Microsoft Security

Zero Trust Lab Guide Map

Scenario only applicable to the Hybrid Identity lab

Base Requirements	Introduction & lab guide use
	Sign up for my.visualstudio.com
	Create your M365 E5 Developer Tenant
	Configure your Azure Subscription

Start here

Choose your lab

| Hybrid Identity With Password Hash Sync | Cloud Only |

Azure

- Active Directory — 1 Windows Domain Controller
- Azure Bastion — Secure RDP Access

Zero Trust Pillar | Identity

- Cloud Sync
- Protect Your Global Admins & Enforce Least Privileged With PIM
- Secure Your Tenant With Conditional Access & Identity Protection
- Automating Group Membership & License Assignment
- Password Protection + Password Writeback
- Password Reset

Passwordless
1. Phone Sign-in → 2. Cert Based Auth → 3. WH4B + TAP → 4. FIDO2

- SaaS App Integration
- Application Proxy

Governance
1. Entitlement Management → 2. Access Reviews → 3. Lifecycle Workflows

Zero Trust Pillar | Devices

Devices
1. App Protection Policies (BYOD) → 2. Device Enrollment (MDM)

- Defender for Identity
- Defender for Office 365 → Defender for Endpoint → Defender for Cloud Apps → Defender for Cloud

Zero Trust Pillar | Data

Information Protection
1. Classify & Label Data → 2. Data Loss Prevention → 3. Data Retention Policies

Governance
1. Data Mapping → 2. Data Catalog → 3. Data Estate Insight

Zero Trust Pillar | Infrastructure

Security Controls
1. Security Benchmark → 2. Azure Policies → 3. Azure Infrastructure

Zero Trust Pillar | Threat Protection

1. Log Analytics → 2. Azure AD Workbooks → 3. Query AAD Audit/Sign-in logs

1. Data Collectors → 2. Investigate → 3. Respond