and include these in the scope of MFA policies
- **1** Configure cloud identity: cloud only, hybrid with Password Hash Synchronization (PHS), hybrid with Pass-Through Authentication (PTA), or federated

Microsoft 365 Zero Trust deployment stack

- Identity
- Devices
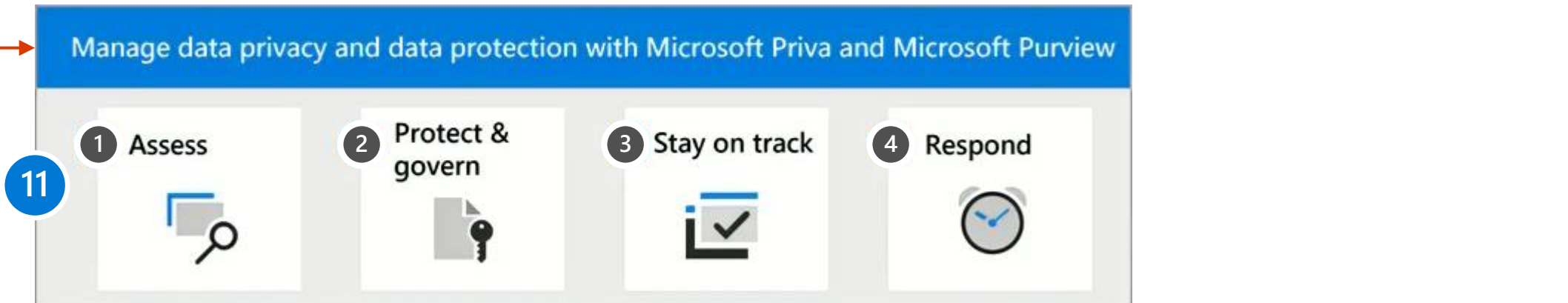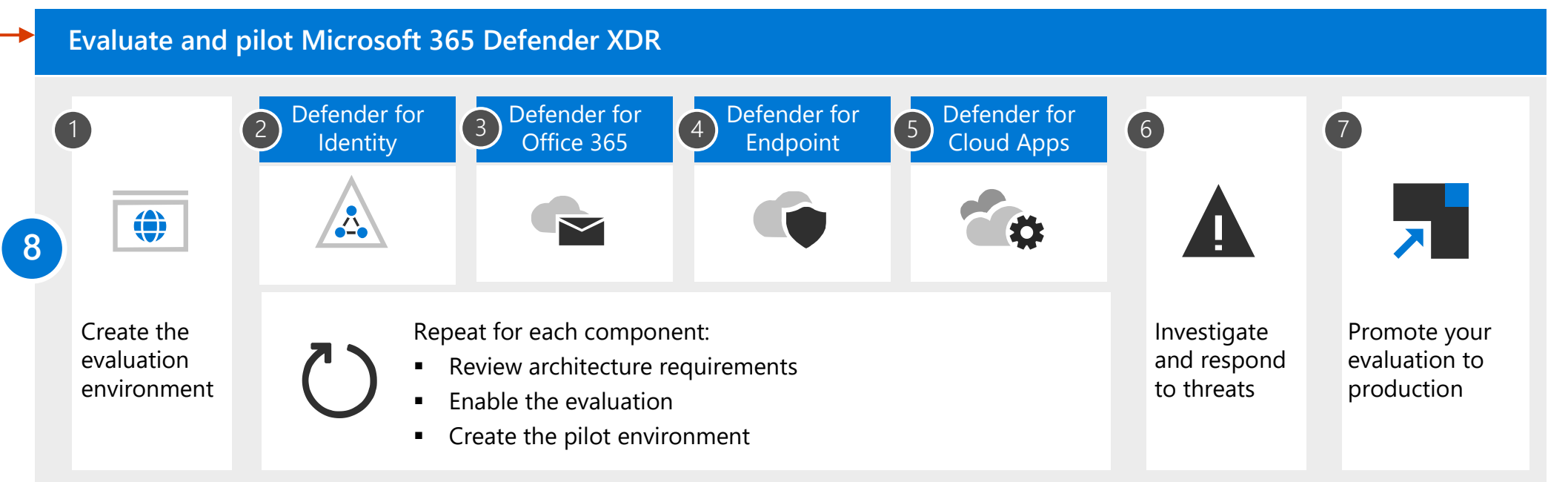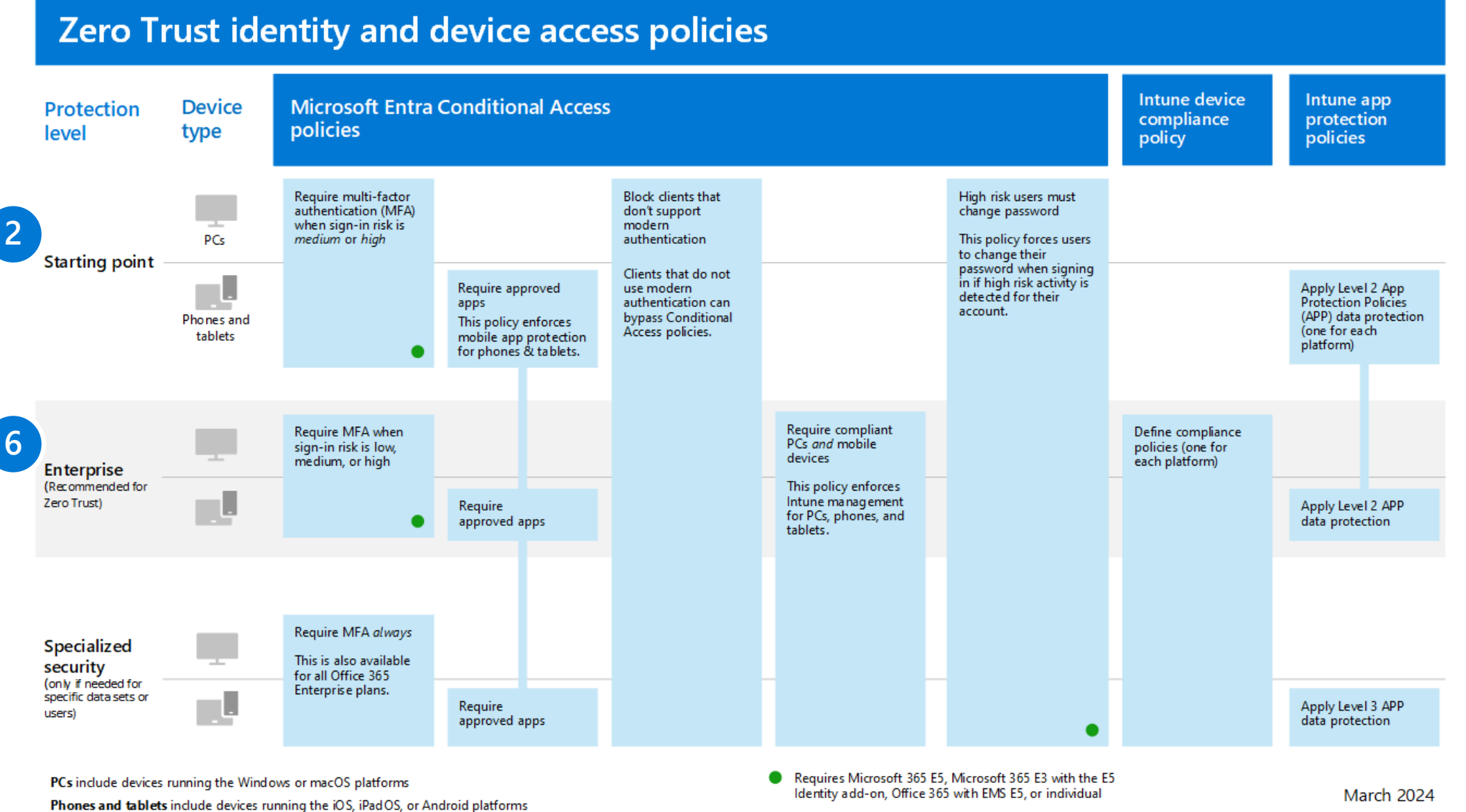- Security operations
- Information protection & governance

Prescriptive solution guides

Each of these guides describe how to accomplish specific units of work that are prescribed by the deployment plan.

Work unit	Solution guides
1	**Deploy your identity infrastructure for Microsoft 365** aka.ms/zero-trust-m365-identity
2 **6**	**Zero Trust identity and device access configurations** aka.ms/zero-trust-m365-mfa-policies
4 **5** **7** **9** **12**	**Manage endpoints with Intune and Microsoft 365** aka.ms/zero-trust-m365-devices Step 1. Implement App Protection policies Step 2. Enroll devices into management Step 3. Set up compliance policies Step 4. Require healthy and compliant devices Step 5. Deploy device profiles Step 6. Monitor device risk Step 7. Implement DLP
8	**Evaluate, pilot, and deploy Microsoft 365 Defender XDR** aka.ms/zero-trust-m365-defender-xdr
11	**Deploy a Microsoft Information Protection solution** aka.ms/zero-trust-m365-info-protect
	Manage data privacy and data protection aka.ms/zero-trust-m365-data-privacy
3 **10** **13**	**Integrate SaaS apps for Zero Trust with Microsoft 365** aka.ms/zero-trust-m365-saas 1. Add SaaS apps to Microsoft Entra and MFA 2. Create Defender for Cloud Apps policies 3. Deploy information protection for SaaS apps

Supporting illustrations

These illustrations from the prescriptive solution guides are included here for your reference.

Zero Trust identity and device access policies

March 2024

Evaluate and pilot Microsoft 365 Defender XDR

- **1** Create the evaluation environment
- **2** Defender for Identity
- **3** Defender for Office 365
- **4** Defender for Endpoint
- **5** Defender for Cloud Apps
- **6** Repeat for each component:
  - Review architecture requirements
  - Enable the evaluation
  - Create the pilot environment
- Investigate and respond to threats
- **7** Promote your evaluation to production

Manage data privacy and data protection with Microsoft Priva and Microsoft Purview

- **1** Assess
- **2** Protect & govern
- **3** Stay on track
- **4** Respond

Apply Zero Trust principles to Azure services
aka.ms/zero-trust-azure
This set of articles shows you how to apply the Zero Trust approach to new or already deployed Azure services, such as storage, virtual machines, virtual networks (Vnets), Azure Virtual Desktop, and Azure Virtual WAN.

Microsoft