



Architecting Zero Trust in Azure: Real-World Scenario for Secure Access & Device Protection

Built with ❤️ by #PerparimLabs

[Home](#) > [Perparims Cloud Solutions](#) >

Perparims Cloud Solutions ...



◆ Microsoft Entra | Intune | Defender | Conditional Access



What Is Zero Trust?



Assume Breach

Treat every access attempt as if it comes from an untrusted source — internal or external.



Verify Explicitly

Always authenticate and authorize based on identity, location, device compliance, and risk.



Use Least Privilege Access

Limit user access with just-in-time (JIT) and just-enough-access (JEA), risk-based policies, and adaptive controls.



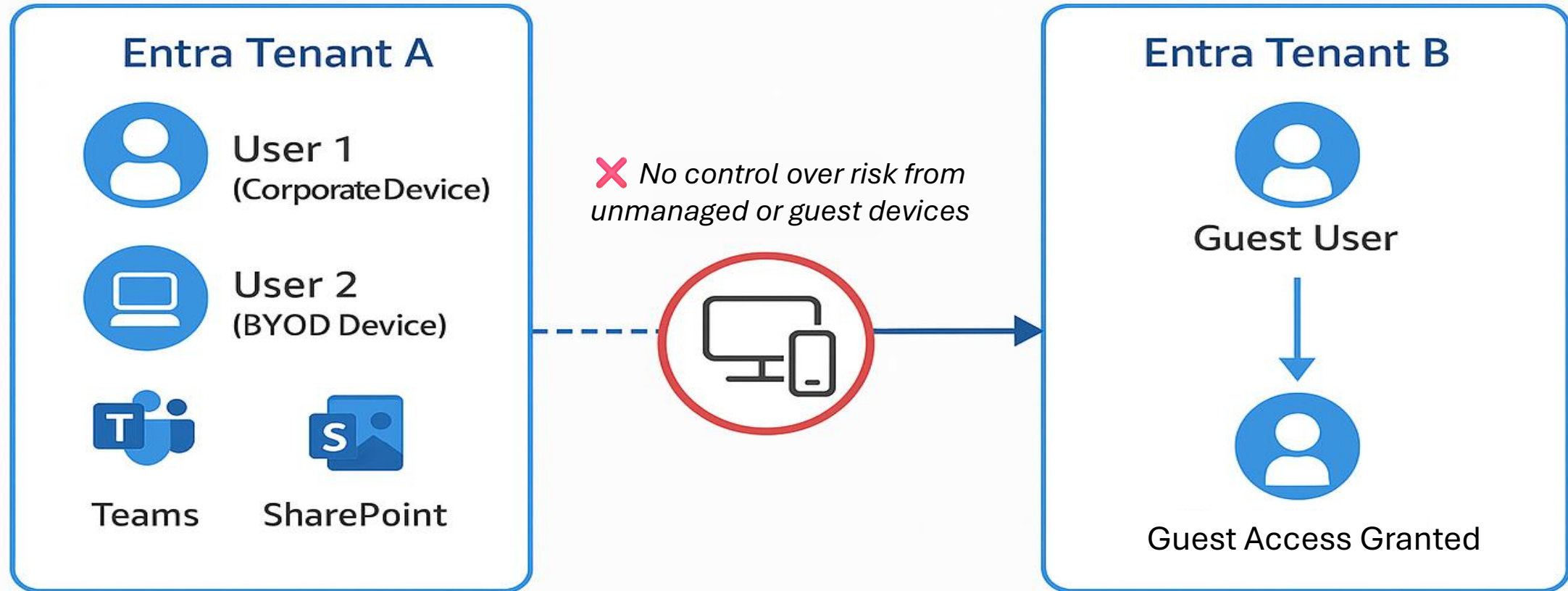
Real-World Scenario: Securing Access Across Devices & Tenants

- A global consulting company supports **hybrid work** across two Microsoft Entra tenants.
- Users access **Teams, SharePoint, and Microsoft 365 apps** from a mix of **corporate and BYOD devices**.
- Leadership needs to ensure secure collaboration without disrupting productivity — while **blocking risky logins, protecting data**, and keeping visibility across both environments.

★ Challenges:

- Unmanaged devices accessing corporate data
- Limited visibility into risky sign-ins
- Lack of control over guest and cross-tenant collaboration
- Data leakage concerns from mobile or personal devices

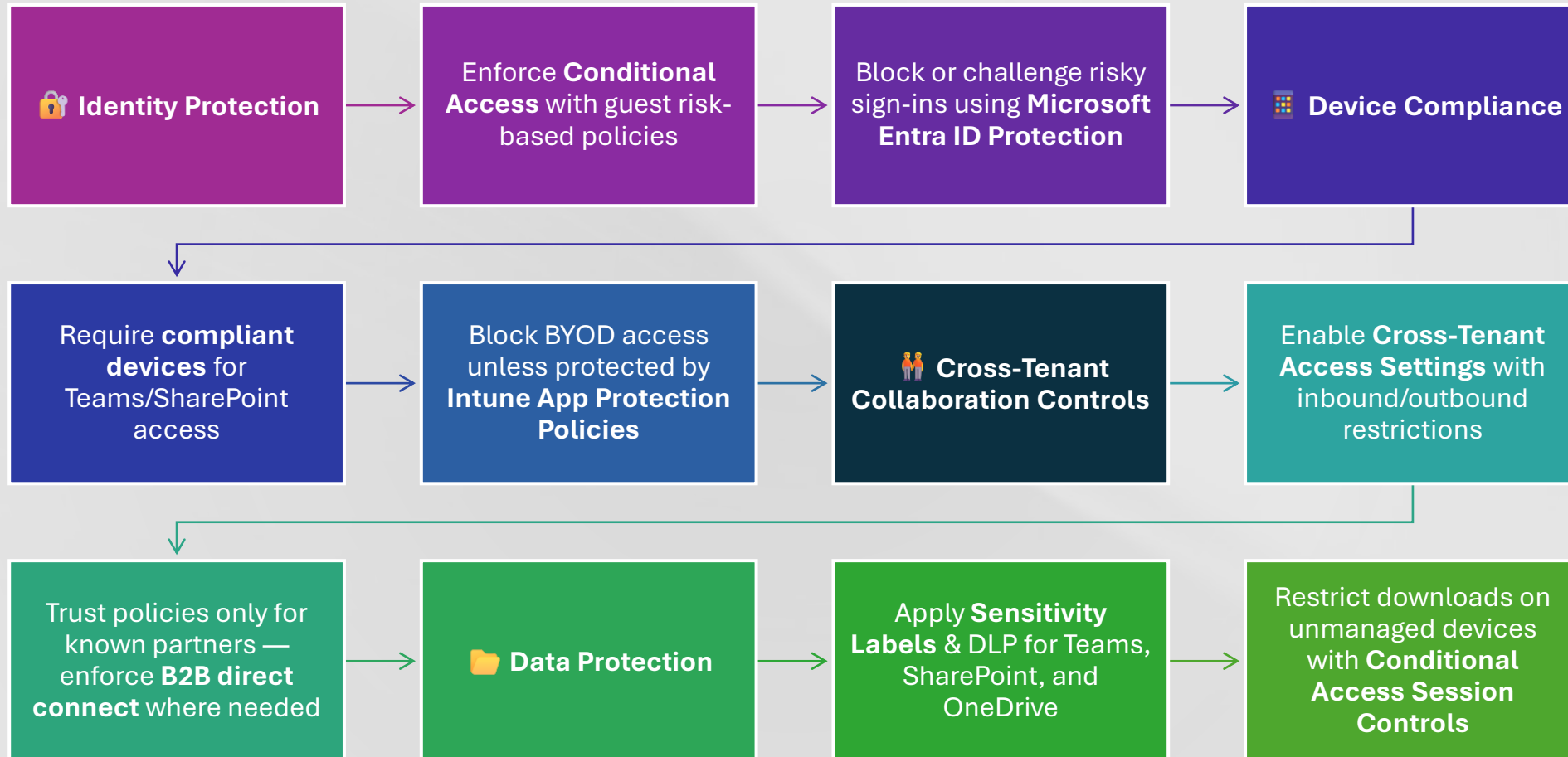
Cross-Tenant & BYOD Collaboration – Security Gaps



 **Goal**

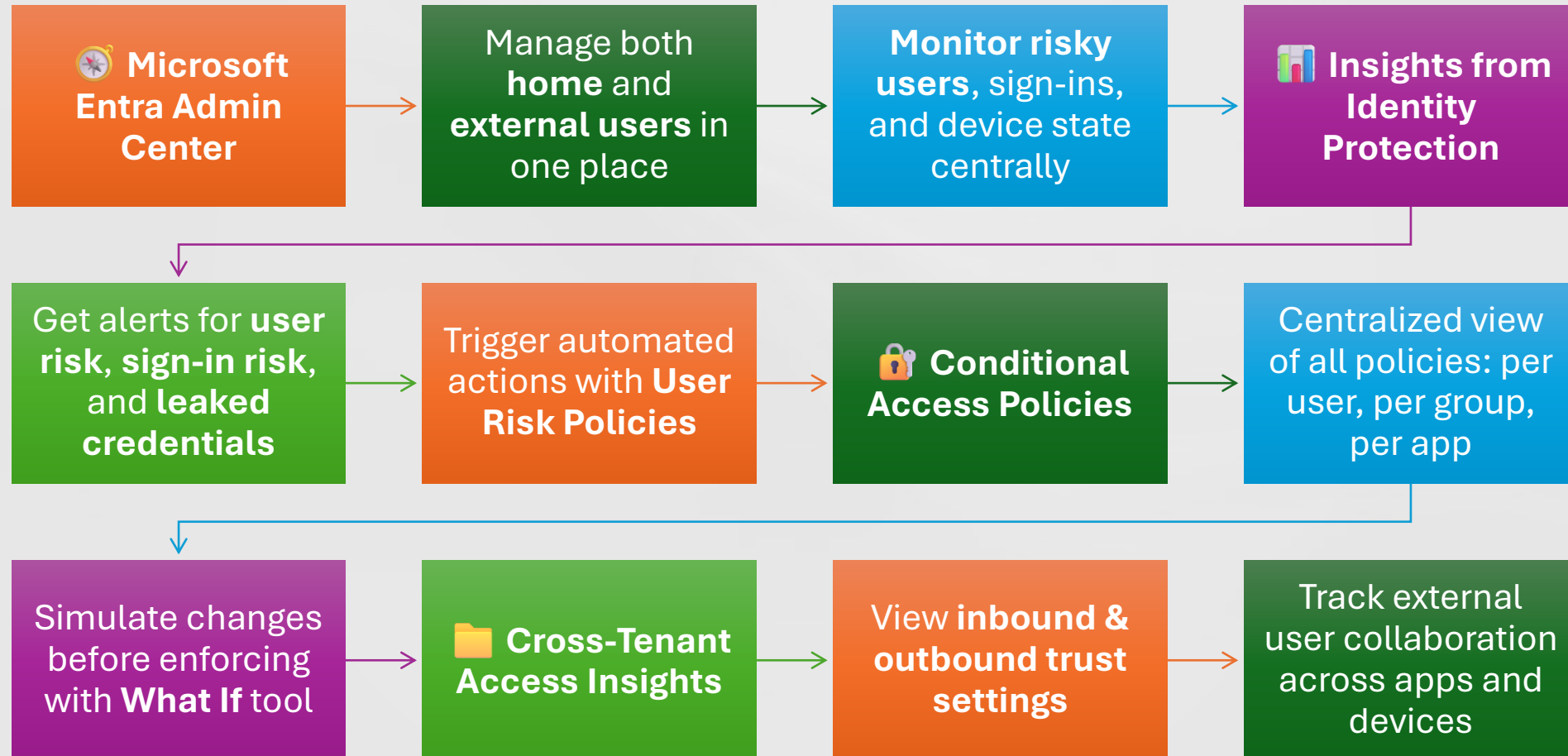
Apply Zero Trust — Protect access based on identity, device, and risk

Zero Trust in Action: Protecting Identities, Devices & Data



💡 **Security Principle: Never trust, always verify — enforce least privilege across tenants.**

Unified Visibility & Control Across Tenants



Even across two tenants, Microsoft Entra gives IT a single lens to manage security, access, and compliance.

Enforce Policies Based on Risk, Device & Location

Targeted Access Controls

Apply policies to **specific users, groups, or guests**

Enforce protection for apps like **Teams, SharePoint, Exchange**

Identity & Sign-In Risk Conditions

Block access for **high-risk users** (e.g., leaked credentials)

Require **MFA** for sign-ins from **new or suspicious locations**

Device State Enforcement

Block or limit access from **unmanaged (BYOD) devices**

Require **Intune-compliant** or **Hybrid Azure AD joined** status

Location & IP-Based Policies

Block access from **non-approved countries or IP ranges**

Allow trusted locations for smoother experience

Real-World Impact

Minimize exposure to threats

Maintain productivity without sacrificing security

With Conditional Access, every login is evaluated in real time — identity, device, risk, and location — then access is either granted, challenged, or denied.



Secure BYOD & Corporate Devices with Intune

✅ Real-World Benefit:

Guarantees that only secure, healthy devices can access sensitive company data — even in cross-tenant, hybrid scenarios.

Enroll Devices into Intune

- Support for **iOS, Android, Windows, macOS**
- Allow users to enroll **personal (BYOD)** or **corporate devices**


Apply Compliance Policies


- Block access for devices that:
 - Are **jailbroken/rooted**
 - Don't have **passcode/PIN**
 - Have **malware or outdated OS**

Conditional Access + Compliance

- Allow Teams, SharePoint access **only from compliant devices**
- Enforce **app protection policies** for BYOD (no data leaks)

Data Protection for BYOD

- Prevent copy/paste, screen capture, or saving to personal storage
-  Wipe corporate data remotely if needed



Control Guest Access with Microsoft Entra B2B & Cross-Tenant Policies

Add External Users as Guests

- Invite users from other tenants via **Microsoft Entra ID**
- Require them to **redeem the invitation** and accept terms

Cross-Tenant Access Settings

- Define **inbound & outbound rules** per connected organization
- Allow or block **MFA trust**, **device trust**, and **group membership mapping**


Limit Guest Permissions

- Restrict guests to **specific Microsoft 365 groups or Teams**
- Prevent elevation of privileges via **Role Assignments** or **Directory Roles**

Secure Resource Sharing

- Protect SharePoint/OneDrive access with:
 - **Sensitivity Labels**
 - **DLP rules**
 - **Session controls** (e.g., block download)

Monitor & Review Guest Access

- Use **Access Reviews** to regularly review guests
-  Auto-remove inactive or unapproved external users

Zero Trust means trusting guests by policy, not by default.





Real-Time Monitoring with Microsoft Defender & Logs



Microsoft Defender for Cloud Apps

- Detect **suspicious guest activity** (e.g., impossible travel, large downloads)
- Apply **session policies** to limit risky behavior
- Integrates with Entra ID, Intune, and Defender for Endpoint

Sign-In & Audit Logs in Microsoft Entra

- Track every login attempt, policy evaluation, and access granted/denied
- Correlate with user risk, device risk, and IP location


Defender for Identity (optional)


- Monitor **hybrid identities** and **on-prem AD threats** (if used)
- Detect lateral movement, pass-the-hash, brute force attacks

Alerts & Automated Response


- Route alerts to **Microsoft Sentinel** for full SIEM/SOAR visibility
- Trigger **automated remediation**: disable user, reset password, block session

In Zero Trust, visibility is everything. You can't protect what you don't monitor





Zero Trust in Action: Key Takeaways



1. Identity Is the New Perimeter

- Secure every user — internal or guest — with **Conditional Access, risk detection, and MFA.**

2. Devices Must Be Compliant

- Only healthy, managed or protected devices get access — **Intune** is key.

3. External Access Must Be Governed


- Control guests and B2B users with **Cross-Tenant Access, Access Reviews, and limited permissions.**

4. Visibility = Control

- Use **Entra logs, Defender for Cloud Apps, and Sentinel** to detect and respond in real-time.

5. Zero Trust Is a Strategy, Not a Switch

- This is a journey — but each control you apply builds a more secure, resilient Azure environment.

 *These principles turn Zero Trust from theory into action — one identity, one device, one policy at a time.*



Microsoft Tools That Brought This Solution to Life



Microsoft Entra ID

- Identity Governance, Conditional Access, Cross-Tenant Access, Risk Policies

Microsoft Intune

- Device Compliance, App Protection Policies for BYOD

Microsoft Teams + SharePoint Online

- Core collaboration platform protected by policies

Microsoft Defender for Cloud Apps

- Session Controls, Threat Detection for guest and app activity

Microsoft Sentinel (Optional)

- SIEM integration for advanced threat response (if mentioned earlier)

Microsoft Purview (Optional)

- Sensitivity Labels, DLP for secure file sharing (if shown in your flow)

All part of Microsoft's modern security stack — enabling real-world Zero Trust, not just buzzwords.





Join the Journey – Cloud Security, Zero Trust & More



 I post weekly projects on:

- Microsoft Entra ID
- Intune & Endpoint Security
- Defender, Conditional Access, Governance
- Real-world Zero Trust architecture



 **Follow or connect with me:**
Perparim Abdullahu | Cloud Security Architect
 [linkedin.com/in/perparim-abdullahu-2b0530324](https://www.linkedin.com/in/perparim-abdullahu-2b0530324)

[Home](#) > [Perparims Cloud Solutions](#) >
Perparims Cloud Solutions ...

